[redacted]

(U) ORGANIZATIONAL ASSESSMENT: THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

(U) AUDITS AND PROJECTS REPORT 22-01

(U) SELECT COMMITTTEE ON INTELLIGENCE

(U) UNITED STATES SENATE

[redacted]

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

(U) ORGANIZATIONAL ASSESSMENT: THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Table of Contents

(U) EXECUTIVE SUMMARY 1

(U) ABBREVIATIONS 10

(U) INTRODUCTION AND METHODOLOGY 12

(U) CURRENT THREAT LANDSCAPE 14

A. (U) Current Adversaries and Threat Actors 14

B. (U) Current FIE Targets 28

C. (U) Current FIE Tactics 35

D. (U) Overview of the National Counterintelligence and Security Center 50

(U) FINDINGS 57

A. (U) MISSION 57

1. (U) It is Unclear Whether Certain FIE Threats and USG Activities to Counter Them Fall within the Definition of CI 57

2. (U) The Boundaries of the CI Enterprise are Unclear 62

3. (U) Traditional CI and Strategic CI are Different Missions—but it is Unclear Whether NCSC Should Focus on Traditional CI, Strategic CI, or Both 69

4. (U) NCSC Plays a Limited Role in Offensive CI Despite its Importance to the Strategic CI Mission 75

B. (U) DUTIES AND AUTHORITIES 81

1. (U) NCSC Does Not Fulfill All Statutorily Assigned Duties Partly Due to Authority and Resource Limitations 81

2. (U) NCSC Conducts Several Duties Not Assigned in Statute due to Perceived IC Need 102

C. (U) RESOURCES AND STAFFING 108

1. (U) Key NCSC Duties are Limited due to Staffing and Resource Constraints 108

2. (U) NCSC's Staff Composition is Appropriate 110

3. (U) Change in NCSC Staffing Over Time 111

4. (U) NCSC's Hiring Procedures Take Time 112
5. (U) NCSC's Budget is Small Relative to its Mission 113
D. (U) LOCATION AND STRUCTURE 116
1. (U) NCSC Experiences Drawbacks and Benefits as an ODNI Center 116
2. (U) Officials Disagree Over Whether NCSC Should Remain Exclusively Within the IC 121
(U) CONCLUSION AND RECOMMENDATIONS 129
(U) APPENDIX A: EVOLUTION OF CI AUTHORITIES 134

(U) EXECUTIVE SUMMARY

(U) The Senate Select Committee on Intelligence (SSCI or the Committee) has long expressed interest in reviewing the United States Government (USG) counterintelligence (CI) enterprise to identify actions needed to enhance its posture, capabilities, and responsibilities in response to contemporary foreign intelligence entity (FIE) threats. The Committee tasked the Audits & Projects Team (Team) with conducting a targeted organizational assessment of the National Counterintelligence and Security Center (NCSC or the Center)—the statutory head of U.S. CI—to understand whether this entity is properly authorized, resourced, and structured to carry out its mission. ***This report seeks to (1) identify the key challenges facing NCSC in carrying out its mission and (2) capture a range of opinions from CI experts on those challenges and potential ways forward.***

(U) CURRENT THREAT LANDSCAPE

(U) The United States faces a dramatically different threat landscape today than it did just a couple of decades ago. Multiple adversaries target nearly every sector of U.S. society using traditional and novel tactics and techniques. As the current National CI Strategy notes, FIEs—"to include nation-states, organizations, and individuals—are employing innovative combinations of traditional spying, economic espionage and supply chain and cyber operations to gain access to critical infrastructure and steal sensitive information, research, technology, and industrial secrets." These changes have profound implications for the mission, structure, authorities, and resources of the CI enterprise in general and NCSC in particular.

(U) During the Cold War, the United States' main adversary was the Soviet Union and other Warsaw Pact countries, as well as Soviet client states such as Cuba. After the terrorist attacks of September 11, 2001, the United States pivoted to focus on al-Qaeda and other extremist jihadist groups around the world. Today, however, the United States faces a wide variety of adversaries to include powerful state rivals with global ambitions—namely China and Russia—regional adversaries, minor states aligned with U.S. adversaries, ideologically motivated entities, and transnational criminal organizations.

(U) FIEs target desired information wherever it may reside. Many FIE efforts previously focused primarily on state secrets held by the Intelligence Community (IC) and the broader national security establishment. Now, however, FIEs target a wide range of information from entities and individuals across nearly every sector of U.S. society. As the *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Iraq WMD Commission) noted: "Spies have always existed, but currently our adversaries—and many of our 'friends'—are expanding and intensifying their intelligence activities against U.S. interests worldwide. They target virtually all of our nation's levers of power." Put simply, FIE threats to the United States are now more complex, diverse, and harmful to U.S. interests, and FIEs are targeting a wider set of public and private

[redacted]

entities to include NT-50s (that is, non-IC USG departments and agencies that do not have 50 U.S.C. authorities, such as the Department of Health and Human Services or the National Science Foundation) as well as national laboratories, the financial sector, the U.S. industrial base, and academic entities.

(U) In the past, U.S. adversaries had relatively limited options for stealing information, influencing U.S. officials, or inflaming social and political tensions. Traditional intelligence collection and influence efforts required foreign nations to, for example, send spies to U.S. soil, co-opt an insider, target U.S. officials when overseas, bug offices, or intercept U.S. communications from collection facilities around the world. Today, however, U.S. adversaries have access to a much wider variety of tools to accomplish their goals, and the damage is far greater. In addition to traditional espionage—which continues unabated—FIEs can now exploit non-traditional human, cyber, advanced technical, and open source intelligence operations to collect against U.S. plans and policies, sensitive technology, personally identifiable information (PII), and intellectual property, as well as to influence U.S. decision-making and public opinion on a scale previously unimaginable.

(U) FINDINGS

(U) As illustrated above, the FIE threat landscape facing the country today is wide-ranging and sophisticated. Yet ***NCSC, as the USG lead for CI, lacks a clear mission as well as sufficient and well-defined authorities and resources to effectively confront this landscape.*** Moreover, ***NCSC's placement within the Office of the Director of National Intelligence (ODNI) may hinder its ability to scale and respond to threats in an agile manner.*** Despite these challenges, ***there is no consensus among CI officials on a way forward for NCSC.***

(U) MISSION

(U) Under current law, the mission of the Director of NCSC is to "serve as the head of national counterintelligence for the United States Government." The Committee, however, found that the scope of this mission is not clear to the Committee, to the broader IC, or even to some NCSC officials. First, it is unclear whether certain FIE threats—namely, cyber and foreign malign influence—as well as USG activities—namely, "CI awareness" activities such as FIE target identification, foreign travel briefings, and receipt and review of certain CI products —fall within the current definition of CI. Second, various current and former NCSC officials disagree over which types of entities comprise the CI enterprise that NCSC is tasked with leading. Specifically, it's not clear whether non-title 50s (NT-50s)—that is, non-IC entities that do not have 50 U.S.C. authorities—private sector entities, or academic institutions should be considered part of the CI enterprise and should therefore have CI responsibilities. Third, there is no consensus as to whether NCSC should focus on traditional CI activities, the strategic CI mission, or both. Traditional CI is internally-focused on the protection of individual IC entities,

[redacted]

[redacted]

whereas strategic CI focuses on using all available national resources to defend the United States as a whole rather than on protecting individual IC entities or their parochial operations. Fourth, NCSC plays a marginal role in offensive CI, despite the importance of offensive CI to the CI mission. Finally, officials disagree on the optimal relationship between CI, which directly deals with the threat from FIEs, and security, which indirectly defends against FIE actions by minimizing vulnerabilities, and over what specific role NCSC should play with regards to security.

(U) DUTIES AND AUTHORITIES

(U) NCSC's duties have changed over its 20-year lifespan, due in part to lack of clarity over its mission. Various duties are enumerated in statute, but NCSC does not effectively fulfill all of them. In addition, NCSC has taken on several duties not explicitly assigned in statute. In general, the Committee assesses that NCSC's focus at any given time is based on the perceived CI gaps the IC needs filled or the interests of its Director, rather than on a well-formulated and enduring vision of the activities it should be undertaking to support its mission. Former National CI Executive Michelle Van Cleave noted that "fundamentally, there is no agreed-upon understanding of what NCSC is supposed to do." Several FBI officials also told the Committee that NCSC "seems to be all over the place." One NCSC official said that NCSC's "sweet spot" is not to replicate work already being done by the IC, but to identify and fill gaps and seams. Thus, NCSC often takes on projects that do not have "natural homes" at other agencies, offloading projects to agencies better suited to handle them when possible.

(U) NCSC is also limited in its ability to carry out its duties by ambiguous or insufficient authorities. NCSC can influence and advocate for IC CI spending, but NCSC has little authority or leverage over IC entities' budgets and budget priorities. NCSC can also provide voluntary guidance, threat awareness, and advice to NT-50s and non-USG entities on developing and maintaining effective CI and security programs, but NCSC cannot provide direct financial support, and NT-50s and non-USG entities are not required to maintain CI programs. NCSC officials told the Committee that much of NCSC's ability to influence CI and security programs across the USG stems from personal relationships and advocacy, rather than statutes, regulations, or other authorities.

(U) RESOURCES AND STAFFING

(U) Staffing and resource constraints impact NCSC's ability to effectively carry out its mission. One senior NCSC official described [redacted] For example, several key NCSC duties, including [redacted] constrained due to NCSC staffing levels.

(U) Despite [redacted] staffing and resource levels, NCSC officials indicated that its current mix of permanent staff (cadres), joint-duty staff (detailees), and

[redacted]

[redacted]

contractors was appropriate. NCSC, however, faces several unique staffing challenges owing to its position as a Center within ODNI. For instance, several NCSC officials described how the approval process for cadres and detailees is time consuming—it is a "nonstop challenge." One NCSC official told the Committee that it can take more than two months to bring on a detailee and between 12 and 18 months to hire an external candidate, leading some candidates to seek a position elsewhere.

[redacted] Finally, NCSC's budget is small relative to its mission and is controlled by ODNI. Yet ODNI has not requested any substantial growth for NCSC's budget or full-time employees (FTE), nor has Congress provided it. Moreover, NCSC's budget is [redacted]

(U) LOCATION AND STRUCTURE

[redacted] NCSC is structured as a Center within ODNI. There are various drawbacks and benefits associated with this structure. According to various officials, drawbacks include: [redacted]

(U) NCSC is also located entirely within the IC, as its authorities stem from Title 50 and it is funded by the National Intelligence Program (NIP). Officials disagree over whether this is the appropriate location for NCSC. Some officials argue that CI is primarily an IC responsibility and thus should remain exclusively within the purview of the IC. Other officials argue that strategic CI is a whole-of-society responsibility, so NCSC should span the IC and NT-50 worlds.

(U) Finally, former NCSC Director William Evanina has argued for the establishment of an independent National Counterintelligence and Security Agency, which would be responsible for the strategic CI mission and focus on protecting the United States as a whole. If such an agency were to be established, several officials suggested incorporating other existing USG entities with close ties to the strategic CI mission.

(U) CONCLUSION AND RECOMMENDATIONS

[redacted]

(U) The U.S. CI enterprise is not postured to confront the whole-of-society FIE threat landscape facing the country today. CI as a mission first arose throughout the IC after World War II to defend IC operations, and the United States is still living with the legacy of that structure. Although that structure may have been appropriate when FIEs were primarily targeting information held by the IC and other national security entities, today's FIEs dedicate enormous energy and resources to acquiring not only sensitive state secrets, but also information from NT-50s and non-USG entities—which are significantly more vulnerable targets than the IC. There is thus a "disconnect" between the location of valuable information relevant to U.S. national security interests and what the U.S. CI enterprise is tasked with protecting.

(U) As more and more sensitive information has moved outside the protective walls of the IC, CI as a mission has struggled to adapt. The very definition of CI—both in terms of the types of activities FIEs conduct to target the United States, as well as the types of U.S. efforts to counter those activities—is murky and no longer clearly reflects the reality on the ground. For instance, various non-IC entities have established or are establishing "CI programs," but their CI activities conceptually overlap in many ways with the security mission and do not conform to the traditional understanding of CI activities—namely efforts to identify, deceive, exploit, disrupt, or protect against espionage. ***The USG must determine which FIE and USG activities fall within the CI mission set today, draw clear boundaries between the CI and security missions and clarify where "CI awareness" activities fall, and clarify the roles and responsibilities of USG and non-USG entities tasked with carrying out the CI and/or security missions.***

(U) This distinction is important because it implies different national security models; CI measures deal directly with FIE activities, whereas security programs indirectly defend against FIE actions by minimizing vulnerabilities. Thus, under an expansive CI enterprise model, the entire USG and potentially non-USG entities would bear responsibility for dealing directly with FIE activities. On the other hand, a more traditional CI enterprise model would be based exclusively on the IC—but could nevertheless require non-IC entities to be responsible for defensive security measures to identify and mitigate vulnerabilities.

[redacted] In either case, tactical, one-off responses are no longer sufficient to address the current FIE threat landscape; a strategic response is required. Yet, the U.S. CI enterprise has not fully pivoted to confront this new reality. [redacted]

[redacted]

[redacted]

[redacted]

(U) Moreover, CI as a discipline has traditionally been undervalued in the USG. Back in 2005, the Iraq WMD Commission, for example, noted that CI has been "plagued by a lack of policy attention and national leadership" and is largely neglected by policymakers and the IC. The Commission also stated that CI actually lost stature after September 11, 2001 as the USG turned its attention to counterterrorism (CT). The 2009 Intelligence and National Security Alliance (INSA) report *Counterintelligence for the 21st Century* noted that CI was not a priority for their first two Directors of National Intelligence (DNI). Mr. Evanina added that agency heads often assign lower priority to CI divisions and programs than to offensive mission requirements. As of July 2022, the Administration has not yet officially nominated a permanent NCSC Director, despite the position being vacant for over a year.

(U) The impact of all these challenges is clear: foreign adversaries compromise U.S. assets across the globe, acquire billions of dollars a year in U.S. research and technology, jeopardize the competitiveness of U.S. companies and the economic dominance of the United States, steal sensitive PII on USG employees and U.S. citizens, and interfere in domestic affairs. The USG cannot allow this situation to continue without serious repercussions for U.S. national security.

(U) Congress last tried to seriously reform CI statutes in 2002, when it passed the Counterintelligence Enhancement Act and created NCSC's precursor to try to better integrate the CI silos scattered across the IC. The Committee believes that NCSC has made progress towards achieving that goal. Yet NCSC lacks the necessary clarity of mission, sufficient authorities and resources, and an optimal location and structure to truly lead U.S. CI and to execute the strategic CI mission.

[redacted] It is time for Congress to take another hard look at the ability of the U.S. CI enterprise in general and NCSC in particular to confront today's FIE threat landscape. As Vice Chairman Rubio noted during a hearing on CI in 2020: "The IC may need a fundamental rethink of its counterintelligence enterprise." As Ms. Van Cleave told the Committee: "The USG does not have the right 'business model' for CI; rather than being strategic, forward-looking, and proactive, U.S. CI is tactical, reactive, and defensive." Mr. Evanina has similarly called for "a dramatic new construct to ensure adequate and enhanced coordination of a holistic CI program for the United States."

(U) There is no easy "fix" to U.S. CI, nor is there one single way in which NCSC could be reformed to better serve as head of national CI. If Congress and ODNI determine that NCSC should focus exclusively on better operationalizing

[redacted]

traditional CI activities, then NCSC may not need additional authorities or resources, and a structural change to the Center may not be necessary. ***Yet, there must be an "owner" for strategic CI to address the FIE landscape facing the nation today, and NCSC is currently the only USG entity positioned lead this mission.*** If Congress and ODNI assign the strategic CI mission to NCSC, then bigger changes to the Center may be warranted. Owning strategic CI would require sufficient authorities and resources to enable NCSC to successfully develop a strategic CI program to bring together all the means of execution for strategic CI priorities. In addition, Congress may want to consider whether NCSC can best carry out the strategic CI mission as a Center within ODNI, or whether such a mission requires the establishment of an independent agency spanning the IC and NT-50s universe.

(U) This Committee recognizes that any major change to the CI enterprise will be difficult and time consuming, and that various members of the USG may fiercely resist such changes. However, the USG has made big, bold changes before. After the terrorist attacks of September 11, 2001, Congress reorganized the U.S. national security enterprise to better confront terrorism. But more importantly, Congress helped to reorient the CT mission away from reactive, defensive efforts focused on figuring out who conducted a specific terrorist attack towards a proactive, offensive posture focused on stopping terrorists before they strike. It is time for CI to undergo a similar revolution and to receive the national-level attention it deserves.

(U) SSCI Recommendations

Definitions

1. The Executive Branch should develop and adopt, and Congress should codify, a consistent USG-wide definition of CI that:
    a. Reflects today's FIE threat landscape; and
    b. Delineates CI and security.
2. The Executive Branch should develop and adopt, and Congress should codify, related definitions to include strategic CI and offensive CI.

The CI Enterprise

3. NCSC, in consultation with ODNI, should identify the conceptual boundaries of the CI enterprise, including by identifying key stakeholders (e.g., which entities are members, partners, beneficiaries, etc.); outline stakeholders' CI and security roles and responsibilities; and clarify their relationship with NCSC.

[redacted]

4. NCSC, in consultation with ODNI, should determine what role each element of the IC should play in protecting non-USG entities that FIEs target for their research, technologies, data, and IP.
5. NT-50s should consistently establish "CI awareness" and/or security programs to ensure that USG data and sensitive information are identified and protected.

NCSC's Mission and Structure

6. Congress, in consultation with the Executive Branch, should clarify NCSC's mission and determine what, if any, role it should play in:
    a. Traditional CI;
    b. Strategic CI; and
    c. Offensive CI operations.
7. Congress, in consultation with the Executive Branch, should determine whether NCSC should remain a Center within ODNI or should be established as an independent agency.
8. Congress, in consultation with the Executive Branch, should determine which aspects of the security mission NCSC should retain.
9. Congress, in consultation with the Executive Branch, should consider whether the Director of NCSC/NCSA should be the official Sec/EA.

NCSC's Duties

10. NCSC should develop a strategic plan to conduct vulnerability assessments within the IC, NT-50s, and selected non-USG entities or sectors, and should request resources and authorities necessary to conduct those assessments.
11. NCSC should develop a plan for IC CI outreach to non-IC entities, including:
    a. Identifying IC outreach roles and responsibilities for each element of the IC; and
    b. Identifying and requesting resources and authorities necessary to implement this plan.
12. The USG should consider establishing a dedicated CI R&D fund and a CI R&D board to fund and oversee R&D efforts.
13. NCSC should develop a strategic plan, in consultation with relevant stakeholders, for CI R&D efforts.
14. NCSC should develop a plan for strategic CI training across the IC as well as for NT-50s and non-USG entities.
15. NCSC should establish a clear vision of what, if any, role it should play in developing and maintaining IC databases that support the CI mission.

NCSC's Authorities and Resources

[redacted]

16. Congress or the Executive Branch should provide NCSC with explicit authorities to ensure that NCSC can require appropriate CI entities to participate in NCSC-led efforts in support of the National CI Strategy.
17. If Congress determines that NCSC should own the strategic CI mission, then Congress should provide NCSC with the appropriate authorities and resources necessary to develop and execute a strategic CI program including:
    a. Strengthening NCSC's authorities to determine IC strategic CI budgets.
    b. Considering the establishment of a separate appropriation for NCSC to support NT-50 and non-USG CI programs with strategic CI and/or security objectives and/or clarifying ODNI's ability to transfer NIP resources to NT-50s.
    c. Providing NCSC with authorities to task CI entities with carrying out specific elements of a strategic CI program.

(U) ABBREVIATIONS

APT	Advanced Persistent Threat
CBP	Customs and Border Protection
CI	Counterintelligence
CIA	Central Intelligence Agency
CD	(FBI) Counterintelligence Division
CIMC	(CIA) Counterintelligence Mission Center
CISA	(DHS) Cybersecurity and Infrastructure Security Agency
CITF	Counterintelligence Task Force
CRS	Congressional Research Service
CSE	Center for Security Evaluation
CT	Counterterrorism
DCI	Director of Central Intelligence
DCIF	Defensive Counterintelligence Frame Work
DCSA	(DOD) Defense Counterintelligence and Security Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EO	Executive Order
FBI	Federal Bureau of Investigation
FIE	Foreign Intelligence Entity
FMIC	Foreign Malign Influence Center
FTE	Full Time Employee
FY	Fiscal Year
HHS	Department of Health and Human Services
GAO	Government Accountability Office
IAA	Intelligence Authorization Act
IC	Intelligence Community
ICD	Intelligence Community Directive
ICIG	Intelligence Community Inspector General
INSA	Intelligence and National Security Alliance
IoT	Internet of Things
IP	Intellectual Property
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
MCD	Mission Capabilities Directorate
MID	Mission Integration Directorate
NACIPB	National Counterintelligence Policy Board

NASA	National Aeronautics and Space Agency
NCD	National Counterintelligence Directorate
NCITF	National Counterintelligence Task Force
NCIX	National Counterintelligence Executive
NCPC	National Counterproliferation Center
NCSC	National Counterintelligence and Security Center
NCTC	National Counter-terrorism Center
NGA	National Geospatial-Intelligence Agency
NIH	National Institutes of Health
NIM-CI	National Intelligence Manager for Counterintelligence
NIC	National Intelligence Council
NIP	National Intelligence Program
NITTF	National Insider Threat Task Force
NSA	National Security Agency
NSC	National Security Council
NSPM	National Security Presidential Memoranda
NSF	National Science Foundation
NT-50	Non-Title 50 (non-IC USG entities that do not have 50 U.S.C. authorities)
NTIPA	National Threat Identification and Prioritization Assessment
OCD	Operations Coordination Directorate
ODNI	Office of the Director of National Intelligence
ONCIX	Office of the National Counterintelligence Executive
OPM	Office of Personnel Management
OSINT	Open Source Intelligence
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PDD	Presidential Decision Directive
PLA	People's Liberation Army
PII	Personally Identifiable Information
RDI	Research, Development, and Integration Fund
Review Group	National Counterintelligence Review Group
R&D	Research and Development
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SecEA	Security Executive Agent
SSC	Special Security Center
State	Department of State
S&T	Science and Technology
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USG	United States Government

[redacted]

(U) INTRODUCTION AND METHODOLOGY

(U) The Senate Select Committee on Intelligence (SSCI or the Committee) has long expressed interest in reviewing the United States Government (USG) counterintelligence (CI) enterprise to identify actions needed to enhance its posture, capabilities, and responsibilities in response to contemporary foreign intelligence entity (FIE) threats. The Committee tasked the Audits & Projects Team (Team) with conducting a targeted organizational assessment of the National Counterintelligence and Security Center (NCSC or the Center)—the statutory head of U.S. CI—to understand whether this entity is properly authorized, resourced, and structured to carry out its mission. ***This report seeks to (1) identify the key challenges facing NCSC in carrying out its mission and (2) capture a range of opinions from CI experts on those challenges and potential ways forward.***

[redacted] For purposes of this organizational assessment, the Team focused on NCSC's core CI mission, although the Team also sought to understand any tensions or interdependencies with NCSC's security mission. To conduct this review, the Team met with dozens of current and former CI officials across the Intelligence Community (IC),[1] including the first National Counterintelligence Executive (NCIX) Michelle Van Cleave,[2] former Director of NCSC William Evanina, and Acting Director of NCSC Michael Orlando; NCSC executive leadership, including the head of every NCSC directorate supporting the CI mission; Central Intelligence Agency's (CIA) Counterintelligence Mission Center (CIMC); and the Federal Bureau of Investigation's (FBI) Counterintelligence Division (CD), National Counterintelligence Task Force (NCITF), and local field offices in Washington, D.C., New York, and Houston. The Team also met with officials from the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) and the Department of Defense's (DOD) Defense Counterintelligence and Security Agency (DCSA)—which are not part of the IC. In addition, the Team met with officials from several non-USG entities to understand their perspectives on U.S. CI, including

---

[1] The 18 members of the IC include two independent agencies (the Office of Director of National Intelligence and Central Intelligence Agency); nine Department of Defense elements (Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the intelligence elements of the five Defense services: the Army, Navy, Marine Corps, Air Force, and Space Force); and seven elements of other departments and agencies (Department of Energy's Office of Intelligence and Counter-Intelligence, Department of Homeland Security's Office of Intelligence and Analysis and U.S. Coast Guard Intelligence, Department of Justice's Federal Bureau of Investigation and the Drug Enforcement Agency's Office of National Security Intelligence, Department of State's Bureau of Intelligence and Research, and the Department of the Treasury's Office of Intelligence and Analysis). *What We Do—Members of the IC*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, dni.gov/index.php/what-we-do/members-of-the-ic.

[2] The Counterintelligence Enhancement Act of 2002 codified the establishment of the NCIX to serve as the head of national CI for the USG. The NCIX position was later abolished by the FY 2017 Intelligence Authorization Act, and its responsibilities were assumed by the newly-established Director of NCSC. See Appendix A for more information about the evolution of CI authorities and entities.

[redacted]

officials from three universities, two private sector companies, and one research institution. Finally, the Team met with officials from the United Kingdom's MI5 to understand its CI model and identify best practices.

(U) The Team also reviewed various documents pertaining to CI and NCSC, including CI legislation, executive orders, and IC policies; prior CI-related commission reports to include the 2005 *Commission on the Intelligence Capabilities of the United States Regarding the Weapons of Mass Destruction* (Iraq WMD Commission), the 2009 CI Review Group, and Intelligence and National Security Alliance's (INSA) 2009 *Counterintelligence for the 21st Century*; congressional hearing transcripts and supporting documentation; congressional briefing materials; previous congressional reports and investigations from this Committee and the Senate Permanent Subcommittee on Investigations; the National Intelligence Council's (NIC) *Global Trends 2040: A More Contested World* report; current and previous national security strategies; NCSC's *National Threat Identification and Prioritization Assessment* (NTIPA); the 2020-2022 *National Counterintelligence Strategy* (National CI Strategy) and various country-specific and issue-specific strategies; NCSC's current Strategic Plan; NCSC's *Foreign Intelligence Threat Landscape*; NCSC offensive CI assessments; NCSC white papers and outreach products; NCSC's *2019 Year in Review*; congressional budget justification books for fiscal years (FY) 2021 and 2022 from the Office of the Director of National Intelligence (ODNI); USG press releases; CIA WIRe reports and intelligence memorandums; open source publications on strategic CI, research security, cybersecurity, Chinese and Russian national strategies, and Chinese technology transfer strategies; and reports from the Congressional Research Service (CRS) and Government Accountability Office (GAO).

(U) Finally, the Team assessed the 2020-2022 National CI Strategy against GAO's "desired characteristics" for national strategies to identify gaps and analyzed NCSC's budgetary data for the prior ten years to identify trends. The Team also compared NCSC's funding levels to the National Counterterrorism Center's (NCTC) funding levels to highlight resource discrepancies.

[redacted]

(U) CURRENT THREAT LANDSCAPE

(U) The United States faces a dramatically different threat landscape today than it did just a couple of decades ago. Multiple adversaries target every sector of U.S. society using various traditional and novel tactics and techniques. As the current National CI Strategy notes, FIEs—"to include nation-states, organizations, and individuals—are employing innovative combinations of traditional spying, economic espionage and supply chain and cyber operations to gain access to critical infrastructure and steal sensitive information, research, technology, and industrial secrets."[3] These changes have profound implications for the mission, structure, authorities, and resources of the CI enterprise in general and NCSC in particular.

(U) This section highlights key threats facing the United States today, including current FIE adversaries, targets, tactics, and techniques.

A. (U) Current Adversaries and Threat Actors

(U) During the Cold War, the United States' main adversary was the Soviet Union and other Warsaw Pact countries, as well as Soviet client states such as Cuba. After the terrorist attacks of September 11, 2001, the United States pivoted to focus on al-Qaeda and other extremist jihadist groups around the world.[4] Today, however, the United States faces a wide variety of adversaries to include powerful state rivals with global ambitions, regional adversaries, minor states aligned with U.S. adversaries, ideologically motivated entities, and transnational criminal organizations who may work on behalf of foreign governments. As the world continues to change, new adversaries—some of whom are currently considered allies or friendly nations—may also emerge.

[redacted] New adversaries have emerged for a variety of reasons. The biggest driver has been the rise of China—economically, technologically, militarily, and diplomatically—as well as a revanchist Russia.[5] However, other trends are also driving this change. As the NCSC's 2018 report *The Foreign Intelligence Threat Landscape: Challenges and Opportunities* notes, FIE activities against the United States are becoming democratized by three trends.[6]

[redacted] First, rapidly advancing technology and the increasing availability and affordability of cyber tools has expanded the pool and range of actors who can threaten the United States.[7] Specifically, the internet and other cyber tools have lowered the bar to entry for FIEs and other players looking to

---

[3] **(U)** NAT'L COUNTERINTELLIGENCE & SEC. CTR., NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA, 2020-2022, 2 (2020) [hereinafter THE NATIONAL CI STRATEGY].

[4] **(U)** Hal Brands, *America's War for Global Order is a Marathon*, FOREIGN POLICY (Jan. 25, 2022).

[5] [redacted]

[6] **(U)** *Id.*

[7] **(U)** *Id.* at 1.

[redacted]

[redacted]

collect against the United States, who can now target the United States from the safety of their own countries.[8]

[redacted] Second, a greater emphasis on asymmetric intelligence strategies and capabilities enables FIEs to challenge the United States in the "gray zone" between war and peace. In other words, FIEs are using a combination of cyber operations, media manipulation and other forms of propaganda, covert operations, political subversion, and economic espionage to attain their goals.[9] One former NCSC official explained that adversaries' use of "gray zone" tactics enables them to better hide the hand of their governments and deny responsibility.[10]

[redacted] Finally, the rise of non-state actors such as hackers, public disclosure organizations, transnational criminal organizations, and powerful companies challenges traditional state authority.[11] These entities, enabled by cyber and other technologies, have demonstrated the ability to obtain and share sensitive U.S. information, [redacted]

(U) Moreover, U.S. adversaries no longer need embassies or consulates to target the United States. As Ms. Van Cleave noted:

> **(U)** [F]oreign powers increasingly are running intelligence operations with unprecedented independence from their diplomatic establishments. The number of formal and informal ports of entry to the country, the ease with which people can travel internally, and the relatively benign operational environment of the United States are tailor-made for embedded clandestine collection activities. Thousands of foreign-owned commercial establishments in the United States, the routine interactions of trade and transnational business and finance, and the exchange of hundreds of thousands of students and

---

[8] **(U)** THE NATIONAL CI STRATEGY at 1-3.

[9] **(U)** *Id.* at 2-3.

[10] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).

[11] **(U)** *See* THE NATIONAL CI STRATEGY at I; *Transnational Organized Crime: A Growing Threat to National and International Security*, NAT'L SEC. COUNCIL, obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat; U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-204SP, NATIONAL SECURITY—LONG-RANGE EMERGING THREATS FACING THE UNITED STATES AS IDENTIFIED BY FEDERAL AGENCIES (2018).

[12] [redacted]

[redacted]

academicians, all potentially extend the reach of foreign intelligence into the core structures of our nation's security.[13]

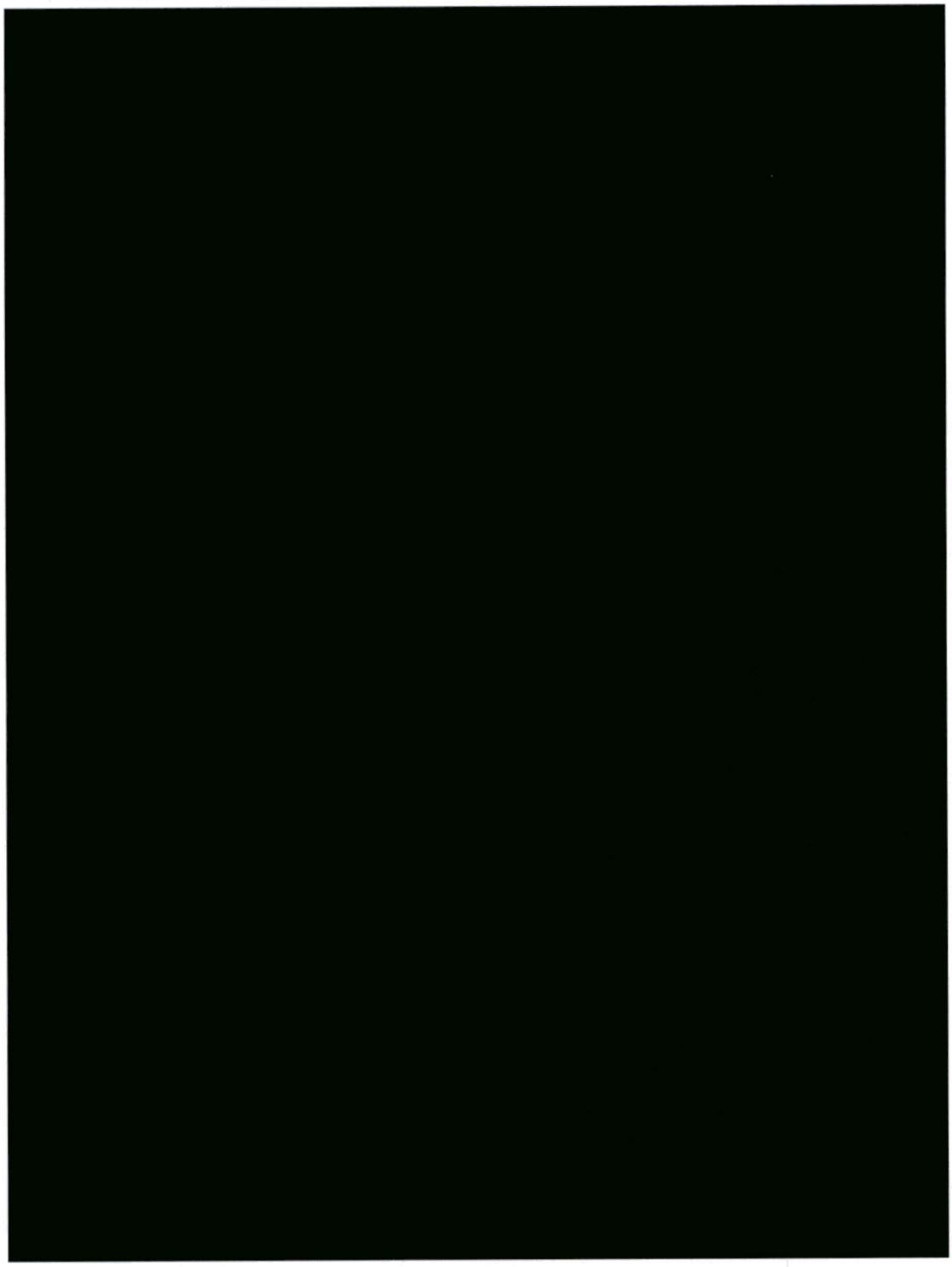
(U) In aggregate, FIEs are working to undermine the security of the United States, erode the United States' economic and technological preeminence, and threaten U.S. social cohesion, critical infrastructure, and basic government functions.[14]

(U) The implications for CI are profound. In the past, CI activities focused primarily on "outwitting structured foreign intelligence services operating out of official platforms whose organizations were basically stable and discoverable, whose vulnerabilities could be identified and exploited, and whose officers showed some commitment to professional tradecraft."[15] Today, a new approach is needed.

[13] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 3 (2007).
[14] **(U)** THE NATIONAL CI STRATEGY at 3, 6, 9.
[15] **(U)** INTELLIGENCE & NATIONAL SECURITY ALLIANCE, COUNTERINTELLIGENCE FOR THE 21ST CENTURY 4 (Sept. 1, 2009) [*hereinafter* 2009 INSA CI REPORT].

[redacted]

[redacted] **Graphic A: Key FIE Threat Actors**[16]



[16] [redacted]

[redacted]

[redacted]

a. (U) Global Adversaries

[redacted] The United States' global adversaries—China and Russia—operate around the world, use all instruments of national power to target the United States, and have a broad range of sophisticated intelligence capabilities[17] to include cyber, supply chain, technical, and human intelligence.[18] [redacted] These two countries pose the biggest, most long-term, and most strategic threats to the United States[20] and are working to shape a new international order more favorable to their interests and governing systems.[21]

[redacted] While the United States was focused on CT efforts over the past two decades, China and Russia continued to target the United States. [redacted]

(U) *China*

(U) Of the two, China poses the greater long-term strategic threat and is a unique challenge to the United States.[24] China is a rising power approaching parity with the United States in gross domestic product as well as in certain aspects of military power.[25] Unlike the prior rivalry with the Soviet Union, which was military and ideological in nature, the rivalry with China exists across the economic, technological, military, diplomatic, and ideological spectrums.[26] Moreover, the United States and China are interdependent in ways that the United States has never been with other adversaries.[27] China seeks to first displace the United States

---

[17] **(U)** THE NATIONAL CI STRATEGY at 2.
[18] **(U)** *See id.*; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 4, 11, 20 (2021).
[19] [redacted]
[20] **(U)** *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 4, 11, 20 (2021); THE NATIONAL CI STRATEGY at 6-11.
[21] **(U)** NAT'L INTELLIGENCE COUNCIL, GLOBAL TRENDS 2040: A MORE CONTESTED WORLD 98 (Mar. 2021).
[22] [redacted]
[23] [redacted]
[24] **(U)** Hal Brands, *America's War for Global Order is a Marathon*, FOREIGN POLICY (Jan. 25, 2022).
[25] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 5 (2022).
[26] **(U)** *Id.*
[27] **(U)** Christopher Wray, Dir., Fed. Bureau of Investigation, Remarks at the Ronald Reagan Presidential Library and Museum: Countering Threats Posed by the Chinese Government Inside the U.S. (Jan. 31, 2022).

[redacted]

[redacted]

as the regional power in East Asia, and then to eventually displace the United States as the global hegemon.[28]

(U) Technology is a major part of this plan; China sees technology and innovation as a key enabler of economic growth and as a pillar of national strength,[29] and aims to become the world leader in science and technology (S&T) by 2050.[30] To achieve this ambition, the Chinese government has issued a variety of national strategic plans. For example, the National Medium and Long-Term Program for Science and Technology Development, issued in 2006, elevated the importance of S&T development to a key Chinese strategic goal.[31] The Made in China 2025 plan, issued in 2015, seeks to make China dominant in global high-tech manufacturing (especially for electric cars, next-generation IT and telecommunications, advanced robotics, artificial intelligence, agricultural engineering, aerospace engineering, synthetic materials, biotechnology and high-end rail infrastructure) using government subsidies, state-owned enterprises, and intellectual property acquisitions to catch up with, and eventually surpass, the United States.[32] The China Standards 2035 Plan, issued in 2021, lays out a strategy for China's government and leading companies to set global standards for emerging technologies, which would enable data associated with these standards to be subject to China's various data localization and access policies[33] and would give China enormous influence over the evolution and interoperability of these technologies.[34]

(U) China's quest to become the world leader in biotech is a good example of the strategic risks that Chinese technology dominance could pose to the United States. Chinese pharmaceutical dominance would create U.S. dependencies and bolster China's influence over the drug supply chain, which would enable China to dictate price or limit supply. China already accounts for 50 percent of global trade in raw pharmaceutical ingredients, [redacted]

(U) It is important to emphasize that China is an authoritarian nation that makes little distinction between its public and private sectors. For example, recent laws have mandated government access to private sector data and required citizens

---

[28] **(U)** 2017 NATIONAL SECURITY STRATEGY.

[29] [redacted]

[30] **(U)** *See* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS 14 (2019).

[31] **(U)** *Id.*

[32] **(U)** James McBride and Andrew Chatzky, *Is 'Made in China 2025' a Threat to Global Trade?* COUNCIL ON FOREIGN RELATIONS (May 13, 2019).

[33] [redacted]

[34] **(U)** Arjun Gargeyas, *China's 'Standards 2035' Project Could Result in a Technological Cold War*, THE DIPLOMAT (Sept. 18, 2021).

[35] [redacted]

[redacted]

[redacted]

and private sector organizations to provide national security authorities, public security authorities, military authorities, and national intelligence efforts with any needed support and assistance.[36] [redacted]

(U) China's 14th Five-Year Plan has further expanded the state's role in the economy and seeks to advance national economic security interests. For example, the Plan calls for using market restrictions and the Belt & Road Initiative to foster Chinese-controlled supply chains; sharpening the use of antitrust, intellectual property, and standards tools to advance industrial policies; focusing on obtaining foreign technology through partnerships in open technology and basic research, the establishment of R&D centers overseas, and talent programs; securing China's supply chains and boosting self-sufficiency in key sectors; using existing global dependences on China as a counterweight pressure and the size of China's market to deepen global dependencies on China; and developing and leveraging control of "core technologies" in sectors such as high speed rail, telecommunications, and new energy.[38]

(U) It is also important to note that the Chinese government makes little distinction between the military and civilian sectors. For example, China's policy of Military-Civil fusion calls for the seamless "fusing" of the military and civilian sectors with resources, technologies, information, and people. The Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations notes that the Military-Civil fusion policy:

> **(U)** [A]llows China to pool its talent and resources from the two sectors to jointly develop technologies, conduct research, and attract talent that mutually reinforces both the military and civilian sectors, enabling China to continue international collaboration with scientists while not disclosing that such collaboration may be for modernizing China's military.[39]

[redacted] However, China is unable to indigenously develop all the technologies it needs within these timeframes.[40] [redacted]

---

[36] **(U)** *Id.* at 9.
[37] **(U)** *Id.* at 10.
[38] **(U)** *Id.* at 6.
[39] **(U)** *See* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS 14 (2019).
[40] **(U)** MICHAEL BROWN & PAVNEET SINGH, DEF. INNOVATION UNIT EXPERIMENTAL, CHINA'S TECHNOLOGY TRANSFER STRATEGY: HOW CHINESE INVESTMENTS IN EMERGING TECHNOLOGY ENABLE A STRATEGIC COMPETITOR TO ACCESS THE CROWN JEWELS OF U.S. INNOVATION (2018).

[redacted]

[redacted]

[redacted] The Chinese government uses **all** available means of collection, including human intelligence collection, technical collection, and cyber espionage, to penetrate the USG, the private sector, and academia.[42] This includes a wide variety of non-intelligence personnel, including businesspeople, students studying at U.S. universities, and researchers working at U.S. labs, to transfer this information back to China.[43]

[redacted]

(U) China is particularly adept at computer hacking. As FBI Director Christopher Wray noted in a January 2022 speech, China has "unleased" massive, sophisticated computer hacking programs that are bigger than those of every other major nation combined. He added that Chinese cyber forces operate from every major city in China and have robust funding and sophisticated tools.[46]

(U) China is also becoming more brazen in violating U.S. citizens' and residents' rights. For instance, the Chinese Embassy has warned U.S. businesses that if they want to do business in China, they need to fight against Chinese government-related bills in Congress. China has also threatened and harassed students at U.S. universities who speak out against Chinese government abuses and punished U.S. businesses whose employees "like" anti-China posts on social media.[47]

(U) Finally, China is increasing its foreign malign influence activities to exploit doubts about U.S. leadership, bolster China's image, and undermine democracy.[48] ODNI, in its 2022 *Annual Threat Assessment of the Intelligence Community*, notes that China is spreading COVID-19 misinformation, including claims that the United States created the disease; intensifying efforts to "mold U.S.

---

41 [redacted]

42 **(U)** *Id.*

43 *See* "Current Tactics and Techniques" section of this report.

44 **(U)** Email from Nat'l Counterintelligence & Sec. Ctr. to Staff, S. Select Comm. on Intelligence (June 8, 2022).

45 [redacted]

46 **(U)** Christopher Wray, Dir., Fed. Bureau of Investigation, Remarks at the Ronald Reagan Presidential Library and Museum: Countering Threats Posed by the Chinese Government Inside the U.S. (Jan. 31, 2022).

47 **(U)** *Id.*

48 **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 11 (Feb. 2022).

[redacted]

[redacted]

public discourse;" and muffling criticism of China's oppression of Uyghurs in Xinjian, among other issues.[49]

(U) Because of China's unique operating model, its novel tactics and techniques, and the fact that it targets strategic sectors of the U.S. economy, FBI Director Wray characterized the Chinese government as the deepest, most diverse, most vexing, most challenging, most comprehensive and most concerning CI threat this country has faced, perhaps in its history.[50] He noted that over 2,000 FBI investigations are currently focused on Chinese government efforts to steal U.S. information and technology, noting that "there is just no country that presents a broader threat to our ideas, our innovation, and our economic security than China."[51] He also emphasized that the harm from Chinese economic espionage isn't just that Chinese companies pull ahead based on stolen technology; it's that they push U.S. companies and workers behind, leading to company failures and job losses.[52] For instance, a Chinese government-owned company stole the propriety source code for controlling wind turbines from a U.S. company in Massachusetts, causing the company to lose over $1 billion in market capitalization and lay off 600 employees.[53] In sum:

> **(U)** Whatever makes an industry tick, they target: source code from software companies, testing data and chemical designs from pharma firms, engineering designs from manufacturers, personal data from hospital, credit bureaus and banks. They've even sent people to sneak into agribusinesses' fields and dig up advanced seeds out of the ground. The common theme is that they steal things companies can't afford to lose.[54]

(U) *Russia*

(U) Russia poses a different threat from China. Russia's population is decreasing and its economy remains statist and largely stagnant.[55] Russia is an energy superpower, wheat producer, and key weapons producer and supplier, but it otherwise has few "national champions" on the world stage.[56]

---

[49] **(U)** *Id.*
[50] **(U)** *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence,* 117th Cong. (2022).
[51] **(U)** Christopher Wray, Dir., Fed. Bureau of Investigation, Remarks at the Ronald Reagan Presidential Library and Museum: Countering Threats Posed by the Chinese Government Inside the U.S. (Jan. 31, 2022).
[52] **(U)** *Id.*
[53] **(U)** *Id.*
[54] **(U)** *Id.*
[55] **(U)** JOANNA PRITCHETT, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, LESS THAN A FULL DECK: RUSSIA'S ECONOMIC INFLUENCE IN THE MEDITERRANEAN (2021).
[56] **(U)** *Id.*

[redacted]

[redacted]

[redacted] Nevertheless, Russia remains a dangerous adversary [redacted] As the NIC's *Global Trends 2040* report notes, Russia is likely to remain a disruptive player for much or all of the next two decades, even as its material capabilities decline relative to other major players. "Russia's advantages, including a sizeable conventional military, weapons of mass destruction, energy and mineral resources, an expansive geography, and a willingness to use force overseas, will enable it to continue playing the role of spoiler and power broker in the post-Soviet space."[58] [redacted] This statement proved prescient; shortly before the Committee finalized this report, Russia invaded Ukraine and has threatened any nation state that would interfere in the conflict.

[redacted] Russia has a longstanding desire to "undermine the U.S.-led liberal democratic order" and works to damage public faith in the U.S. democratic process through both covert operations (such as cyber activities) and overt efforts (such as state-funded media or paid social media users).[60] Russia is also highly adept at information operations, including malign influence operations. In fact, the "weaponization of disarray" is central to Russian statecraft.[61] In 2013, Russia's Chief of General Staff noted that Russia would pursue "new generation warfare" as the "fusion of information, intelligence, and other tools to paralyze an enemy by infiltrating and disrupting its political system."[62] Former Director of National Intelligence (DNI) Dan Coates stated, during this Committee's 2018 Worldwide Threats hearing, that "Russia's approach relies on misdirection and obscuration as it seeks to destabilize and diminish the United States' standing in the world."[63] Specifically, Russia uses malign influence efforts to shape and influence U.S. domestic politics and public opinion.[64]

[redacted]

---

[57] [redacted]

[58] **(U)** NAT'L INTELLIGENCE COUNCIL, GLOBAL TRENDS 2040: A MORE CONTESTED WORLD 95 (Mar. 2021).

[59] [redacted]

[60] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS ii (2017).

[61] **(U)** Hal Brands, *America's War for Global Order is a Marathon*, FOREIGN POLICY (Jan. 25, 2022).

[62] **(U)** *Id.*

[63] **(U)** *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence*, 117th Cong. (2022).

[64] [redacted]

[redacted]

[redacted] For example, in early 2019, the Russian Foreign Intelligence Service breached the computing networks at SolarWinds, a Texas-based network management software company. The company's software, SolarWinds Orion, was widely used in the federal government to monitor network activity and manage network devices on federal systems. This incident allowed the threat actor to breach several federal agencies' networks that used the software.[70] The breach also enabled the Foreign Intelligence Service to compromise critical infrastructure entities and private sector organizations with "high intelligence value." GAO characterized this as "one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and the private sector."[71]

b. (U) Regional Adversaries

(U) Regional adversaries, namely the Islamic Republic of Iran and the Democratic People's Republic of North Korea, also pose significant national security threats.[72] Unlike China and Russia, these actors [redacted][73] However, their growing cyber capabilities make them potentially more disruptive and dangerous than before.

---

[65] [redacted]

[66] **(U)** *Id.*

[67] **(U)** *Id.*

[68] [redacted]

[69] [redacted]

[70] **(U)** U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-22-104746, CYBERSECURITY: FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 16-17 (2022).

[71] **(U)** *Id.* at 3-4.

[72] **(U)** THE NATIONAL CI STRATEGY at 2.

[73] [redacted]

[redacted]

[redacted]

(U) ***Iran***

[redacted] Iran is driven primarily to maintain the stability of the ruling regime and minimize outside influence—namely from the United States—in its internal affairs.[74] Iran is also a major state sponsor of terrorism around the world and has supported various proxies and partner groups to include Hezbollah and Hamas.[75] Iran also aims to develop a nuclear weapon.[76] Iran has growing intelligence and CI capabilities to advance its geopolitical objectives. However, Iranian intelligence organizations conduct intelligence activities mostly in permissive and semi-permissive Middle Eastern countries rather than in the United States.[77]

(U) That being said, Iran's cyber capabilities are advancing, enabling it to conduct espionage, computer network attacks, and information operations around the globe, including against the United States.[78] The Cybersecurity & Infrastructure Security Agency (CISA) notes that various Iranian Advanced Persistent Threat (APT) actors conduct ongoing malicious cyber activities against the United States. For example, Iranian government-sponsored APT groups have exploited Microsoft and Fortinet vulnerabilities, enabling them to gain initial access to various systems in advance of follow-on operations. Iran has also targeted U.S. state websites, including election websites, to obtain voter registration data.[79]

(U) Finally, several Iranian APT actors sought to interfere in the 2020 presidential elections by sowing discord among voters.[80] One Iranian APT group, for example, sent false Facebook messages and emails, purportedly from the Proud Boys, to Republican Senators, Republican members of Congress, and individuals associated with President Trump's campaign claiming that the Democratic Party was planning to "exploit serious security vulnerabilities in state registration websites." The same group also engaged in an online voter intimidation campaign involving the dissemination of threatening messages, also purportedly from the Proud Boys, to tens of thousands of registered Democrats, threatening the recipients with physical injury if they did not vote for President Trump.[81]

---

[74] **(U)** *Id.*
[75] **(U)** U.S. DEP'T OF STATE, *Country Reports on Terrorism 2020*, 3, 199 (Dec. 2021).
[76] **(U)** *See* Eric Brewer, *Iran's Evolving Nuclear Program and Implications for U.S. Policy*, CTR. FOR STRATEGIC & INT'L STUDIES (Oct. 15, 2021).
[77] **(U)** *Id.* at 2.
[78] **(U)** *Iran Cyber Threat Overview and Advisories*, CYBERSECURITY & INFRA. SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., cisa.gov/uscert/iran.
[79] **(U)** *Id.*
[80] **(U)** *Id.*
[81] **(U)** Press Release, U.S. Dep't of Justice, Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election (Nov. 18, 2021).

[redacted]

[redacted]

(U) *North Korea*

(U) North Korea has pursued nuclear weapons for decades to ensure regime survival, achieve reunification of the Korean peninsula, and attain regional great power status.[82] North Korea uses its intelligence services to support these ambitions as well as to collect political, military, economic, and technical information through open source intelligence, human intelligence, cyber activities, and signals intelligence.[83]

(U) As DOD noted in a 2017 report to Congress, North Korea "probably views cyber operations as an appealing, cost-effective, and deniable means by which to collect intelligence and cause disruption against its highly networked adversaries."[84] For example, in 2014 North Korean APT actors launched a cyber-attack against Sony Pictures to prevent it from releasing the movie "The Interview," which portrayed North Korean leader Kim Jong Un in an unfavorable light. The same APT group also launched a cyber-attack against AMC Theaters, which either delayed or cancelled screenings of "The Interview" as a result.[85] Additionally, in 2017, North Korea launched the WannaCry 2.0 global ransomware attack, which crippled networks in more than 150 countries and cost potentially billions of dollars' worth of economic damage.[86]

c. (U) Minor States Aligned with U.S. Adversaries

[redacted] For example, Cuba's intelligence services have highly developed human intelligence tradecraft, as well as a history of effective operations against U.S. targets.[88] [redacted]

---

[82] **(U)** BRUCE W. BENNETT ET AL., RAND CORP., COUNTERING THE RISKS OF NORTH KOREAN NUCLEAR WEAPONS x-xi (2021).

[83] **(U)** OFFICE OF THE SEC'Y OF DEF., MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA: REPORT TO CONGRESS 14 (2017).

[84] **(U)** *Id.* at 13.

[85] **(U)** Christopher Bing & Sarah Lynch, *U.S. charges North Korean hacker in Sony, WannaCry cyberattacks*, REUTERS (Sept. 6, 2018).

[86] **(U)** Press Release, U.S. Dep't of Justice, North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 20218).

[87] **(U)** THE NATIONAL CI STRATEGY at 2; [redacted]

[88] **(U)** William Rosenau & Ralph Espach, *Cuba's Spies Still Punch Above Their Weight*, THE NAT'L INTEREST (Sept. 29, 2013).

[redacted]

[redacted]

d. (U) Ideologically Motivated Entities and Transnational Criminal Organizations

[redacted]

(U) Cyber tools have enabled much of the growth of this group as a threat actor. For example, jihadist groups have successfully radicalized American citizens using social media.[94] As an FBI official noted, "through the internet, terrorists overseas now have access into our local communities to target and recruit our citizens and spread the message of radicalization to violence."[95] Cyber tools have also enabled hackers and hacktivists to harm U.S. critical infrastructure. For example, in 2021 a Russia-based cybercrime group known as DarkSide launched a ransomware attack against Colonial Pipeline[96]—which provides the states along the

---

[89] [redacted]

[90] **(U)** *Id.*

[91] **(U)** *Id.*

[92] [redacted]

[93] [redacted]

[94] **(U)** *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015)

[95] **(U)** BIPARTISAN POLICY CTR., DIGITAL COUNTERTERRORISM: FIGHTING JIHADISTS ONLINE (2018).

[96] **(U)** Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021).

[redacted]

[redacted]

eastern seaboard of the United States with half of their gas, jet fuel, and heating oil supplies—causing fuel shortages and price spikes.[97]

[redacted]

B. (U) Current FIE Targets

(U) FIEs target desired information wherever it may reside. Many FIE efforts previously focused on state secrets held by the IC and the broader national security establishment. Now, however, FIEs target a wide range of information from entities and individuals across nearly every sector of U.S. society. As the *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Iraq WMD Commission) noted back in 2005: "Spies have always existed, but currently our adversaries—and many of our 'friends'—are expanding and intensifying their intelligence activities against U.S. interests worldwide. They target virtually all of our nation's levers of power."[101] Put simply, FIE threats to the United States are now more complex, diverse, and harmful to U.S. interests, and FIEs are targeting a wider set of public and private entities.

(U) The National CI Strategy states that FIEs are "targeting most U.S. government departments and agencies—even those without a national security mission—as well as national laboratories, the financial sector, the U.S. industrial base and other private sector and academic entities."[102] Former Director of NCSC

---

[97] **(U)** Kenneth B. Medlock III, Baker Institute Contributor, *The Colonial Pipeline Outage: An Important Lesson for US Energy Security*, FORBES (May 11, 2021).

[98] [redacted]

[99] [redacted]

[100] **(U)** *Id.* at 13.

[101] **(U)** COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, FINAL REPORT TO THE PRESIDENT OF THE UNITED STATES 488 (2005) [hereinafter 2005 WMD FINAL REPORT].

[102] **(U)** THE NATIONAL CI STRATEGY at 3.

[redacted]

William Evanina further summarized this issue in a written response to the Committee:

> **(U)** In the past, government organizations and personnel were the primary targets of foreign intelligence efforts. Today, foreign intelligence targets (and CI challenges) go well beyond government-controlled national security information and government personnel, and include sectors of society involved in technological, political, legal, social, academic, and commercial pursuits.[103]

(U) ***NT-50s***

(U) FIEs now focus more on targeting NT-50s—that is, non-IC entities that do not have 50 U.S.C. authorities—to acquire sensitive data and a wide range of information, including information on advanced technology and cutting-edge research. Some of these NT-50s include large federal grant-making agencies, such as the National Science Foundation (NSF) and the National Institutes of Health (NIH). China, in particular, relies on non-traditional collectors, such as graduate students and research scientists, to acquire technology, know-how, and expertise through various talent recruitment efforts such as its Thousand Talents Plan (TTP).[104] Some of these TTP recruits even work at NT-50s. For example:

- **(U)** In January 2021, a senior National Aeronautics and Space Administration (NASA) scientist pled guilty to making false statements to the FBI and other federal agencies related to participation in TTP.[105]

- **(U)** In September 2020, a former employee at Los Alamos National Laboratory was sentenced to five years of probation and fined $75,000 for providing a false statement to the Department of Energy (DOE). The individual falsely denied to a CI officer that he had been recruited or applied for a job with TTP.[106]

(U) TTP recruits "strategically important scientists in key innovation programs, laboratories, state corporations, and high-tech parks." The IC believes

---

[103] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020). Evanina continued: "Previous approaches to CI work do not adequately address significant vulnerabilities that exist in other USG organizations and within non-governmental entities, such as academic, business, and other organizations.").

[104] **(U)** *See* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS (2019).

[105] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, OVERSIGHT OF FOREIGN INFLUENCE IN ACADEMIA 13 (2021).

[106] **(U)** *Id.*

[redacted]

"TTP participants to be a pipeline to channel American technologies and intellectual property into the PRC."[107]

(U) NSF, an NT-50 agency frequently targeted by FIEs, is responsible for roughly 27 percent of all federal funds devoted to basic scientific research at U.S. institutions—but NSF did not have a dedicated research security director until 2020.[108] NSF has recognized that "the U.S. science community faces threats to its longstanding position of openness and transparency of research and its results."[109] The NSF Inspector General, one body responsible for investigating potential theft of U.S.-funded research, recently requested more staff and funding because its workload of theft cases by foreign governments has increased 30 percent over the past two years.[110]

(U) NIH is another NT-50 agency that is now frequently targeted by FIEs. NIH is the world's largest biomedical research agency and invests nearly $40 billion annually in medical research through 50,000 grants to more than 300,000 grantees.[111] The NIH Director recently acknowledged that "threats to the integrity of U.S. biomedical research exist. NIH is aware that some foreign entities have mounted systematic programs to influence NIH researchers and peer reviewers and to take advantage of the long tradition of trust, fairness, and excellence of NIH-supported research activities."[112]

(U) *U.S. Private Sector and U.S. Academic Institutions*

[redacted] FIEs have also increased their targeting and exploitation of important non-USG sectors, particularly U.S. higher education institutions and companies that conduct advanced research and design. The United States is a global center for high-technology research, technology, and innovation. As such, "[f]oreign intelligence actors have embedded themselves into U.S. national labs, academic institutions, and industries that form America's national innovation base. They have done this to acquire information and technology that is critical to the growth and vitality of the U.S. economy."[113] As NCSC also notes, FIEs "are actively targeting information, assets, and technologies that are vital to both U.S. national security and our global competitiveness. Increasingly, U.S. companies are in the cross-hairs of these foreign intelligence entities, which are breaching private

---

[107] **(U)** *Id.* at 11.
[108] **(U)** Nat'l Science Foundation, *NSF Creates New Research Security Chief Position* (Mar. 2, 2020).
[109] **(U)** *Id.*
[110] **(U)** Andrew Silver, *U.S. National Science Foundation reveals first details on foreign-influence investigations*, NATURE (July 7, 2020).
[111] **(U)** *See* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS (2019).
[112] **(U)** Francis Collins, Dir., Dep't of Health & Human Servs., *Dear Colleague Letter on Foreign Influence* (Aug. 20, 2018).
[113] **(U)** *Id.*

[redacted]

[redacted]

computer networks, pilfering American business secrets and innovation, and carrying out other illicit activities."[114]

[redacted] According to an ODNI report titled *Oversight of Foreign Influence in Academia*, [redacted]

(U) ODNI compiled a list of recent examples of Department of Justice (DOJ) indictments or other actions taken regarding PRC-related investigations. The examples below illustrate the wide range of private sector entities targeted by FIEs.[120]

- **(U)** May 2021: A rheumatology professor and researcher in Ohio who concealed his participation in Chinese government-funded talent programs was sentenced to 37 months in prison for making false statements to federal authorities as part of an immunology research fraud scheme. The individual admitted he lied on applications in

---

[114] **(U)** *NCSC Awareness Materials*, NAT'L COUNTERINTELLIGENCE & SEC. CTR., OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials.

[115] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, OVERSIGHT OF FOREIGN INFLUENCE IN ACADEMIA 13 (2021).

[116] **(U)** *Id.*

[117] **(U)** *Id.* at 9 (emphasis added).

[118] **(U)** *Id.*

[119] **(U)** *Id.* at 10.

[120] **(U)** *Id.* at 12.

[redacted]

[redacted]

order to use approximately $4.1 million in grants from the NIH to benefit the PRC.[121]

- **(U)** April 2021: A federal jury in Greeneville, Tennessee reached a verdict to convict an individual of conspiracy to commit trade secret theft, conspiracy to commit economic espionage, possession of stolen trade secrets, economic espionage, and wire fraud. The individual stole the trade secrets to set up a new company in the PRC, and received millions of dollars in Chinese government grants to support the new company.[122]
- **(U)** February 2021: A former University of Florida professor and researcher and PRC resident was indicted for fraudulently obtaining $1.75 million in federal grant money from the NIH by concealing support he received from the Chinese government and a company that he founded in the PRC to profit from that research.[123]
- **(U)** February 2021: An individual and co-conspirator were sentenced to prison for conspiring to steal trade secrets from a private company concerning the research, identification, and treatment of a range of pediatric medical conditions. Court documents detail that the individual received benefits from the Chinese government, including the State Administration of Foreign Expert Affairs and the National Natural Science Foundation of China.[124]
- **(U)** January 2021: A professor and researcher at the Massachusetts Institute of Technology (MIT) was charged and arrested in connection with failing to disclose contracts, appointments, and awards from various entities in the PRC to the DOE.[125]

[redacted] ODNI judges that the PRC is not the only adversary targeting professors, universities, and advanced research—other foreign nations continue to seek to licitly and illicitly target sensitive U.S. technology held by private companies and research institutions. [redacted]

[121] **(U)** *Id.*
[122] **(U)** *Id.*
[123] **(U)** *Id.*
[124] **(U)** *Id.*
[125] **(U)** *Id.*
[126] **(U)** *Id.* at 13.

[redacted]

[redacted]

(U) The Iranian government also targets companies and universities. A recent indictment alleges that nine Iranians working on behalf of the Islamic Revolutionary Guard Corps "hacked the computers of 7,998 professors at 320 universities around the world over the last five years."[127] According to the DOJ, the hackers stole 315 terabytes of documents and data, including scientific research, journal, and dissertations. The targets included not only higher education institutions, but also the United Nations, 30 U.S. companies, and five U.S. government agencies.[128] The Iranian hack stole data that costs these institutions about $3.4 billion to "procure and access."[129]

[redacted] ***Targeted Information, Technologies, and Assets.***

(U) Within USG and non-USG entities, NCSC has recently identified several types of information, technologies, and assets that are priority FIE targets, as highlighted in the National CI Strategy. These priority targets are critical to U.S. national power and to U.S. political, military, economic, and technological superiority.[130] These target sets encompass both traditional targets and strategic targets.

[redacted] The National CI Strategy's "Priority Targets" of FIES are listed below:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[127] **(U)** Press Release, U.S. Dep't of Justice, Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps (Mar. 23, 2018).
[128] **(U)** *Id.*
[129] **(U)** *Id.*
[130] **(U)** THE NATIONAL CI STRATEGY at 14.

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted] As noted above, critical infrastructure is one sector that has come under particularly intense public scrutiny as a new target given the implications of potential attacks or disruptions. [redacted]

[redacted] The National CI Strategy further breaks-down U.S. critical infrastructure into sixteen distinct targets: dams, financial services, information technology, commercial facilities, defense industrial base, food and agriculture, nuclear reactors, materials, and waste, communications, energy

---

[131] **(U)** In October 2021, NCSC released additional guidance highlighting which technologies it deemed most important to protect. This guidance prioritized artificial intelligence, biotechnologies, autonomous systems, quantum technologies, and semiconductors, noting that these sectors are "where the stakes are potentially greatest for U.S. economic and national security. These sectors produce technologies that may determine whether America remains the world's leading superpower or is eclipsed by strategic competition in the next few years. NAT'L COUNTERINTELLIGENCE & SEC. CTR., OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PROTECTING CRITICAL AND EMERGING U.S. TECHNOLOGIES FROM FOREIGN THREATS 1 (Oct. 1, 2021).

[132] **(U)** NAT'L COUNTERINTELLIGENCE & SEC. CTR., OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 2019 YEAR IN REVIEW 8 (2019) [hereinafter 2019 YEAR IN REVIEW].

[redacted]

services, government facilities, transportation systems, critical manufacturing, energy, healthcare and public health, and water and wastewater systems.[133]

(U) The food and agriculture sector may not be the first thing that comes to mind when thinking of critical infrastructure. However, the FBI published a case example of an insider threat and non-traditional collector targeting this industry that illustrates how widespread FIE threats truly are. "A Chinese citizen was sentenced to three years in prison for conspiracy to steal trade secrets from U.S. agriculture companies. The Chinese citizen and five others participated in the theft of inbred corn seeds from fields the companies owned, with the aim of shipping them to a Chinese company."[134] These technologically advanced seeds were "genetically modified to be strong and enhance desirable traits such as resistance to pests and drought."[135] The U.S. company estimated that the theft of the seeds would have resulted in the loss of five to eight years of research and at least $30 million.[136]

C. (U) Current FIE Tactics

(U) In the past, U.S. adversaries had relatively limited options for stealing information, influencing U.S. officials, or inflaming social and political tensions.[137] Traditional intelligence collection and influence efforts required foreign nations to, for example, send spies to U.S. soil, co-opt an insider, target U.S. officials when overseas, bug offices, or intercept U.S. communications from collection facilities around the world.[138] Despite this, FIEs still managed to inflict major damage on U.S. national security, including compromising U.S. military plans and capabilities, exposing diplomatic secrets, overcoming U.S. technological advantages in certain areas, and costing the USG and the U.S. economy billions of dollars.[139] For instance, this Committee found in a 1986 CI review that hostile intelligence services had acquired sensitive technological data in the United States and elsewhere, which significantly reduced the time it took for the Soviets to develop new weapons systems and field countermeasures to U.S. systems.[140]

[redacted] Today, however, U.S. adversaries have access to a much wider variety of tools to accomplish their goals, and the damage is far greater. In addition to traditional espionage—which certainly continues—FIEs can now exploit non-

---

[133] **(U)** THE NATIONAL CI STRATEGY at 6.
[134] **(U)** Fed. Bureau of Investigation, *Case Example: Insider Threat and Non-Traditional Collection* (2019).
[135] **(U)** *Id.*
[136] **(U)** *Id.*
[137] **(U)** Allies and friendly nations also collect against the United States and seek to influence U.S. officials or public opinion. However, this report focuses primarily on adversary collection and influence efforts given the potential for extreme damage to U.S. national security.
[138] **(U)** S. SELECT COMM. ON INTELLIGENCE, 116TH CONG. REP. ON RUSSIAN ACTIVE MEASURES CAMPAIGN AND INTERFERENCE IN THE 2016 U.S. ELECTION VOL. 2: RUSSIA USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS (2020).
[139] **(U)** *Id.* at 12.
[140] **(U)** *Id.* at 16.

[redacted]

traditional human, cyber, advanced technical, and open source intelligence operations to collect against U.S. plans and policies, sensitive technology, personally identifiable information (PII), and intellectual property, as well as to influence U.S. decision-making and public opinion on a scale previously unimaginable.[141]

(U) As INSA put it succinctly in its report *Counterintelligence for the 21st Century*: "Today, neither the strategists nor the tacticians are dealing with 'our fathers' CI."[142] These new tactics reduce the risk of action, make attribution more difficult, and provide more avenues for success. The NTIPA notes that:

> [redacted]Hostile FIEs are emphasizing intelligence strategies and capabilities to challenge the U.S. and its allies in the "gray zone" between war and peace. Nation states are using a combination of cyber operations, media manipulation, covert operations, political subversion, and economic and psychological coercion to divide the West, erode U.S. global influence, and sow tensions and instability in key regions. Nation states are conducting these activities to enhance their ability to coerce and deter the U.S. with plausible deniability in a crisis.[143]

(U) One NCSC official confirmed that the "United States' adversaries are employing their intelligence services and proxies in unique ways, and are able to better hide the hand of their governments." He noted that this "gray zone warfare" enables our adversaries to have a greater degree of freedom to operate within the United States using means such as cyber, economic tools, and social media.[144]

(U) The CI landscape continues to evolve, and our adversaries are becoming more and more creative about how to acquire the information they need, influence elected officials, or sway public opinion in ways that meet their strategic goals.[145] Many of these mechanisms are not illegal, which further complicates U.S. strategies to disrupt FIE efforts.[146]

(U) As the National CI Strategy points out: "[T]he escalating volume and sophistication of intelligence operations against U.S. interests and innovative blending of collection methods and tools [redacted]

---

[141] [redacted].

[142] **(U)** 2009 INSA CI REPORT at 4.

[143] [redacted]

[144] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).

[145] **(U)** *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence,* 117th Cong. (2022).

[146] **(U)** MICHAEL BROWN & PAVNEET SINGH, DEF. INNOVATION UNIT EXPERIMENTAL, CHINA'S TECHNOLOGY TRANSFER STRATEGY: HOW CHINESE INVESTMENTS IN EMERGING TECHNOLOGY ENABLE A STRATEGIC COMPETITOR TO ACCESS THE CROWN JEWELS OF U.S. INNOVATION (2018).

[redacted]

[redacted]

[redacted] ***Congress has not substantially and comprehensively updated CI laws since 2002***—before U.S. adversaries began using many of the tactics and techniques identified below, such as cyber hacking and social media influence campaigns.

a. (U) Cyber and Social Media

[redacted]) Cyber tools have dramatically impacted the CI landscape. Although not all malicious cyber activities pose a CI threat, cyber lowers the "bar to entry" for FIEs looking to penetrate the United States because it is cheaper than most other intelligence collection resources; often poses less risk of attribution; and increases the chance of success, especially given the vulnerability of many U.S. networks.[148]

[redacted]

(U) As explained in Appendix A, the DNI established the National Counterintelligence Review Group (the Review Group) in 2009 to review the role, mission, capabilities, and resources of all national CI activities within the IC. One of the Review Group's key findings was that:

[redacted]

[147] **(U)** THE NATIONAL CI STRATEGY at 2. (emphasis added).

[148] **(U)** U.S. CYBERSPACE SOLARIUM COMM'N, REPORT (2020).

[149] [redacted]

[150] **(U)** *Id.* at 2-3.

[151] [redacted]

[redacted]

[redacted]

(U) The NTIPA also identified four ways in which cyber is facilitating FIE activities:

1. **(U)** *Cyber as a Communications and Data Channel*

[redacted]

(U) The Committee previously investigated Russia's use of social media during the 2016 presidential election campaign and found that:

> Russian operatives associated with the St. Petersburg-based Internet Research Agency used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States. . . . Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real-world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election.[155]

(U) The use of social media cyber tools to influence U.S. public opinion can be extremely effective and challenging to counteract. As then-Chairman of this Committee Richard Burr noted during the Committee's 2019 Worldwide Threats hearing:

> **(U)** When this country's democracy was attacked in 2016, it wasn't with a bomb, or a missile or a plane. It was with social media accounts that any 13-year old can establish for free. The enemies of this country aren't going to take us on a straight-up fight, because they know they'd lose. They're going to keep finding new ways of attacking us, ways that

---

[152] **(U)** *Id.*

[153] **(U)** *Id.*

[154] **(U)** THE NATIONAL CI STRATEGY at 9.

[155] **(U)** S. SELECT COMM. ON INTELLIGENCE, 116TH CONG. REP. ON RUSSIAN ACTIVE MEASURES CAMPAIGN AND INTERFERENCE IN THE 2016 U.S. ELECTION VOL. 2: RUSSIA USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS (2020).

[redacted]

[redacted]

> exploit the openness of our society, and slip through the seams of a national security architecture designed for the Cold War.[156]

(U) The FBI and the National Security Agency (NSA) assess that FIEs will continue to use social media platforms as a vehicle for weaponizing disinformation and spreading foreign influence in the United States. The FBI further assesses that the Russians continuously adapt their model and that other countries are taking a "keen interest" in their approach.[157] Then Vice-Chairman Warner observed during the Committee's 2019 Worldwide Threats Hearing that this problem is poised to get exponentially worse as "deep fake" technology matures.[158] Then-Director of National Intelligence Dan Coates noted during the same hearing that foreign actors would view the 2020 U.S. elections as an opportunity to advance their interests, and that the IC expected these actors to refine their capabilities and add new tactics as they learned from each other's experiences and efforts in previous elections.[159]

2. **(U)** *Cyber as an Exploitation Tool*

[redacted] During the House Permanent Select Committee on Intelligence's 2021 World Wide Threats hearing, NSA Director General Nakasone noted the sophistication of U.S. adversaries' cyber exploitation capabilities:

> **(U)** Our adversaries' intrusions are not spear-phishing or guessing a password. They are intrusions based upon supply chain or zero-day vulnerabilities, a vulnerability that a provider doesn't even know

---

[156] **(U)** *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence,* 117th Cong. (2022).
[157] **(U)** *Id.*
[158] **(U)** *Id.*
[159] **(U)** *Id.*
[160] **(S//NF)** NAT'L COUNTERINTELLIGENCE & SEC. CTR., NATIONAL THREAT IDENTIFICATION AND PRIORITIZATION ASSESSMENT: AN INCREASINGLY COMPLEX INTELLIGENCE THREAT LANDSCAPE 3 (2018).
[161] **(U)** *Id.*
[162] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Supply Chain Directorate (June 1, 2021)

[redacted]

[redacted]

about.[163] So what we are seeing is our adversaries understanding the limitations of our ability to monitor what is going on within the United States . . . what our adversaries are doing inside the United States is looking for our infrastructure, our internet service providers, our cloud providers, and being able to very quickly set up a capability, and then utilizing that as a jumping off point to create intrusions.[164]

(U) In March 2021, for example, Microsoft reported that an actor associated with the Chinese government exploited zero-day vulnerabilities in several versions of its Microsoft Exchange Server used by the federal government. These vulnerabilities enabled the actor to gain access to federal systems, which in turn allowed for persistent malicious operations even after the vulnerabilities were patched.[165] Microsoft estimates that the email, address books, and calendars of approximately 400,000 customers—including federal government agencies—were compromised.[166]

(U) According to the U.S.-China Economic and Security Review Commission, cyber espionage has also enabled foreign adversaries, particularly China, to gain access to a wide range of commercially valuable U.S. business information—including intellectual property (IP), trade secrets, technical data, negotiating positions, and sensitive and proprietary internal communications—which are then provided to and utilized by select Chinese firms.[167]

3. **(U)** *Cyber as an Operational Environment*

[redacted] In 2018, Ms. Van Cleave told the House Committee on Science, Space, and Technology that "U.S. academic institutions, with their great concentration of

---

[163] **(U)** U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-22-104746, CYBERSECURITY: FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 5 (2022) (Zero-day vulnerabilities are security vulnerabilities unknown to the public before they are announced. By writing an exploit for the previously unknown vulnerability, an attacker creates a potent threat since the public does not know to defend against it).

[164] **(U)** *Worldwide Threats: Hearing Before the H. Permanent Select Comm. on Intelligence,* 117th Cong. (2022).

[165] **(U)** U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-22-104746, CYBERSECURITY: FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 1 (2022).

[166] **(U)** *Id.* at 4.

[167] **(U)** SEAN O'CONNOR, U.S.–CHINA ECON. & SEC. REVIEW COMM'N, HOW CHINESE COMPANIES FACILITATE TECHNOLOGY TRANSFER FROM THE UNITED STATES 8 (2019).

[168] [redacted]

[169] **(U)** *Id.*

[redacted]

[redacted]

creative talent, cutting edge research endeavors, and open engagement with the world of ideas, are an especially attractive environment for foreign collectors targeting America's R&D wealth."[170] She noted that the advent of social media has "opened the door even wider."[171]

(U) In 2019, for instance, a variety of media outlets reported that China was using LinkedIn to recruit witting and unwitting assets abroad. Mr. Evanina told the *New York Times* that "instead of dispatching spies to the U.S. to recruit a single target, it's more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles."[172]

4. **(U)** *Cyber as a Sensor*

[redacted] In August 2016, an ODNI-commissioned study on how IoT could revolutionize intelligence collection and analysis noted that IoT may enable a "golden age of surveillance."[174] The report also noted that IoT could present a greater opportunity for our adversaries to collect against the United States than the reverse:

> **(U)** Consider, for example, the popularity of wearable technologies—such as smart watches and fitness bands—in the United States. Nearly one in five Americans owns a wearable device, including President Obama. The accumulation of data from these devices and the correlation of this information with other behavioral and environmental data create significant counterintelligence and protection challenges.[175]

(U) In December 2019, the *New York Times*'s Privacy Project obtained a dataset with more than 50 billion location pings from the phones of more than 12 million people in the United States. Using this information, it took only minutes for

---

[170] **(U)** *Scholars or Spies: Foreign Plots Targeting America's Research and Development: Joint Hearing Before the Subcomm. On Oversight and Subcomm. on Research & Tech of the H. Comm. on Sci., Space, & Tech.*, 115th Cong. (2018) (statement of Michelle Van Cleave).

[171] **(U)** *Id.*

[172] **(U)** Edward Wong, *How China Uses LinkedIn to Recruit Spies Abroad*, N.Y. TIMES (Aug. 27, 2019).

[173] [redacted]

[174] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, GOING BRIGHT: HOW THE INTERNET OF THINGS COULD REVOLUTIONIZE INTELLIGENCE COLLECTION AND ANALYSIS (2016).

[175] **(U)** *Id.*

[redacted]

[redacted]

reporters to de-anonymize location data and track the whereabouts of President Trump.[176]

b. (U) Economic Espionage

(U) Foreign adversaries have conducted economic espionage against the United States for many decades. However, the nature, scope, and scale of economic espionage has expanded dramatically over the past few decades.[177]

(U) In 2010, Mr. Bryant, in a Statement for the Record for this Committee, said that

[redacted]

(U) FIEs exploit the U.S. culture of openness and collaboration, as well as policy and legal gaps to acquire information.[179] As Ms. Van Cleave told the House Committee on Science, Space, and Technology in 2018:

> **(U)** American R&D—the engine for new ideas and products and capabilities and wealth—is systematically targeted by foreign collectors to fuel their business and industry and military programs at our expense. By far the vast majority of foreign acquisition of U.S. technology is open and lawful, as are the transactions of individuals and businesses involved in international commerce, as well as the free exchange of ideas in scientific and academic forums. Even so, while the United States leads the world in R&D spending, with annual investments of some $510 billion, we are losing most if not more of that dollar amount every year through systemic theft. It continues to be what General Keith Alexander, then-Director of the National Security Agency, memorably called the "greatest transfer of wealth in history."[180]

---

[176] **(U)** Stuart Thompson & Charlie Warzel, *How to Track President Trump*, N.Y. TIMES (Dec. 20, 2019).

[177] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE (Nov. 3, 2011).

[178] **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 7).

[179] **(U)** THE NATIONAL CI STRATEGY at 2.

[180] **(U)** *Scholars or Spies: Foreign Plots Targeting America's Research and Development: Joint Hearing Before the Subcomm. On Oversight and Subcomm. on Research & Tech of the H. Comm. on Sci., Space, & Tech.*, 115th Cong. (2018) (statement of Michelle Van Cleave).

[redacted]

[redacted]

[redacted] U.S. adversaries have undertaken massive efforts to steal or otherwise acquire U.S. intellectual property, research, and know-how on key technologies that the United States is developing.[181] [redacted]

(U) China, however, is the "600 pound gorilla in the room" and has launched a full-scale campaign to develop or acquire technologies it deems critical to its national interests, including AI, quantum computing, integrated circuits, genetics and biotechnology, high end new materials, new energy and intelligent vehicles, smart manufacturing, aerospace engines and gas turbines, deep space, deep earth, deep sea, and polar exploration, among others.[183] FBI Director Wray, in his testimony before this Committee during the 2018 Worldwide Threats Hearing, noted that the FBI has economic espionage investigations in virtually all of its 56 field offices, and almost all of them trace back to China.[184]

(U) In addition to the cyber espionage activities noted previously,[185] China conducts a variety of other activities to acquire desired U.S. technology or information (see graphic B). For instance, China makes extensive use of technology transfer programs. "Chinese companies—in many cases with the backing of the Chinese government—use a variety of methods to acquire valuable technology, IP, and know-how from U.S. firms. Some of these tactics are legal, while others involve coercive or covert means." [186]

---

[181] [redacted]

[182] **(U)** *Id.*

[183] [redacted]

[184] **(U)** *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence,* 117th Cong. (2022).

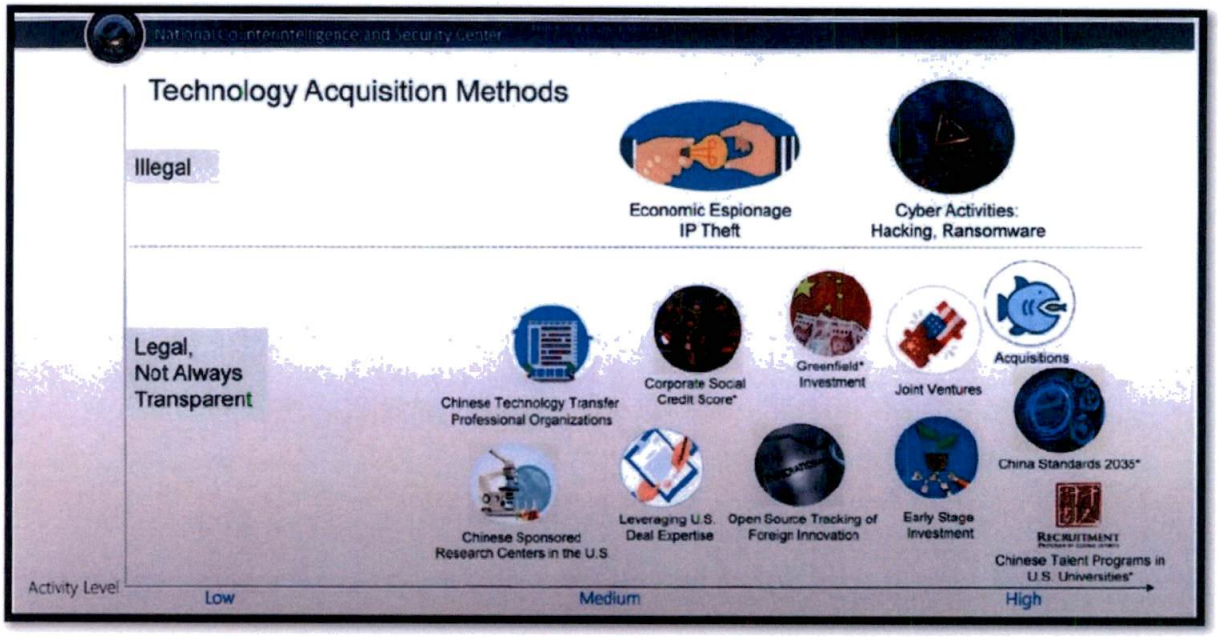
[185] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE (Nov. 3, 2011).

[186] **(U)** SEAN O'CONNOR, U.S.–CHINA ECON. & SEC. REVIEW COMM'N, HOW CHINESE COMPANIES FACILITATE TECHNOLOGY TRANSFER FROM THE UNITED STATES 3 (2019).

[redacted]

[redacted]

(U) Graphic B: Illegal and Legal Technology Acquisition Methods[187]



(U) The Chinese government has prioritized technology transfer as a matter of policy and provides direct and indirect support to companies engaging in these anticompetitive activities. Chinese acquisition attempts frequently target advanced technologies that are still in the early stages of development but could provide dual military and civilian capabilities in the future.[188] Taken together, these technology transfer methods have led to the loss of billions of dollars in U.S. R&D, IP, and technology products. According to the Commission on Theft of American Intellectual Property, the annual cost of IP theft (globally, not just from China) to the U.S. economy could be as much as $600 billion. However, China is the world's "principal IP infringer."[189]

(U) In May 2019, the U.S.-China Economic and Security Review Commission outlined five key ways, in addition to cyber espionage, that China has been facilitating this technology transfer:[190]

1. **(U)** *Foreign Direct Investment.* The Chinese government directs Chinese firms to invest in and acquire U.S. companies and assets to obtain cutting-edge technologies and IP in strategic industries.[191]

2. **(U)** *Venture Capital Investments.* Chinese venture capital investments in the U.S. have increased in recent years, in particular targeting U.S.

---

[187] **(U)** *Id.*
[188] **(U)** *Id.*
[189] **(U)** *Id.*
[190] **(U)** *Id.*
[191] **(U)** *Id.*

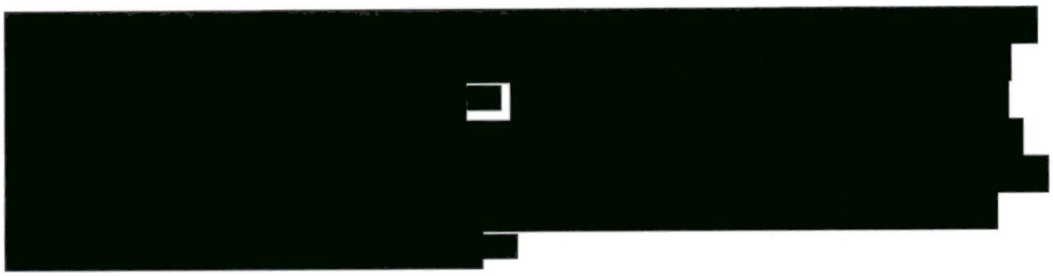
[redacted]

[redacted]

technology startups. Chinese venture capital investment in the United States may allow Chinese firms to access valuable U.S. technology and IP, including technologies with potential dual-use applications.[192]

3. **(U)** *Joint Ventures.* In many industries, foreign firms must enter into joint ventures to invest or operate in China. Joint ventures are often the source of Chinese companies' most technologically advanced and innovative procedures and products, acquired through technology transfer from their foreign joint venture partner.[193]

   (U) A March 2018 study from the National Bureau of Economic Research found that joint ventures often generate Chinese companies' most technologically advanced and innovative procedures and products, acquired through technology transfer from their foreign joint venture partner.[194]



4. **(U)** *Licensing Agreements.* Licensing approval processes in China are often unclear and arduous, requiring companies to disclose sensitive information typically not required in other markets. For instance, commercial firms are required to provide detailed product and process information to Chinese government agencies at the local and central levels. Chinese government agencies often do not have to agree to destroy company information submitted in the licensing process, so companies' IP can be shared or exposed even after the license is adjudicated. These licensing processes allow Chinese regulators to discriminate against foreign investors while keeping protectionist practices from being documented and used against China at the World Trade Organization.[197]

5. **(U)** *Talent Acquisitions.* The Chinese government maintains government programs aimed at recruiting overseas Chinese and foreign experts and

---

[192] **(U)** *Id.*
[193] **(U)** *Id.*
[194] **(U)** *Id.* at 7.
[195] [redacted]
[196] **(U)** *Id.*
[197] **(U)** SEAN O'CONNOR, U.S.–CHINA ECON. & SEC. REVIEW COMM'N, HOW CHINESE COMPANIES FACILITATE TECHNOLOGY TRANSFER FROM THE UNITED STATES 8 (2019).

[redacted]

[redacted]

entrepreneurs in strategic sectors to teach and work in China. Beijing utilizes intergovernmental and academic partnerships and collaborations in the United States, establishes Chinese research facilities in the United States, and sends experts abroad to gain access to cutting-edge research and equipment without disclosing the organization's or individual's connections to the Chinese government.[198] The Senate Permanent Subcommittee on Investigations noted in 2018 that the Chinese government had more than 200 such talent recruitment plans.[199]

(U) Project 111, for example, was launched by the Chinese government in 2006 to recruit 1,000 foreign experts in strategic sectors from the world's top 100 universities and research institutes. By 2009, it had recruited 39 Nobel Prize winners and 591 academics. Similarly, the TTP was launched in December 2008, and by mid-2014 had brought more than 4,000 foreigners to China's scientific laboratories, companies, and research centers.[200] Recent publicity and USG scrutiny of the TTP has pushed it underground, but the Permanent Subcommittee on Investigations assessed that China will continue with its talent recruitment plans.[201]

(U) Supply Chain Attacks

(U) The National CI Strategy identifies supply chain attacks as a complex and growing threat to strategically important U.S. economic sectors and to U.S. critical infrastructure.[202] A supply chain attack is when an actor compromises the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the USG, the Defense Industrial Base, or the broader private sector.[203]

(U) The United States is increasingly reliant on foreign-owned or controlled hardware, software, and services.[204] Current DNI Avril Haines noted that the IC is particularly worried about supply chain vulnerabilities in microelectronics and semiconductors, as well as in battery technology, new energy technologies, and weapons systems.[205]

---

[198] **(U)** *Id.* at 9.
[199] **(U)** *See* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS (2019).
[200] **(U)** SEAN O'CONNOR, U.S.–CHINA ECON. & SEC. REVIEW COMM'N, HOW CHINESE COMPANIES FACILITATE TECHNOLOGY TRANSFER FROM THE UNITED STATES 9 (2019).
[201] **(U)** *See* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS 3 (2019).
[202] **(U)** THE NATIONAL CI STRATEGY at 12.
[203] **(U)** *Id.*
[204] **(U)** *Id.*
[205] **(U)** *Worldwide Threats: Hearing Before the H. Permanent Select Comm. on Intelligence,* 117th Cong. (2022).

[redacted]

[redacted]

(U) There are many ways that a foreign adversary could compromise the integrity of U.S. supply chains. As Mr. Bryant noted in testimony before this Committee:

[redacted]

(U) Software supply chains have unique vulnerabilities, and the exploitation of information and communications technology products through the supply chain is an emerging threat.[207] A software supply chain attack—such as the previously-mentioned SolarWinds attack—occurs when a cyber-threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or systems.[208] An adversary can compromise software not only during initial development, but also during implementation, maintenance and updates, and disposal.[209] A successful compromise enables an actor to degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.[210]

(U) Other Tactics

(U) U.S. adversaries are continually identifying new tactics and techniques to collect against the United States and influence U.S. policymakers and the public. This trend is likely to intensify as the pace of innovation accelerates. Mr. Evanina characterized such tactics and techniques as "the new CI," noting that they all

---

[206] **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 8).

[207] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-22-104746, CYBERSECURITY: FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 4 (2022).

[208] **(U)** *Id.* at 1.

[209] **(U)** *Id.* at 5.

[210] **(U)** *Id.*

[redacted]

[redacted]

operate in the "gray zone" of state conflict.[211] Below are just a few additional avenues that adversaries have pursued or may pursue to illustrate the creative ways adversaries may target the United States.

- **(U)** *Open Source Intelligence (OSINT).* OSINT—or intelligence produced from publicly available information—has been revolutionized over the past two decades given the rise of the internet and social media. Americans freely share enormous amount of information online that benefit FIEs. For example, many individuals voluntarily share photographs, personal sentiments, and information about personal and professional networks in ways that were never possible before.[212] Universities also widely disseminate the results of their research.[213] While the United States uses OSINT to enable or augment classified reporting, other adversaries—especially China—view it as the "intelligence of first resort."[214]

- [redacted] *Emerging and Dual Use Technologies.* Emerging technologies with intelligence applications such as artificial intelligence, quantum computing, nanotechnology, advanced materials, advanced sensors, surveillance systems, unmanned systems, improved encryption, and robotics will likely enable adversaries to more precisely target U.S. citizens for recruitment and compromise, enhance monitoring and surveillance capabilities, and covertly access and exfiltrate sensitive U.S. communications.[215] Some of these technologies are commercially available at an affordable cost, which has enabled a wider range of threat actors to acquire sophisticated intelligence capabilities that previously were the domain of well-resourced states.[216]

- **(U)** *Biotechnology.* China and other adversaries could use various biotechnologies to target the United States. For example, adversaries could use U.S. genetic data to target DOD and IC personnel, including by combining U.S. genetic data with other PII, making cover or alias more difficult. Further, the Chinese government's collection of U.S. PII and health information could fill gaps from other large datasets—such as the

---

[211] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).
[212] **(U)** Heather Williams & Ilana Blum, *Defining Second Generation open Source Intelligence for the Defense Enterprise*, RAND CORP. 1 (2018).
[213] **(U)** William Hannas & Huey-Meei Chang, *China's STI Operations*, GEORGETOWN, CTR. OF SEC. & EMERGING TECH. (Jan. 2021).
[214] **(U)** *Id.* at iii.
[215] **(U)** THE NATIONAL CI STRATEGY at 3
[216] **(U)** *Id.*

[redacted]

[redacted]

Office of Personnel Management (OPM) data breach—to identify and develop more comprehensive profiles on high-value targets.[217]

- **(U)** *Confucius Institutes.* The Chinese government funds Confucius Institutes on U.S. colleges and universities and hires Chinese teachers to teach language and culture classes to student and non-student community members. A Senate Permanent Subcommittee on Investigations report, however, found that the funding for these institutes comes with "strings" that can compromise academic freedom. For instance, professors funded by a Confucius Institute are not allowed to discuss sensitive topics. Moreover, these institutes seeks to manipulate U.S. perceptions of China in a more favorable light.[218]
- [redacted]
- [redacted]

[217] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-22-104746, CYBERSECURITY: FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 10-12 (2022).

[218] **(U)** *See* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON CHINA'S IMPACT ON THE U.S. EDUCATION SYSTEM (2019).

[219] [redacted]

[220] **(U)** Interview with Fed. Bureau of Investigation, New York City Field Office (Dec. 6, 2021).

[221] **(U)** Press Release, U.S. Dep't of Justice, Five Individuals Charged Variously with Stalking, Harassing, and Spying on U.S. Residents on Behalf of the PRC Secret Police (Mar. 16, 2022).

[redacted]

[redacted]

D. (U) Overview of the National Counterintelligence and Security Center

(U) NCSC was established in 2014 as a component of ODNI. The NCSC integrated into one organization the functions of the Office of the NCIX and multiple other entities with CI responsibilities. NCSC draws it responsibilities and authorities from a series of laws, Presidential directives, and executive orders, which are described in more detail below and in Appendix A.

(U) According to ODNI, NCSC "leads and supports the U.S. Government's counterintelligence and security activities critical to protecting our nation, provides CI outreach to U.S. private sector entities at risk of foreign intelligence penetration, and issues public warnings regarding intelligence threats to the United States."[222]

(U) Graphic C: NCSC Organizational Chart (As of 16 August 2021)

[redacted]

[redacted]

[222] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CONG. BUDGET JUSTIFICATION BOOK, FISCAL YEAR 2022, 6 [*hereinafter* ODNI FY2022 CBJB].

[redacted]

[redacted]

a. NCSC's Eight Directorates

(U) NCSC currently maintains eight directorates[223] to carry out its responsibilities. This section provides a brief description of the roles and responsibilities of each directorate, as well as an overview of current staffing levels (see Graphic D).

(U) Graphic D: NCSC Staffing Levels, Per Directorate (As of 23 November 2021) [redacted]

[redacted]

i. (U) Operations Coordination Directorate (OCD)

[redacted] OCD coordinates [redacted]

[223] (U) Graphic D references a "Front Office" to handle administrative duties, but that is not considered a directorate.

[224] [redacted]

[redacted]

[redacted]

[redacted]

ii. (U) Supply Chain & Cyber Directorate (SCD)

[redacted] SCD is responsible for identifying efforts to reduce the risks to key U.S. supply chains as identified in the National CI Strategy. [redacted]

[redacted]

iii. (U) Insider Threat Directorate (ITD)

[redacted] ITD is responsible for co-leading the National Insider Threat Task Force (NITTF) with the FBI and for managing the Unauthorized Disclosure Program. The NITTF, created after the 2010 WikiLeaks disclosures, helps the USG build insider threat programs that "deter, detect and mitigate actions by insiders who may represent a threat to national security."[231] The NITTF develops guidance, provides assistance, assesses progress, and analyzes new and continuing insider threat challenges. As part of the NITTF, NCSC's Insider Threat Directorate publishes the *National Insider Threat Policy and Minimum Standards*; *Guide to Accompany the National Insider Threat Policy and Minimum Standards*; *Protect*

---

[225] **(U)** NAT'L COUNTERINTELLIGENCE & SEC. CTR., NCSC STRATEGIC PLAN 2018-2022, 13 (Dec. 21. 2017) [hereinafter NCSC STRATEGIC PLAN 2018-2022].

[226] **(U)** *Id.*

[227] [redacted]

[228] **(U)** *Id.*

[229] **(U)** ODNI FY2022 CBJB.

[230] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Organization: About* (Mar. 11, 2020).

[231] [redacted]

[redacted]

[redacted]

Your Organization from the Inside Out: Government Best Practices; and other annual reports.[232]

[redacted] The NITTF has published an Annual Report each year since 2015.[233] These reports detail department/agency progress in meeting the insider threat program requirements set forth in the National Insider Threat Policy & Minimum Standards and EO 13587.[234] The reports also depict program status and annual progress across the IC, DOD, and NT-50s.[235]

[redacted] The ITD is also responsible for coordinating the production of certain national CI strategic assessments, including damage assessments from unauthorized disclosures and lessons learned from those activities. "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 [IC] partners to improve CI and security programs and develop mitigation measures."[236]

iv. (U) Mission Integration Directorate (MID)

[redacted] MID is responsible for NCSC's federal partner outreach, national CI and security policy development, strategic resource advocacy, and CI and security workforce talent development and recognition.[237] [redacted]

[redacted] examines CI budgets across the IC and conducts "Mission Reviews" of the IC to ensure that each agency is aligned with the National CI Strategy [redacted] sends each IC agency an annual survey [redacted], which it supplements with data obtained through Personnel and Insider Threat Reviews. After reviewing all the data it receives, [redacted] conducts in-person visits with the IC entities to discuss. These conversations [redacted] how to guide its advocacy efforts to increase federal spending on CI initiatives, as well as understand the extent to which prior recommendations have been implemented.[239]

---

[232] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CONG. BUDGET JUSTIFICATION BOOK, FISCAL YEAR 2021 [*hereinafter* ODNI FY2021 CBJB].

[233] [redacted]

[234] **(U)** *Id.*

[235] **(U)** *Id.*

[236] **(U)** NCSC STRATEGIC PLAN 2018-2022 at 13.

[237] **(U)** *Id.*

[238] **(U)** *Id.*

[239] **(U)** *Id.* at 16.

[redacted]

[redacted]

[redacted] produces a report after each review and sends it to the agency head. These reports generally include sections on the following topics: [redacted] also examines CI data and spending figures (through an annual data call) to get a "state of CI spending" across the IC.[241]

[redacted] helps bridge the gap between the NCSC and the broader USG. [redacted] conducts two main functions: liaison and vulnerability assessments. Liaisons serve as the lead integrators for NCSC engagement and as the focal point for queries. Vulnerability assessment staff conduct multi-disciplinary assessments, provide recommendations, and leverage expertise against partner issues and concerns. [redacted] supports approximately 140 NT-50 and DOD federal partner agencies and departments to counter foreign intelligence threats.[242]

[redacted] also sends self-assessment questionnaires [redacted] to NT-50 agencies. The questionnaire is similar to [redacted] Mission Reviews of IC agencies, but is less detailed and is also voluntary. [redacted] then meets with the agencies that complete [redacted] to gain "a better understanding of the specific needs of [the NT-50 agencies'] CI programs with periodic updates and revisits by request to further advance CI programs."[244]

v. (U) Special Security Directorate (SSD)

[redacted] SSD serves as the Executive Staff for all DNI Sec/EA functions and responsibilities. SSD works on extensive security clearance reform measures to "address longstanding problems with the timeliness and effectiveness of the process for granting national security clearances."[245] This includes, but is not limited to, establishing a "continuous evaluation" program and improving reciprocity across the USG in recognizing clearances from agency-to-agency.[246]

---

[240] **(U)** *Id.*
[241] **(U)** *Id.*
[242] **(U)** *Id.*
[243] **(U)** *Id.*
[244] **(U)** *Id.*
[245] **(U)** OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Organization: About* (Mar. 11, 2020).
[246] **(U)** *Id.*

[redacted]

[redacted]

vi. (U) National Counterintelligence Directorate (NCD)

[redacted] NCSC is responsible for national CI and security policy development, compliance, and oversight. The Director of NCSC serves as National Intelligence Manager for CI (NIM-CI) for the IC. NCD is responsible for producing, in consultation with USG departments and agencies, the NTIPA and the National CI Strategy on behalf of the Director.[247]

[redacted] NCD oversees and coordinates the production of national CI strategic analyses, including damage assessments from espionage and unauthorized disclosures, and lessons learned from these activities. This directorate also coordinates national CI collection and targeting, and develops priorities for CI investigations and operations.[248] Specifically, this directorate coordinates and publishes a range of foundational and strategic planning documents focusing on CI, including *Counterintelligence Production Guidance*, *Strategic Counterintelligence Priorities*, *Collection Emphasis Messages,* and *CI Collection Assessments.*[249]

[redacted] NCD also chairs the National Counterintelligence Policy Board (NACIPB),[250] which serves as the principal mechanism for developing national policies and setting priorities to guide the conduct of CI activities across the USG.[251]

vii. (U) Center for Security Evaluation (CSE)

[redacted] CSE provides Congressionally-mandated support to the Department of State (State) on "physical and technical security for U.S. diplomatic facilities, which includes identifying and countering foreign technical penetrations, technical surveillance, or technical collection efforts."[252] In addition, CSE leads IC-wide efforts to:

1. [redacted]
2. [redacted]

---

[247] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (May 12, 2020).
[248] **(U)** NCSC STRATEGIC PLAN 2018-2022 at 13.
[249] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).
[250] **(U)** NCSC STRATEGIC PLAN 2018-2022 at 11.
[251] **(U)** *Id.*
[252] **(U)** NCSC STRATEGIC PLAN 2018-2022 at 21.

[redacted]

[redacted]

[redacted]

viii. Mission Capabilities Directorate (MCD)

[redacted] During the course of the Committee's review, NCSC created the MCD "to combine the Center's mission IT systems and capabilities into a single directorate, improving upon the current construct where these entities are scattered across several NCSC directorates and the IT group."[254] Today, NCSC manages or will manage [redacted] different databases [redacted] the USG's Continuous Evaluation System.[255]

[253] **(U)** *Id.*
[254] **(U)** ODNI FY2022 CBJB at 81.
[255] **(U)** NCSC Database Summary Document.

[redacted]

[redacted]

(U) FINDINGS

(U) As previously illustrated, the FIE threat landscape facing the country today is wide-ranging and sophisticated. Yet ***NCSC, as the USG lead for CI, lacks a clear mission as well as sufficient and well-defined authorities and resources to effectively confront this landscape.*** Moreover, ***NCSC's placement within ODNI may hinder its ability to scale and respond to threats in an agile manner***. Despite these challenges, ***there is no consensus among CI officials on a way forward for NCSC.***

A. (U) MISSION

(U) Under current law, the mission of the Director of NCSC is to "serve as the head of national counterintelligence for the United States Government."[256] However, the Committee found that the scope of this mission is not clear to the Committee, to the broader IC, or even to some NCSC officials. First, it is unclear whether certain FIE threats and USG activities fall within the definition of CI. Second, NCSC is unsure which entities comprise the CI enterprise—that is, the collection of entities with CI responsibilities—that it is tasked with leading. Third, there is no consensus as to whether NCSC should focus on traditional internally-focused CI activities, the strategic CI mission, or both. [redacted] Finally, officials disagree on the optimal relationship between CI and security and over what specific role NCSC should play with regards to security.

1. (U) It is Unclear Whether Certain FIE Threats and USG Activities to Counter Them Fall within the Definition of CI

(U) The FIE threat landscape has changed dramatically over the past few decades, yet officials disagree over whether certain current FIE threats and USG activities to counter them fall within the definition of CI. Consequentially, officials disagree over what role NCSC, as lead of national CI, should play in mitigating evolving threats and overseeing new USG activities to counter them.

(U) The National Security Act of 1947, as amended in 1992, defines CI as "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[257] Executive Order 12333 promulgated a similar definition of CI, but included additional USG activities to counter FIE threats: "Counterintelligence means 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

---

[256] **(U)** 50 U.S.C. § 3382(b).

[257] **(U)** National Security Act of 1947, 50 U.S.C. § 3001 (3.5)(a).

[redacted]

[redacted]

organizations or activities."[258] Given the evolving foreign threat landscape and USG efforts to counter these threats, ***uncertainty surrounds two aspects of these definitions***.

(U) First, there is no consensus as to whether certain emergent threats, particularly foreign malign influence and cyber threats, fit within the definition of CI.[259] Ms. Van Cleave told the Committee that NCSC and other CI entities currently address such threats under the ambiguous "other intelligence activities" clause of the CI definition.[260]

(U) NCSC believes that countering foreign malign influence falls within the definition of CI. To this end, NCSC included "Defending American Democracy from Foreign Influence" as one of the key National CI Strategy pillars.[261] Former NCSC Director Evanina told the Committee that NCSC is the "only entity postured to counter foreign malign influence," and he previously sought to establish a Foreign Influence Directorate within NCSC—but ODNI rejected this request for a variety of reasons.[262] Acting Director Michael Orlando also agreed that foreign malign influence should be considered part of the CI mission.[263]

(U) However, actions taken by ODNI officials suggest a different view of foreign malign influence and its relationship to CI. For example, ODNI's FY 2022 Congressional Justification Budget Book [redacted][264] Moreover, ODNI is establishing a separate Foreign Malign Influence Center (FMIC) not under NCSC control, due, in part, to a statutory requirement from Congress in the FY 2020 IAA.[265]

(U) Similar questions exist regarding where cyber fits into the CI mission. As noted in the Current Threat Landscape section of this report, cyber is now one of the primary means by which FIEs target the USG, academia, the private sector,

---

[258] **(U)** Exec. Order No. 12333 3.5 (as amended in 2008) (emphasis added).

[259] **(U)** 50 U.S.C. § 3059 (e)(2). Foreign malign influence is defined as: "Any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means—(a) the political, military, economic, or other policies or activities of the United States Government or state or local governments, including any election within the United States; or (b) the public opinion within the United States."

[260] **(U)** Email from Michelle Van Cleave, Former ONCIX Director, to Staff, S. Select Comm. on Intelligence (Jan. 31, 2022).

[261] **(U)** THE NATIONAL CI STRATEGY at 4.

[262] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).

[263] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[264] **(U)** ODNI FY2021 CBJB at 15.

[265] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[redacted]

[redacted]

and public opinion.[266] Mr. Evanina told the Committee that ***cyber is now the main CI modality***, yet cyber and CI are treated as distinct disciplines.[267] [redacted] Other officials agreed that there should be greater integration between the cyber and CI communities.[270]

(U) One FBI official told the Committee that "philosophically" national security cyber (as opposed to criminal cyber)[271] is just a modality and thus should fit squarely within the realm of CI.[272] Yet, one NCSC official explained that national security cyber has historically been treated as distinct from CI because cyber is seen as a "technical skill" whereas CI is traditionally viewed as a "soft skill."[273] An FBI official similarly noted that, because most CI practitioners lack cyber skills, cyber has been treated as a separate discipline. He characterized this as a "workforce issue."[274]

[redacted] Other USG agencies, however, play a more prominent role in carrying out the national security cyber mission. Most notably, the newly established CISA, which is not part of the IC, "leads the national effort to understand, manage, and reduce risk to [U.S.] cyber and physical infrastructure."[276] CISA is the operational lead for federal cybersecurity, as well as the national coordinator for critical infrastructure security and resilience.[277] The May 2021 EO on "Improving the Nation's Cybersecurity" clearly envisions CISA retaining the lead on the cyber mission, with the FBI, NSA,

---

[266] **(U)** *See* "Current Tactics" section of this report.
[267] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).
[268] **(U)** *Id.*
[269] **(U)** Email from the Nat'l Counterintelligence & Sec. Ctr. to Staff, S. Select Comm. on Intelligence (June 8, 2022).
[270] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022); Interview with Fed. Bureau of Investigation, Washington Field Office (Dec. 2, 2021); Interview with Nat'l Counterintelligence & Sec. Ctr., Supply Chain Directorate (June 1, 2021).
[271] **(U)** Interview with Fed. Bureau of Investigation, Counterintelligence Div. (Sept. 20, 2021). FBI officials defined national security cyber as cyber activity conducted by a foreign state or non-state adversary in support of political or strategic objectives, whereas criminal cyber is cyber activity conducted by non-state entities in support of criminal enterprises.
[272] **(U)** Interview with Fed. Bureau of Investigation, Washington Field Office (Dec. 2, 2021).
[273] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Supply Chain Directorate (June 1, 2021).
[274] **(U)** Interview with Fed. Bureau of Investigation, Washington Field Office (Dec. 2, 2021).
[275] **(U)** *See* NCSC overview section of this report.
[276] **U)** *About CISA,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC.
[277] **(U)** *Id.*

[redacted]

[redacted]

and others in a supporting role; NCSC was not mentioned.[278] DCSA's CI mission also plays a key role in identifying, assessing, and disrupting FIE threats, to include cyber threats, to the nation's defense industrial base.[279] Furthermore, the new National Cyber Director for Federal Cybersecurity at the White House serves as "a principal advisor to the president on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders" and will look to "bring 'unity of effort' to U.S. cybersecurity efforts."[280]

[redacted] Treating national security cyber as distinct from CI may hinder an appropriate USG response. For instance, in 2020 the IC discovered a Russian cyberattack on SolarWinds, which enabled Russia to gain access to multiple USG networks.[281] The Committee viewed this cyberattack [redacted][282] Yet despite the CI nexus, NCSC—the lead for national CI—was not included in the Unified Coordination Group established by the White House to address this cyber intrusion.[283]

(U) Second, in addition to the threats themselves, there is also uncertainty about whether certain new USG activities to counter FIE threats fit within the definition of CI. As discussed more below, various NT-50s have established "defensive CI programs" that include activities such as FIE target identification, foreign travel briefings, and receipt and review of certain CI products.[284] This report refers to these activities as "CI awareness" activities, as they fall outside customary CI activities [redacted] Officials disagree about whether such activities truly fit within the definition of CI—that is, whether they can be considered activities conducted to identify, deceive, exploit, disrupt, or protect against FIE threats—or whether these should be considered ***security*** activities. This distinction is important because it determines the range of activities that a non-IC entity would be responsible for conducting in response to FIE threats.

(U) As this Committee noted as far back as 1986, security is complementary to, but distinct from, CI:

---

[278] **(U)** *Executive Order on Improving the Nation's Cybersecurity*, WHITE HOUSE (May 12, 2021).
[279] **(U)** *White Paper For Submission to Senator Angus King*, Defense Counterintelligence & Security Agency.
[280] Justin Doubleday, *Agencies Entering Execution Phase of Biden's Cyber Executive Order*, FED. NEWS NETWORK (Nov. 19, 2021).
[281] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-22-104746, CYBERSECURITY: FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 16-17 (2022).
[282] [redacted] Letter from Chairman Warner & Vice Chairman Rubio, S. Select Comm. on Intelligence [redacted] (Dec. 11, 2020).
[283] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021).
[284] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).

[redacted]

[redacted]

> **(U)** The Committee believes it is important to distinguish between counterintelligence efforts and security programs, while ensuring that both are a part of a national policy framework that takes account of all aspects of the threat. ***The best way to explain the difference is to say that counterintelligence measures deal directly with the foreign intelligence service activities, while security programs are indirect defensive actions that minimize vulnerabilities.***[285]

(U) In practice, however, these lines often blur and create confusion. As one OUSD(I&S) official noted, "There is not a lot of 'pure CI' out there; most defensive CI activities actually fall under the definition of 'security.'"[286] On the other hand, several NCSC officials told the Committee that "CI awareness" activities should be considered part of the CI mission because they include actives that extend beyond security.[287] That is, "CI awareness" activities involve more than just minimizing vulnerabilities to include ***identifying*** FIE activities targeting a given agency. Mr. Evanina felt strongly that the definition of CI must broaden to include such "CI awareness" activities, as CI is no longer just counter-espionage; "We have moved way beyond that."[288]

(U) Congress has not updated the statutory definition of CI since 1992, which continues to differ from the Executive Branch definition of CI. Without additional clarity on the universe of FIE threats that fall under this definition and the types of activities that counter them, NCSC and other USG entities may not know which FIE activities they are responsible for addressing or with which USG entities they should be coordinating to combat such threats.

[redacted] Various CI professionals indicated that it is time for Congress to provide a clearer definition of CI that reflects today's threat landscape. For example, a former NCSC official told the Committee that the definition of CI must be updated to include new unconventional and non-traditional threats.[289] Mr. Evanina, in testimony before this Committee, said that "we have to re-look at the lexicon of what we say counterintelligence is."[290] [redacted]

---

[285] **(U)** S. SELECT COMM. ON INTELLIGENCE, MEETING THE ESPIONAGE CHALLENGE: A REVIEW OF UNITED STATES COUNTERINTELLIGENCE AND SECURITY PROGRAMS 522 (1986) (emphasis added) [hereinafter 1986 SSCI REPORT].

[286] **(U)** Interview with U.S. Dep't of Def., Under Sec'y of Def. for Intelligence & Security, Counterintelligence & Law Enforcement (Aug. 3, 2021). Note: Joint Publication 3-10 defines security as measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. As an example of overlap between CI and security, [redacted] *See* email from Dep't of Def. to Staff, S. Select Comm. on Intelligence (May 27, 2022).

[287] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Feb 4, 2022).

[288] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).

[289] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Former Deputy Director (Oct. 8, 2020).

[290] [redacted] *Closed Oversight Hearing on Counterintelligence with NCSC, FBI, and CIA Before the S. Select Comm. on Intelligence* (Dec. 1, 2020).

[redacted]

[redacted]

[redacted]

2. (U) The Boundaries of the CI Enterprise are Unclear

(U) NCSC is the statutory head of the CI enterprise, but NCSC officials do not have a complete list of CI entities, and several current and former NCSC officials disagree over which types of entities fall within the enterprise. [292] Specifically, there is disagreement amongst current and former officials over whether NT-50s and non-USG entities (such as universities and private sector companies) that conduct "CI awareness" activities should be considered part of the CI enterprise.

(U) NCSC officials generally view the CI enterprise as being comprised of or supporting three broad "stakeholder" categories: (1) the IC, (2) NT-50s, and (3) non-USG entities, such as academia and private industry.[293] However, due in large part to lack of clarity within the USG regarding the scope of CI, there is no consensus on whether NT-50s and non-USG entities should be considered (1) members of the CI enterprise or (2) "customers" or beneficiaries of the CI enterprise, which would have only security responsibilities. As a result, it is unclear what CI responsibilities, if any, NT-50s and non-USG entities are expected to have, or what NCSC's relationship to these entities should be.

[291] [redacted]

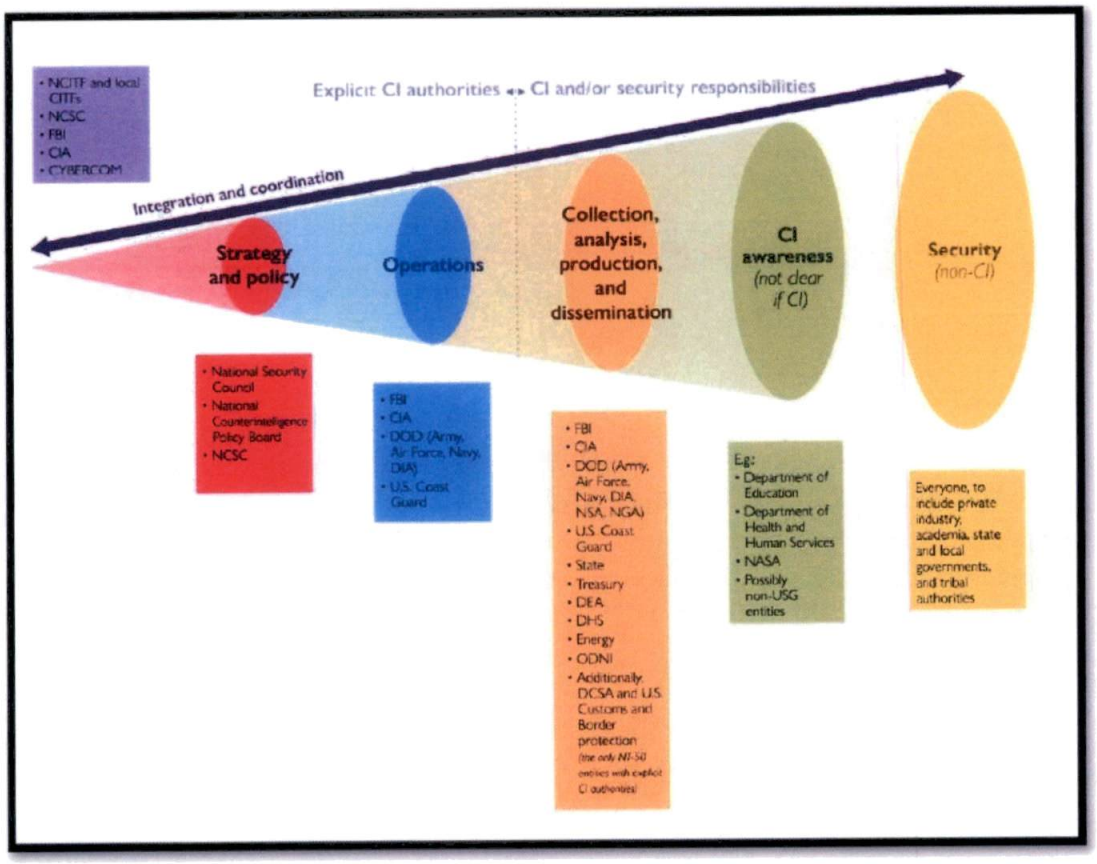
[292] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Feb 4, 2022).

[293] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

[redacted]

[redacted]

Graphic E: Conceptual Depiction of CI and Security Activities and Associated Entities[294]



(U) *The IC*

(U) There is consensus that the IC is and should remain part of the CI enterprise. As explained in Appendix A, the CI mission arose within individual IC entities as a way to defend their operations[295] and has historically been primarily within the purview of the IC. [296] Today, CI responsibilities remain widely dispersed across the members of the IC.

---

[294] **(U)** [redacted] the entities listed in the "CI Awareness' Category are purely illustrative.

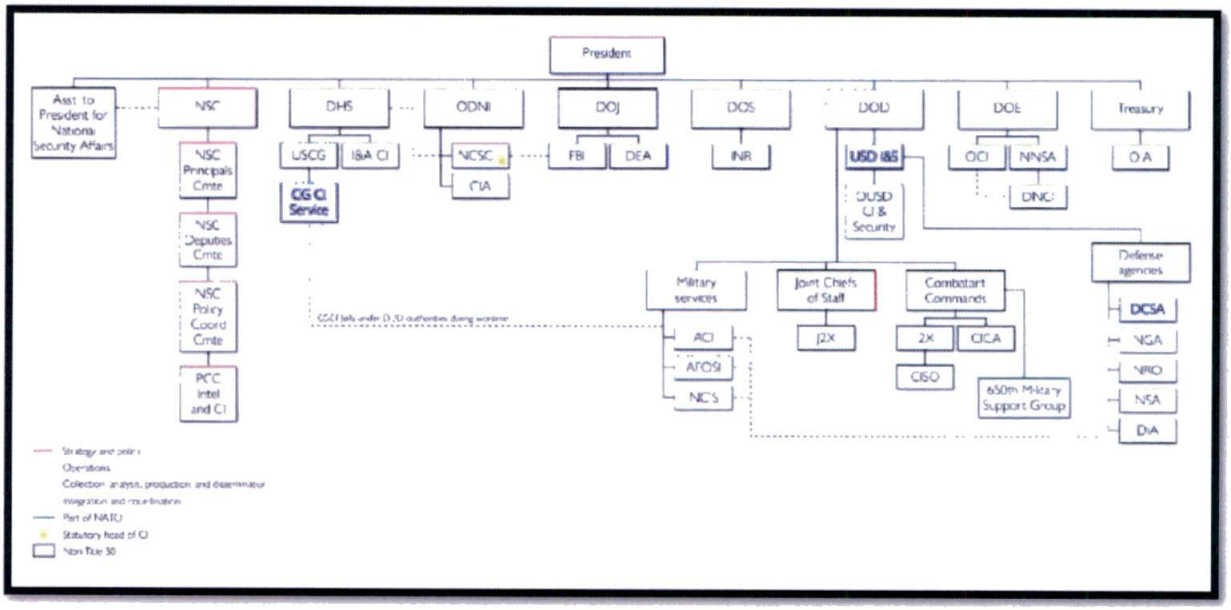
[295] **(U)** *See* "Evolution of CI" section of this report.

[296] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

[redacted]

[redacted]

Graphic F: Entities with Official CI Authorities



(U) EO 12333 details the specific responsibilities of the IC, including CI responsibilities. All IC entities are broadly required to protect the security of intelligence related activities, information, installations, property, and employees by appropriate means.[297] In support of this mission, EO 12333 authorizes the CIA; Defense Intelligence Agency (DIA); NSA; National Geospatial-Intelligence Agency (NGA); the intelligence components of the Army, Navy, Air Force, Marine Corps, and Coast Guard; DOD; the FBI; the intelligence components of Department of State, Department of Treasury, Drug Enforcement Agency, the Department of Homeland Security (DHS), and DOE; and ODNI to collect, analyze, produce, and disseminate CI information.[298] EO 12333 also directs a subset of these entities—namely CIA, DIA, DOD, FBI, and the intelligence components of the Army, Navy, Air Force, Marine Corps, and the Coast Guard—to "conduct" CI activities.[299]

(U) As a result, some CI officials believe that CI should remain solely an IC function. For example, Ms. Van Cleave believes that CI is inherently an IC responsibility, although she recognizes that NT-50s, universities, state and local governments, and academia have an important role to play in ***security***.[300] That is,

---

[297] **(U)** Exec. Order No. 12333 1.4(f).

[298] **(U)** *Id.* at 1.7.

[299] **(U)** *Id.*

[300] **(U)** Exec. Order No. 12,333, 46 Fed. Reg. 235 (1981). Security is related but conceptually distinct from CI. Executive Order 12333 notes that CI does not include "security activities" such as personnel, physical, document or communications security programs. According to a 2011 DOD CI Glossary, security is a "condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences." As Robert Hanssen, former FBI CI agent turned Soviet spy noted, "counterintelligence investigates the enemy … It is not

[redacted]

she argues that the IC should provide threat awareness and protect non-IC entities through offensive CI activities, while NT-50s, universities, state and local governments, and academia should take steps to protect their operations and reduce their vulnerabilities through security measures.[301] Mr. Orlando agreed that only the IC should be considered part of the CI enterprise, arguing that NT-50s, academia, the private sector, and others should be considered "customers" or beneficiaries of CI.[302]

(U) *NT-50 Agencies and Non-USG Entities*

(U) Given the evolving threat landscape, other CI and IC professionals have called for expanding the CI enterprise to include NT-50s and even academia, private sector industries, and state and local governments, because these entities are often on the front lines of the fight against FIEs. For instance, the 2009 Review Group concluded that the "almost total absence of CI" throughout the rest of the USG and the private sector poses a critical national security concern, giving adversaries "almost carte blanche to operate against the United States" in vulnerable areas.[303] In 2010, Mr. Bryant, in testimony before this Committee, said that the effectiveness of CI depends on a unified national effort that complements and enhances the internal efforts of the CI offices found in IC agencies. He added that CI "must become the practice of the entire USG—not just the IC—as well as those elements of the public and private sectors charged with holding and protecting sensitive information and leading-edge technologies."[304] Furthermore, INSA noted that there must be closer partnerships between the government, industry, and academia, and emphasized that strategic challenges expand the U.S. national security environment "well beyond the traditional purview of U.S. intelligence."[305] Specifically, INSA called for the integration of the capabilities of the federal, state, and local governments and the private sector in a secure collaborative national network.[306] Mr. Evanina told this Committee in 2020 that non-IC USG agencies and non-USG entities "must establish robust CI capabilities because they too are targeted by malign foreign actors and insiders."[307]

---

security work. Security protects. It does not attack." Email from Michelle Van Cleave, Former ONCIX Director to Staff, S. Select Comm. on Intelligence (Jan. 31, 2022).

[301] **(U)** Email from Michelle Van Cleave, Former ONCIX Director to Staff, S. Select Comm. on Intelligence (Jan. 31, 2022).

[302] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[303] **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 9).

[304] **(U)** *Id.*

[305] **(U)** 2009 INSA CI REPORT at 7.

[306] **(U)** *Id.*

[307] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S.

[redacted]

[redacted] Two NT-50 entities—the Defense Counterintelligence and Security Agency (DCSA) and the Office of Intelligence within United States Customs and Border Protection (CBP)—already have statutory CI authorities.[308] Several other NT-50 agencies have voluntary "CI awareness" programs. [redacted] Yet, other than DCSA and CBP, no NT-50 agencies are ***required*** to have CI programs, despite the fact that they are a major target of FIEs.[310] [redacted]

(U) Several officials believe that NT-50s should be considered part of the CI enterprise and should be mandated to have CI programs.[312] One NCSC official, for instance, noted that she believes the 2002 Counterintelligence Enhancement Act explicitly broadened the CI enterprise to include non-IC entities such as NT-50s.[313] DCSA officials similarly believed that CI should be considered a whole-of-government responsibility.[314]

(U) As noted above, however, Mr. Orlando told the Committee that NT-50s should not be considered part of the CI enterprise because they should not be collecting or analyzing intelligence or conducting operations. He noted, however, that these entities could nevertheless have defensive CI programs (i.e., conduct "CI awareness" activities) to provide threat awareness and defensive briefings, among other things.[315] [redacted]

Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

[308] **(U)** DCSA's CI authorities come from 10 U.S.C. § 1564 and 50 U.S.C. 3161. CBP's CI authorities come from 6 U.S.C. § 211(h)(3)(B).

[309] [redacted]

[310] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

[311] [redacted]

[312] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Feb 4, 2022); Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022); Interview with Fed. Bureau of Investigation, Nat'l Counterintelligence Task Force. (Feb. 3, 2022); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).

[313] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Feb 4, 2022).

[314] **(U)** Interview with U.S. Dep't of Def., Def. Counterintelligence & Sec. Agency (Oct. 13, 2021).

[315] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[redacted]

[redacted]

(U) Even less clear is whether non-USG entities such as academia, private sector companies, and state and local governments should be considered members, partners, or beneficiaries of the CI enterprise. As explained previously, these sectors are extensively targeted by FIEs—after all, it is often U.S. universities, laboratories and other research institutions, and private sector companies that make scientific discoveries and develop the latest technologies[317]—but it's not clear what national security role the organizations and individuals in these sectors are expected to play.

(U) As noted previously, various CI commissions have called for including non-USG entities in the CI enterprise. Mr. Evanina also noted in his written responses to this Committee that "non-USG entities must establish robust CI capabilities because they too are targeted by malign foreign actors and insiders. Very few of these departments, agencies, and non-USG organizations are appropriately positioned to systematically detect, analyze, and preempt attempts to steal information or conduct interference activities."[318] Several academic and private sector officials also told the Committee that they believe non-USG entities should be considered part of the CI enterprise. For instance, several officials at a financial company told the Committee that the USG needs to do more to bring business into the "CI architecture" and that CI should be viewed as a "whole-of-society" mission.[319] An official at a research institution likewise told the Committee that academia is part of the CI solution and should be complementary to the USG.[320]

[redacted] In contrast, other officials believe that CI is an "inherently governmental" function and should be the exclusive purview of the USG for several reasons.[321] First, the interests of non-USG entities do not always align with national security interests—and the USG does not require non-USG entities to prioritize national security over other concerns, such as profit or advancements in scientific research. [redacted]

---

316 **(U)** Interview with Fed. Bureau of Investigation, Nat'l Counterintelligence Task Force. (Feb. 3, 2022).

317 **(U)** *See* "Current Targets" section of this report.

318 **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

319 **(U)** Interview with U.S. Investment Firm 1 (Dec. 7, 2021).

320 **(U)** Interview with U.S. Research Institutions (Jan. 11, 2022).

321 **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Oct. 6, 2020).

[redacted]

[redacted]

[redacted] Several officials at an energy company similarly told the Committee that they do not consider themselves part of the CI enterprise because their company is an international business with a profit motive and not part of the U.S. national security apparatus.[323] An official at one university said it should be the USG's responsibility to vet foreign students and researchers; "If the State Department gives them a visa, why should I think they're a threat?"[324] Other officials have noted that companies and academia see CI and security as being too costly and that they lack incentives to fully align with national security concerns.[325] [redacted] He also noted that universities get full tuition from foreign students, which is important for their bottom line but may conflict with national security interests.[327]

[redacted]

---

[322] [redacted]

[323] **(U)** Interview with U.S. Energy Company 1 (Jan. 10, 2022).

[324] **(U)** Interview with U.S. University 2 (Dec. 9, 2021).

[325] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020); Interview with U.S. Energy Company 1 (Jan. 10, 2022).

[326] [redacted]

[327] **(U)** *Id.*

[328] **(U)** Interview with Former Nat'l Counterintelligence & Sec. Ctr. Official (Oct. 9, 2020).

[329] **(U)** Interview with U.S. Research Institutions (Jan. 11, 2022).

[330] [redacted]

[331] **(U)** Interview with U.S. Research Institutions (Jan. 11, 2022). One university that the Committee met with, however, has established a dedicated research security office that relies on open source

[redacted]

[redacted]

(U) Officials who oppose officially incorporating non-USG entities into the CI enterprise nevertheless argue for a closer partnership with the USG or for a greater USG role in protecting the information held by non-USG entities. For instance, an official at a research institution told the Committee that academia should not be considered part of the CI enterprise, but that there should be better lines of communication with the USG.[332] One CI official said that the IC should be doing more to protect sensitive information held by non-USG entities from FIE threats, noting that academia, in particular, may not have sufficient expertise to protect its research from exploitation by sophisticated cyber adversaries.[333] An official from a university likewise told the Committee that academia cannot be expected to "protect our country as a hobby."[334] Regarding private companies, an industry official added that they should not be expected to develop their own "missile defense."[335] An official from another company said that companies are inherently defensive and cannot go on the offense against nation state adversaries; "government must play that role."[336]

(U) In the end, there is no consensus on who should be considered a "member" of the CI enterprise versus a "partner" or "beneficiary" of the CI enterprise. Yet, this is not simply a semantic exercise; such clarity is important to understand what NCSC's relationship with those entities should be as the lead for national CI, as well as to understand what responsibilities those entities would be expected to have in support of the CI mission.

3. (U) Traditional CI and Strategic CI are Different Missions—but it is Unclear Whether NCSC Should Focus on Traditional CI, Strategic CI, or Both

(U) NCSC lacks clarity over whether it should focus on traditional CI, strategic CI, or both. NCSC has prioritized the strategic CI mission, but lacks a clear mandate (e.g., explicit authorities, sufficient resources) to compel the operational CI entities to carry out that mission.

(U) IC CI entities were primarily established to protect their own operations and equities—what this report refers to as ***traditional CI***. Mr. Evanina told the Committee, for instance, that IC CI divisions are the "countering-the-threat-internally" portions of their organizations.[337] Consequentially, traditional CI does

---

information to vet visiting researchers and scientists for undisclosed conflicts of interests—such as arrangements with foreign research institutions. Interview with U.S. University 1 (Jan. 12, 2022).

[332] **(U)** Interview with U.S. Research Institutions (Jan. 11, 2022).

[333] **(U)** Interview with Cent. Intelligence Agency, Counterintelligence Mission Ctr. (Feb. 10, 2021).

[334] **(U)** Interview with U.S. Research Institutions (Jan. 11, 2022).

[335] **(U)** Interview with U.S. Investment Firm 1 (Dec. 7, 2021).

[336] **(U)** Interview with U.S. Energy Company 1 (Jan. 10, 2022).

[337] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

[redacted]

[redacted]

not "adequately address significant vulnerabilities that exist within other USG organizations and within non-government entities."[338]

Multiple officials confirmed Mr. Evanina's assertion. [redacted]

[redacted]

[redacted]

[redacted]

[338] **(U)** *Id.*

[339] [redacted]

[340] **(U)** *Id.*

[341] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 6 (2007).

[342] [redacted]

[343] **(U)** Interview with U.S. Dep't of Def., Under Sec'y of Def. for Intelligence & Sec., Counterintelligence & Law Enforcement (Aug. 3, 2021).

[344] **(U)** Interview with Nat'l Security Agency, Counterintelligence Div. (Dec. 8, 2021).

[345] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[redacted]

[redacted] Yet, as described in the Current Threat Landscape section of this report, much of the more concerning FIE activity is actually legal—such as exporting unclassified and uncontrolled technology from U.S. research institutions to China.

(U) NCSC plays a role in supporting traditional CI activities.[349] Mostly, NCSC facilitates collaboration and coordination between IC entities on an ad hoc basis and as an unofficial responsibility.[350] NCSC's interagency damage assessments and Mission Reviews also support the traditional CI mission.[351] Mr. Evanina noted in his written responses to this Committee that the responsibility for traditional CI "has resided and should remain within the separate cognizance and competence of units within the elements of the IC and the DOD."[352] He does see a role for NCSC in advising and assisting the IC with counter-espionage efforts, but notes that NCSC's focus should be on strategy, policy, and threat awareness—not operations, investigations, or collections.[353] Moreover, the general sentiment on NCSC's role in traditional CI appears to be that the IC "has it covered" and does not need NCSC's help.[354] [redacted]

(U) For these reasons, multiple CI experts have therefore been calling for a ***broadening*** of the CI mission towards ***strategic CI***. As Mr. Evanina pointed out in his written response to this Committee, "USG efforts to analyze, pursue, and counter CI threats must include but extend beyond traditional CI work."[356]

---

[346] [redacted]

[347] **(U)** *Id.*

[348] [redacted]

[349] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Deputy Dir. (Oct. 29, 2020).

[350] **(U)** *See* "Duties and Authorities" section of this report.

[351] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).

[352] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020).

[353] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[354] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Former Deputy Dir. (Oct. 8, 2020).

[355] [redacted]

[356] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S.

[redacted]

[redacted]

Strategic CI is not defined in statute and "remains a relatively undeveloped concept, in theory and implementation."[357] However, the prior National CI Strategy defined strategic CI as "the process and product of developing the context, knowledge, and understanding of the strategic environment required to support U.S. national security policy and planning decisions."[358] Ms. Van Cleave told the Committee that strategic CI requires looking at FIEs as strategic targets and aligning appropriate U.S. resources against those targets.[359] ***The fundamental insight of strategic CI is that today foreign actors use all instruments of national power to achieve their objectives, and CI must likewise defend against this full array of activities.***[360] Simply put, strategic CI focuses on using all available national resources to defend the United States as a whole rather than on protecting individual IC entities or their parochial operations. [redacted]

(U) NCSC officials believe that the Center should focus primarily on strategic CI.[363] Mr. Orlando believes that NCSC should fully own the strategic CI mission, while continuing to play a role in coordinating traditional CI activities. [redacted]

Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020).

[357] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 1 (2007).

[358] **(U)** *See* THE NATIONAL CI STRATEGY.

[359] **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Dir. (Apr. 1, 2022).

[360] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 1 (2007).

[361] [redacted]

[362] [redacted]

[363] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[364] **(U)** *Id.*

[365] [redacted]

[redacted]

[redacted]

(U) In practice, the Committee assess that a move towards strategic CI would require that the operational and analytic focus of the U.S. CI enterprise prioritize ***national level requirements***, including for analytic production and operations. Specifically, individual agencies would need to develop CI assessments that feed into (1) ***strategic analyses*** of FIE plans, intentions, capabilities, and vulnerabilities and (2) ***operational planning*** that arrays the resources of the disparate CI entities to protect national security secrets and other valuable information.[369] Such a move would ***complement, not replace***, existing traditional CI activities necessary to protect IC equities.

(U) "Owning" the strategic CI mission would require NCSC to develop a ***national strategic CI program*** to execute the strategic CI mission spelled out in the National CI Strategy.[370] ***A strategic CI program would bring together the budgets, billets, roles and responsibilities, and processes necessary to execute the strategic CI mission.***[371] Such a program would enable integrated planning, orchestration, and execution of strategic CI operations[372] and would sit below the National CI Strategy.[373]

(U) In 2005, the Iraq WMD Commission unequivocally voiced support for building such a strategic CI program.[374] The Commission recommended that NCIX—NCSC's predecessor—assume the power and responsibility to, among other things, prepare the National Intelligence Program's (NIP)[375] CI budget and approve, oversee, and evaluate how agencies execute that budget; produce national CI

---

366 [redacted]

367 [redacted]

368 [redacted]

369 **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 4 (2007) (As one former CI official, and current Committee staff not involved in the drafting of this report noted, strategic CI efforts and requirements are currently "not represented in a distinct way at the ODNI level to get effective coordination, advocacy, and resourcing." This former official noted that, at the moment, tasking for strategic CI priorities is ad hoc and done at the working level).

370 **(U)** *Scholars or Spies: Foreign Plots Targeting America's Research and Development: Joint Hearing Before the Subcomm. On Oversight and Subcomm. on Research & Tech of the H. Comm. on Sci., Space, & Tech.*, 115th Cong. (2018) (statement of Michelle Van Cleave).

371 **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Apr. 1, 2022); Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Apr. 1, 2022).

372 **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Oct. 6, 2020).

373 **(U)** Michelle Van Cleave, *Strategic Counterintelligence* 2 (Oct. 2020).

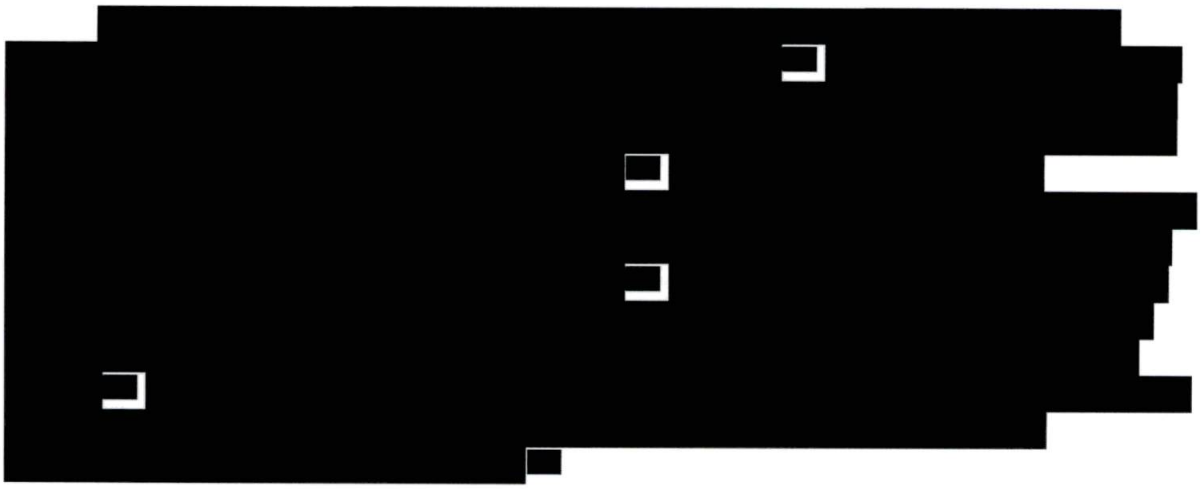
374 **(U)** 2005 WMD FINAL REPORT at 490-91

375 **(U)** The National Intelligence Program funds intelligence activities in several USG departments and the CIA. *National Intelligence Program, Federal Budget: Fiscal Year 2012*, WHITE HOUSE (2012).

[redacted]

[redacted]

requirements and assign operational responsibilities to agencies for meeting those requirements; and evaluate the effectiveness of agencies within the IC in meeting national CI requirements.[376] However, as will be explained in the next section, neither NCIX nor NCSC ever obtained such power.



(U) Mr. Evanina noted in written responses to this Committee that NCSC does "seek to establish" a national-level effort that integrates and coordinates diverse programs, resources, and activities of the USG.[382] Mr. Orlando also noted that NCSC is working with the IC to develop an implementation plan for the next National CI Strategy—but NCSC will still lack any enforcement mechanism.[383]

(U) Despite the growing importance of strategic CI, it remains unclear whether NCSC was established to focus on strategic CI, traditional CI, or both. No law explicitly mentions strategic or traditional CI, or distinguishes between the two. As Ms. Cleave pointed out, "The end goal behind the creation of the NCIX remains a matter of some dispute. Is the objective to establish a new capability to execute the

---

[376] **(U)** *Id.*

[377] [redacted]

[378] [redacted]

[379] [redacted]

[380] [redacted]

[381] [redacted]

[382] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 3 (June 3, 2020).

[383] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[redacted]

[redacted]

strategic CI mission or simply to become more efficient at performing standing [i.e., traditional CI] missions of the several CI agencies?"[384]

4. [redacted]

[redacted] In general, the IC CI enterprise is postured defensively and has a law-enforcement orientation. Given the nature, scale, and sophistication of FIE threats today, [redacted] As Mr. Evanina noted in testimony before this Committee, "We are under persistent, systematic, and strategic attack. We must be aggressive in our defense, protective posture, and offensive operations to provide even a modicum of deterrence."[386] He added that one of the most important tools in the CI space is offensive operations.[387] Mr. Orlando also believes that the CI community should be much more focused on offensive CI; "we need to get there."[388] Ms. Van Cleave believes that offensive CI should be the ***central objective*** of the strategic CI mission.[389]

(U) CI experts have been calling for a reorientation of the CI enterprise toward a more offensive posture for at least twenty years:

- **(U)** Back in 2002, the NCIX conducted a top-to-bottom review of the U.S. CI landscape and concluded that the national CI enterprise needed to be reconfigured to go on the offensive, [redacted]
- **(U)** In 2005, the Iraq WMD Commission also argued for going on the offense. ***The report noted that U.S. CI is "bureaucratically***

---

[384] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 11 (2007).

[385] [redacted]

[386] [redacted]

[387] **(U)** *Id.*

[388] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[389] **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Sept. 28, 2001).

[390] [redacted]

[redacted]

[redacted]

fractured, passive (i.e., focusing on the defense rather than going on the offense), and too often simply ineffective."[391] The report also mentioned that "while our defense is lacking, our current counterintelligence posture also results in the ***loss of offensive opportunities*** to manipulate foreign intelligence activities to our strategic advantage."[392]

- [redacted]
- **(U)** Also in 2009, INSA noted that defensive CI had been favored over the past 20 years and that this posture was insufficient to counter the new strategic threats: "The traditional CI-defensive missions of breeches through risk avoidance, and prosecuting breaches when they are exposed, remain vital but do not meet the broader national security objects of a robust, offensive CI effort."[394]

(U) The USG, however, has not substantially changed its approach to offensive CI. [redacted]

[391] **(U)** 2005 WMD FINAL REPORT at 487 (emphasis added).
[392] **(U)** *Id.* at 486 (emphasis added).
[393] [redacted]
[394] **(U)** 2009 INSA CI REPORT at 2-3.
[395] [redacted]
[396] [redacted]
[397] **(U)** *Id.*
[398] **(U)** *Id.*
[399] **(U)** *Id.*

[redacted]

[redacted]

(U) Despite the importance of offensive CI to confronting today's threat landscape, [redacted] The 2002 CI Enhancement Act is silent on offensive CI and [redacted]

5. (U) NCSC's Security Responsibilities are Important, but there is Disagreement over the Optimal Relationship between CI and Security

(U) When the Counterintelligence Enhancement Act passed in 2002, CI and security were handled separately. DNI Clapper directed the establishment of NCSC in 2014, in part, to consolidate the security and CI missions within one organization.[408] Yet, NCSC was never statutorily assigned a security mission; all statutory duties assigned to NCSC were CI duties. Moreover, there is no statutory definition of "security." Officials are divided over what role NCSC should play, if any, in the security mission.

---

400 [redacted]

401 **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

402 [redacted]

403 [redacted]

404 [redacted]

405 [redacted]

406 [redacted]

407 [redacted]

408 **(U)** MICHAEL E. DEVINE, CONG. RES. SERV., IF11006, THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC): AN OVERVIEW 2 (2018).

[redacted]

[redacted]

(U) Most officials the Committee spoke with agreed that NCSC should play a role in the security mission and believed that CI and security should be tightly intertwined because security remains a crucial part of the solution to the strategic CI problem set. As one official noted, security is "left of CI" and the security mission is responsible for getting involved much sooner in the process to counter a threat than the CI mission. For example, he argued that the IC [redacted] [409]

(U) A former NCSC official further explained that CI is largely "proactive" whereas security is largely "reactive," but there is potential for real synergy between the two that will not happen unless they are joined together.[410] For instance, several officials told the Committee that the main way in which the USG could better protect research paid for by U.S. taxpayer dollars would be to ensure that [redacted].[411]

(U) CI also helps inform security of the nature, scale, and scope of a threat. DNI Clapper noted that CI and security should be addressed as interdependent and mutually supportive disciplines. "These disciplines have shared objectives and responsibilities associated with the protection of information, sources, and methods."[412] [redacted]

[redacted] *NCSC 2024: A Vision of the Future*—a white paper that NCSC developed for the Committee in response to this review—notes that NCSC has [redacted]

---

[409] [redacted]

[410] **(U)** Interview with Former Nat'l Counterintelligence & Sec. Ctr. Official (Oct. 9, 2020).

[411] [redacted]

[412] **(U)** Press Release, Office of the Dir. of Nat'l Intelligence, DNI Clapper Establishes the National Counterintelligence and Security Center (Dec. 1, 2014).

[413] [redacted]

[414] [redacted]

[redacted]

[redacted]

(U) Because of the synergy between CI and security, several current and former NCSC officials suggested officially making the Director of NCSC the Security Executive Agent (SecEA)[416] so that NCSC fully owns both the CI and security mission sets and can de-conflict as appropriate.[417] One former official noted that the Director of NCSC is already the de facto SecEA, but making the title official would "speed along" needed policy changes.[418] Mr. Evanina believes that ODNI does not exercise sufficient leadership as SecEA, and that NCSC should take on the mantle because security and CI are "equally important."[419]

(U) Other CI officials told the Committee that there is still room for improvement in integrating CI and security. One NCSC official told the Committee that CI and security are "two sides of the same coin," but in practice the "connecting pipes" between the two mission sets are not always there, and that the NCSC needs stronger touch points. This official explained, for example, that sometimes [redacted][420]

(U) On the other hand, several CI practitioners warn of too tight a linkage between the CI and security mission sets. Ms. Van Cleave, for example, believes there should be a strong firewall between CI and security. [redacted] "Sound security measures are unquestionably vital, but they can only carry protection so far. One can pile on so much security that no one can move, and still there will be a purposeful adversary

---

[415] [redacted]

[416] **(U)** The SecEA is responsible for providing oversight for background personnel security investigations and determinations of eligibility for access to classified information; developing policies and procedures related to security clearance determinations; and issuing guidelines to heads of agencies promoting security investigation timeliness, uniformity, efficiency, and centralization. The SecEA also serves as the final authority to designate agencies to conduct investigations and determine eligibility for access to classified information in accordance with government standards for eligibility. *See* Appendix A for more information.

[417] **(U)** Currently, the DNI is the SecEA.

[418] **(U)** Document provided by Former Deputy Director, Nat'l Counterintelligence & Sec. Ctr., 3 (Oct. 8, 2020).

[419] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[420] [redacted]

[421] [redacted]

[redacted]

looking for ways to get what he wants. The signature purpose of counterintelligence is to confront and engage the adversary."[422]



[422] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 2 (2007).

[423]

[424]

[425] **(U)** *Id.*

[426] **(U)** *Id.*

[redacted]

B. (U) DUTIES AND AUTHORITIES

(U) NCSC's duties have changed over its 20-year lifespan, due in part to lack of clarity over its mission. Various duties are enumerated in statute, but NCSC does not effectively fulfill all of them. In addition, NCSC has taken on several duties not explicitly assigned in statute. In general, the Committee assesses that NCSC's focus at any given time is based on the perceived CI gaps the IC needs filled or the interests of its Director, rather than on a well-formulated and enduring vision of the activities it should be undertaking to support its mission. Ms. Van Cleave noted that "fundamentally, there is no agreed-upon understanding of what NCSC is supposed to do."[427] Several FBI officials also told the Committee that NCSC "seems to be all over the place."[428] One NCSC official said that NCSC's "sweet spot" is not to replicate work already being done by the IC, but to identify and fill gaps and seams. Thus, NCSC often takes on projects that do not have "natural homes" at other agencies,[429] offloading projects to agencies better suited to handle them when possible.[430]

(U) NCSC is also limited in its ability to carry out its duties by ambiguous or insufficient authorities. NCSC can influence and advocate for IC CI spending, but NCSC has little authority or leverage over IC entities. NCSC can also provide voluntary guidance, threat awareness, and advice to NT-50s and non-USG entities on developing and maintaining effective CI and security programs, but NCSC cannot provide direct financial support, and NT-50s and non-USG entities are not required to maintain CI programs. NCSC officials told the Committee that much of NCSC's ability to influence CI and security programs across the USG stems from personal relationships and advocacy, rather than statutes, regulations, or other authorities.

1. (U) NCSC Does Not Fulfill All Statutorily Assigned Duties Partly Due to Authority and Resource Limitations

(U) NCSC fulfills some, but not all, of the duties currently assigned to it in statute. Authority limitations prevent NCSC from fully carrying out all of its statutory responsibilities. There is also disagreement over whether and how NCSC should be performing some of these duties. The following discusses NCSC's authorities as set forth in 50 U.S.C. § 3383.

i. (U) *Strategic Planning*

(U) The 2002 Counterintelligence Enhancement Act directs NCSC to conduct several strategic planning activities, namely producing an annual strategic

---

[427] **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Oct. 6, 2020).
[428] **(U)** Interview with Fed. Bureau of Investigation, Counterintelligence Div. (Sept. 20, 2021).
[429] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).
[430] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Deputy Dir. (Oct. 29, 2020).

[redacted]

[redacted]

planning assessment of U.S. CI requirements (the NTIPA), as well as an annual strategy for CI programs (the National CI Strategy).[431] NCSC is also responsible for developing Key Intelligence Questions, Collection Emphasis Memos, and Analysis Emphasis Memos,[432] as well as CI priorities for the National Intelligence Priorities Framework (NIPF). NCSC also produces several country-specific CI strategies.

(U) Various officials agreed that NCSC should play this strategic planning role. For instance, multiple NCSC officials confirmed that NCSC plays an important role within the CI community in setting CI priorities and influencing policy and strategy "at the 50,000-foot level."[433] [redacted]

(U) The National CI Strategy, however, is incomplete. The Committee assessed the National CI Strategy against GAO's "desired characteristics" for national strategies[435] and identified several deficiencies.[436] First, the National CI Strategy does not identify subordinate objectives or performance measures.[437] Subordinate objectives explain the steps necessary to achieve the strategic goals and performance measures are necessary to gauge results.[438] The National CI Strategy also does not identify necessary resources and investments or risk management activities.[439] These elements address what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs.[440] In addition, the National CI Strategy does not identify organizational roles and responsibilities or coordination activities.[441] These elements are important because they identify who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.[442] Finally,

---

[431] **(U)** 50 U.S.C. § 3383 (d).
[432] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).
[433] **(U)** Interview with Former Nat'l Counterintelligence & Sec. Ctr. Official (Oct. 9, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr.; Former Nat'l Intelligence Officer (Dec. 18, 2020).
[434] [redacted]
[435] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-408T, COMBATTING TERRORISM: EVALUATION OF SELECTED CHARACTERISTICS IN NATIONAL STRATEGIES RELATED TO TERRORISM (2004).
[436] **(U)** *Id.* National strategies are not required, by statute or by executive mandate, to address a single, consistent set of characteristics. GAO, however, identified the elements that national strategies *should* have.
[437] **(U)** *See* Committee analysis of THE NATIONAL CI STRATEGY.
[438] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-408T, COMBATTING TERRORISM: EVALUATION OF SELECTED CHARACTERISTICS IN NATIONAL STRATEGIES RELATED TO TERRORISM (2004).
[439] **(U)** *See* Committee analysis of THE NATIONAL CI STRATEGY.
[440] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-408T, COMBATTING TERRORISM: EVALUATION OF SELECTED CHARACTERISTICS IN NATIONAL STRATEGIES RELATED TO TERRORISM (2004).
[441] **(U)** *See* Committee analysis of THE NATIONAL CI STRATEGY; Interview with Nat'l Counterintelligence & Sec. Ctr., Former Deputy Director (Oct. 8, 2020).
[442] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-408T, COMBATTING TERRORISM: EVALUATION OF SELECTED CHARACTERISTICS IN NATIONAL STRATEGIES RELATED TO TERRORISM (2004).

[redacted]

[redacted]

the National CI Strategy lacks an integration and implementation plan.[443] Such a plan is important to address how the national strategy relates to other strategies' goals, objectives, and activities and how to subordinate levels of government and their plans to implement the strategy.[444]

(U) Mr. Evanina and Mr. Orlando agreed that the National CI Strategy lacks some key features.[445] Mr. Orlando explained that ***NCSC cannot identify performance measures, resources, organizational roles, and responsibilities in the strategy, or develop an implementation plan for the strategy, because NCSC lacks the requisite authorities.***[446] Mr. Evanina similarly noted, in a letter to the Committee, that "NCSC lacks the authority to direct key stakeholders," including both the IC and NT-50 agencies, to ensure CI requirements are met.[447] As the Iraq WMD Commission noted in 2005, [NCSC] has "no ability to assign operational responsibility."[448]

[redacted] NCSC officials told Congress that the Center had planned to draft interagency implementation plans for the five critical areas outlined in the National CI Strategy: (1) Critical Infrastructure, (2) Supply Chains, (3) Counter Exploitation of U.S. Economy, (4) Foreign Influence, and (5) Cyber/Technical Operations.[449] NCSC planned to use those written "organizational constructs to lay out roles, responsibilities, and authorities of each of the strategic pillars, and to identify the gaps which [the National Security Council (NSC)] will consider how best to fill."[450] [redacted] Regardless, even if it had developed such plans, NCSC would still lack the authorities to ensure compliance with the

---

[443] **(U)** *See* Committee analysis of THE NATIONAL CI STRATEGY; Interview with Nat'l Counterintelligence & Sec. Ctr., Former Deputy Director (Oct. 8, 2020).

[444] **(U)** *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-408T, COMBATTING TERRORISM: EVALUATION OF SELECTED CHARACTERISTICS IN NATIONAL STRATEGIES RELATED TO TERRORISM (2004).

[445] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[446] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021).

[447] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 6 (June 3, 2020).

[448] **(U)** 2005 WMD FINAL REPORT at 490.

[449] **(U)** THE NATIONAL CI STRATEGY at 10.

[450] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[451] **(U)** Email from Office of Legislative Affairs, Office of the Dir. of Nat'l Intelligence to Staff, S. Select Comm. on Intelligence (Feb. 8, 2022).

[redacted]

[redacted]

implementation plans or the priorities laid out in the National CI Strategy more broadly.

ii. **(U)** *Evaluating Implementation of the National CI Strategy*

(U) The 2002 Counterintelligence Enhancement Act also directs NCSC to evaluate on an ongoing basis the implementation of the National CI Strategy and agencies' compliance with the National CI Strategy.[452] Several CI officials believe that evaluating implementation of the National CI Strategy is an important function and should continue.[453] However, NCSC lacks the authority to direct IC entities to address identified deficiencies or to compel NT-50s or non-USG entities to undergo an evaluation.

(U) The primary way in which NCSC evaluates IC agencies' alignment with the National CI Strategy and certain aspects of IC agencies' CI programs is through its Mission Reviews.[454] Mr. Evanina noted that this process has improved over time:

[redacted]

(U) One NCSC official said that these reviews drive a lot of the IC's CI resource alignments to the National CI Strategy.[456] However, Mr. Evanina said that right now no one is in charge of ensuring alignment and that NCSC simply "trusts" agencies to do it.[457] He mentioned that several CI entities, however, have

---

[452] **(U)** 50 U.S.C. § 3383 (d)(3).

[453] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).

[454] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022); Interview with, Nat'l Counterintelligence & Sec. Ctr., Mission Integration Div. (May 12, 2021) (NT-50s do not submit their CI or security budgets to NCSC. NCSC sends each IC agency an annual survey of 59 questions and then conducts site visits. After NCSC's Mission Resources Directorate reviews all the data it received, it conducts in-person visits with the IC entities to discuss. These conversations help Mission Resources understand how to guide its advocacy efforts, and also helps Mission Resources understand the extent to which prior recommendations have been implemented).

[455] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 8 (June 3, 2020).

[456] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).

[457] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[redacted]

[redacted]

voluntarily aligned to the National CI Strategy.[458] Mr. Evanina and Mr. Orlando similarly noted that the IC is generally responsive to NCSC's direction and priorities.[459] However, Mr. Evanina noted that NCSC's ***leverage is admittedly reliant upon the power of persuasion*** and a recognition that NCSC is in a uniquely visible position to be able to advocate for CI and security interests across our stakeholder communities."[460]

[redacted]

(U) As explained above, NT-50s also play an important role throughout the federal government in protecting sensitive information, but NT-50s are not required to have "CI awareness" or security programs, and most do not.[465] NCSC officials told the Committee that it is difficult to evaluate programs that do not exist.[466] Some NT-50s have participated in Mission Reviews, but these are voluntary and more limited in scope compared to IC agency Mission Reviews.[467] As a result, NT-50s may not be closely aligned to the National CI Strategy.[468] Essentially, NCSC is unable to evaluate the compliance of a large portion of the federal government to

---

[458] **(U)** *Id.*

[459] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[460] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 8 (June 3, 2020) (emphasis added).

[461] [redacted]

[462] [redacted]

[463] [redacted]

[464] **(U)** *Id.* (emphasis added).

[465] **(U)** *See also* Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

[466] **(U)** *Id.*

[467] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).

[468] **(U)** *Id.*

[redacted]

[redacted]

the National CI Strategy—including many agencies that oversee the strategic CI priorities laid out in the National CI Strategy.[469]

[redacted]—due, in part, to the lack of clarity over whether NT-50s are part of the CI enterprise. This lack of authority over NT-50 CI programs can be contrasted with NCSC's authority to assess the effectiveness of ***insider threat*** programs across the Executive Branch.

[redacted] In October 2011, President Obama issued EO 13587 establishing the National Insider Threat Task Force (NITTF) under the joint leadership of the Attorney General and the DNI.[471] President Obama later issued the National Insider Threat Policy and Minimum Standards, which mandated that every Executive Branch department/agency with access to classified information establish a formal insider threat program and meet all twenty-six minimum standards.[472] In addition to mandating the drafting of policy and standards, EO 13587 directed the NITTF to independently assess progress in meeting key programmatic milestones and adherence to the standards. The NITTF finalized its assessment process in 2015 and determined that [redacted].[473]

[redacted] The NITTF publishes an Annual Report that details department/agency progress in meeting the insider threat program requirements. In 2017, the NITTF Annual Report highlighted the significant progress that many NT-50s agencies made in developing and executing an insider threat program. After the President mandated minimum standards for insider threats, there were considerable improvements across the USG: "The NT50 Federal Partner community achieved the most progress during 2017... [redacted]

[redacted] Importantly, while President Obama's executive actions mandated certain insider threat requirements, Congress also ***significantly*** increased appropriations to support these new requirements. [redacted]

---

[469] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).

[470] [redacted]

[471] [redacted]

[472] **(U)** *Id.*

[473] **(U)** *Id.*

[474] [redacted] *Id.*

[redacted]

[redacted]

[redacted]

(U) NCSC officials recognize that NCSC's ability to comprehensively influence and impact federal agencies' efforts on insider threat programs stems from President Obama's executive order and subsequent National Insider Threat Policy and Minimum Standards.[476] ***There are no comparable minimum standards for NT-50s to create, maintain, or execute a "CI awareness" or security program of any kind.*** As a result, CI program effectiveness varies greatly across NT-50s. NCSC officials said that currently some NT-50s, such as HHS, maintain fairly robust "CI awareness" and security capabilities, while other agencies have no such programs.

(U) In an attempt to address these deficiencies, the FY21 Intelligence Authorization Act (IAA) directed the NCSC Director "to develop a plan within 90 days of enactment of this Act for assessing the effectiveness of all government agency counterintelligence programs."[477] NCSC officials told the Committee that without Executive Branch-wide mandatory minimum standards or requirements—such as the insider threat minimum standards—NCSC is not properly postured to assess NT-50 CI programs.[478] [redacted]

(U) Non-USG entities, such as industry and academia, are also not universally required to have "CI awareness" or security programs.[480] As Mr. Evanina noted in his written responses to this Committee, private businesses, universities, laboratories, and other non-governmental organizations do not have CI as their core mission function and thus "generally operate at a very low level of CI and security awareness."[481] In some instances, industry and academic institutions that receive federal funding must establish security programs in compliance with the National Industrial Security Program Operating Manual (NISPOM), maintained by DCSA, but NCSC has no insight into these programs.[482] Thus, NCSC

---

[475] [redacted]

[476] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021); Interview with Nat'l Counterintelligence & Sec. Ctr., Deputy Dir. (Oct. 29, 2020).

[477] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).

[478] **(U)** *Id.*

[479] [redacted]

[480] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 4 (June 3, 2020).

[481] **(U)** *Id.*

[482] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022); Interview with U.S. Dep't of Def., Def. Counterintelligence & Sec. Agency (May 14, 2021).

[redacted]

[redacted]

is unable to fully evaluate how the private sector and academia protect the core national security sectors outlined in the National CI Strategy, particularly critical infrastructure or sensitive R&D.

(U) One former NCSC official suggested that NCSC could help private sector companies assess their security programs and identify vulnerabilities[483]—a kind of non-governmental Mission Review—but what this assistance would look like is unclear. Other NCSC officials told the Committee that it is not feasible to expect NCSC to evaluate these sectors' compliance with the National CI Strategy; [redacted]

iii. **(U)** *Analysis*

(U) The 2002 Counterintelligence Enhancement Act directs NCSC to "oversee and coordinate the production of strategic analyses" of CI matters, including the production of CI damage assessments and lessons learned.[485] NCSC's role in overseeing and coordinating strategic analyses has changed over time. NCSC officials also have differing views on whether the Center should have analysis staff and produce original analytic pieces on strategic CI, or if NCSC should simply task other IC entities to do this analysis.

(U) Strategic CI analysis has not always been a focus of the IC. In 2009, the Review Group found that, although assessing the intelligence capabilities and activities of U.S. adversaries had always been an important component of CI, the CI community had not always provided ***strategic CI*** analysis that effectively supported warning, mission planning and operations.[486] One year later, in 2010, the DNI directed the NCIX to undertake appropriate measures to initiate, oversee, and coordinate strategic analysis in accordance with exiting statutory authority.[487] Thus, the Office of the National Counterintelligence Executive (ONCIX) took on strategic CI analysis as a core mission function.

(U) Mr. Evanina changed this mission function when he became Director of NCSC in 2014. He told the Committee that [redacted] were dedicated to doing finished intelligence analysis, but he thought that this work was often duplicative of other IC analytic products and did not always follow IC standards. He eliminated the original analysis mission entirely and refocused

---

[483] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).

[484] [redacted]

[485] **(U)** 50 U.S.C. § 3383 (d)(4).

[486] **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 3).

[487] **(U)** *Id.*

[redacted]

[redacted]

NCSC on driving collection priorities.[488] Under this new analytic model, NCSC issues Collection Emphasis Memos or Analysis Emphasis Memos to IC entities to collect and analyze on key CI priorities instead of doing the actual analytic work. Mr. Evanina told the Committee that he was generally very satisfied with the IC's responsiveness [redacted] and is occasionally "flooded" with responses.[489] One NCSC official [redacted][490]

(U) Several current NCSC officials agreed with Mr. Evanina's approach. One official told the Committee, for example, that NCSC should not be duplicating the analytic work of other IC entities, but should instead conduct mission-level

[redacted]

[488] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[489] **(U)** *Id.*
[490] [redacted]
[491] [redacted]
[492] [redacted]
[493] [redacted]
[494] [redacted]
[495] [redacted]

[redacted]

[redacted]

(U) Multiple CI officials emphasized the importance of interagency damage assessments and believe that NCSC should do more work in this space. [redacted]

iv. **(U)** *National Counterintelligence Program Budget*

(U) The Counterintelligence Enhancement Act directs NCSC, in consultation with the DNI, to coordinate the development of budgets and resource allocation plans for the CI programs and activities of DOD, the FBI, the CIA, and other appropriate elements of the USG to ensure that they are aligned with the National

---

[496] **(U)** *Id.*

[497] [redacted]

[498] **(U)** *Id.*

[499] **(U)** *Id.*

[500] [redacted]

[501] [redacted]

[502] [redacted]

[503] [redacted]

[504] **(U)** *Id.*

[redacted]

[redacted]

CI Strategy.[505] NCSC, however, lacks the authority to directly control IC and NT-50 CI budgets and resource allocation plans. NCSC can instead inform guidance on CI programs and can advocate for specific items, but ODNI maintains ultimate control.[506]

[redacted]

(U) However, in reality ODNI and IC agencies retain ultimate control over CI and security budget decisions. This problem was identified as far back as 2005, when the Iraq WMD Commission noted that the NCIX "has only advisory budget authority" and "little visibility into individual agencies' counterintelligence operations."[509] As Mr. Evanina said, "***NCSC does not control the budgetary process; while we can advocate, we cannot allocate funds.***"[510] [redacted]

(U) In lieu of directly coordinating the development of budgets and resource allocation plans, NCSC "advocates" to help the IC obtain the CI resources needed to carry out their missions.[512] Mr. Evanina noted in his written responses to this Committee that NCSC uses the significant amount of data its collects regarding CI community programs, investigations, analyses, and information sharing activities

---

[505] **(U)** 50 U.S.C. § 3383 (d)(5).

[506] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[507] [redacted]

[508] [redacted]

[509] **(U)** 2005 WMD FINAL REPORT at 490.

[510] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 8 (June 3, 2020) (emphasis added).

[511] **(U)** *Id.*

[512] **(U)** *Id.*

[redacted]

[redacted]

to "make a qualitative assessment of performance," and advocate for the CI community through the resource or policy process.[513] Mr. Evanina characterized such advocacy efforts as a core (though informal) role for NCSC.[514]

[redacted]

(U) These limitations notwithstanding, NCSC officials said the Center has successfully advocated for several NT-50 CI programs over the years to get more resources,

[redacted]

[513] **(U)** *Id.* at 2.
[514] **(U)** *Id.* at 5
[515] **(U)** *Id.*
[516] [redacted]
[517] [redacted]
[518] [redacted]
[519] [redacted]

[redacted]

[redacted]

(U) Finally, NCSC is limited in the direct financial support it can provide NT-50s due to restrictions on providing NIP funding to agencies that operate on non-NIP funding. There are substantial legal and jurisdictional complications associated with NCSC giving NIP funds to NT-50 agencies, yet this issue is worth highlighting because several NCSC officials stressed its importance. [redacted] NCSC instead attempts to serve those organizations through advice, guidance, and "soft power."[524]

v. **(U)** *Vulnerability Assessments*

(U) The 2002 Counterintelligence Enhancement Act directs NCSC to "carry out and coordinate surveys of the vulnerability of the [USG], and the private sector, of intelligence threats in order to identify the areas, programs, and activities that require protection from [FIE] threats."[525] NCSC has not conducted these assessments in approximately ten years, however. NCSC officials provided two reasons for this.[526]

(U) First, NCSC officials explained that NCSC cannot compel any entity to undergo a vulnerability assessment; these are purely voluntary.[527] [redacted]

---

[520] [redacted]

[521] [redacted]

[522] **(U)** *Id.*

[523] [redacted]

[524] **(U)** Interview with Office of the Dir. of Nat'l Intelligence (Oct. 5, 2021); Interview with Office of the Dir. of Nat'l Intelligence (Nov. 18, 2021); **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[525] **(U)** 50 U.S.C. § 3383 (d)(7).

[526] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[527] **(U)** *Id.*

[redacted]

[redacted] For instance, NCSC recently released an unclassified publication entitled *Protecting Critical and Emerging U.S. Technologies from Foreign Threats* aimed at highlighting vulnerabilities in the tech sector.[535]

vi. **(U)** *Outreach to NT-50s and Non-USG Entities*

(U) The 2002 Counterintelligence Enhancement Act directs NCSC to carry out and coordinate CI outreach programs and activities to other elements of the USG and to the private sector and disseminate public warnings on intelligence threats.[536] Most officials told the Committee that they agreed that this is an important role for NCSC to play, but it is not clear what type of outreach NCSC should be conducting or whether it should be a top priority.

(U) Public outreach is a relatively new function for the USG in general and the IC in particular. NCSC's precursor only began outreach to the private sector in 2010, when it first provided briefings on potential FIE threats and risks posed by

---

[528] **(U)** *Id.*

[529] [redacted]

[530] [redacted]

[531] **(U)** *Id.*

[532] **(U)** *Id.*

[533] **(U)** *Id.*

[534] **(U)** *Id.*

[535] **(U)** NAT'L COUNTERINTELLIGENCE & SEC. CTR., OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PROTECTING CRITICAL AND EMERGING U.S. TECHNOLOGIES FROM FOREIGN THREATS (2021).

[536] **(U)** 50 U.S.C. § 3383(d) (7)(B).

[redacted]

[redacted]

foreign acquisitions of U.S. technology.[537] When outreach efforts began, this Committee considered it to be a "major development."[538] Over the past few years, outreach has become a core mission for NCSC.[539] Several officials believe that this is an appropriate focus for NCSC. Mr. Orlando, for instance, told the Committee that the IC strongly supports NCSC's role in interfacing with non-IC entities.[540]

(U) Outreach to industry and academia is important because, in most cases, the federal government does not build national security systems or conduct original research; national security systems are built by the massive defense contractor base and original research is conducted by universities and laboratories.[541] However, individuals working in these sectors may not realize they are being targeted by FIEs. A current NCSC official told the Committee that "non-IC people" generally do not understand how CI pertains to them, so NCSC and other members of the IC need to tell this story.[542] A former NCSC official even said that NCSC's primary role should be focused on threats and warnings to external (i.e., non-IC) groups that do not have the capabilities, resources, or experience to deal with insider or FIE threats.[543]

[redacted]

(U) For example, NCSC provides outreach to key industry partners across 17 critical infrastructure sectors via its Critical Infrastructure Task Force. [redacted]

---

[537] **(U)** Committee briefing with Robert Bryant, Dir., Office of the Nat. Counterintelligence (Feb. 18, 2009).

[538] **(U)** *Id.*

[539] [redacted] NAT'L COUNTERINTELLIGENCE & SEC. CTR., NCSC 2024: A VISION OF THE FUTURE (2021).

[540] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021).

[541] **(U)** *See* Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020).

[542] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).

[543] **(U)** Interview with Former Nat'l Counterintelligence & Sec. Ctr. Official (Oct. 9, 2020).

[544] [redacted]

[545] [redacted]

[redacted]

[redacted]

[redacted] NCSC also conducts "roadshows," in coordination with this Committee and ODNI, to educate key leaders in industry and academia about FIE threats targeting their sectors.

(U) Outreach to NT-50s is also important because FIEs are increasingly targeting agencies such as the Department of Agriculture or OPM. As far back as 2010, Mr. Bryant said that he considered it imperative to engage government at all levels and noted that there are numerous NT-50s that may be targeted by FIE services but that are not adequately organized or resourced to counter the threat.[547] For example, one NCSC official explained that the OPM data hack could be partly attributed to the fact that OPM is an NT-50 agency and simply did not understand the CI and security threats facing the agency.[548] [redacted]

(U) Finally, NCSC also plays a role in educating the public at large. For instance, NCSC partnered with the FBI in September 2020 to release a YouTube campaign called *The Nevernight Connection* to increase awareness of FIE threats on professional networking sites and other social media platforms.[550] [redacted]

(U) NCSC wants to lean further into outreach efforts. According to *NCSC 2024: A Vision of the Future,* NCSC sees such efforts as its number one area for growth going forward,[552] and several other CI officials agree. [redacted]

---

546 [redacted]

547 **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 8).

548 **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Deputy Dir. (Oct. 29, 2020).

549 [redacted]

550 **(U)** Interview with Fed. Bureau of Investigation, Counterintelligence Div. (Sept. 20, 2021).

551 [redacted]

552 [redacted] NAT'L COUNTERINTELLIGENCE & SEC. CTR., NCSC 2024: A VISION OF THE FUTURE (2021).

553 [redacted]

554 [redacted]

[redacted]

[redacted]

(U) NCSC, however, faces several challenges in executing its outreach activities. First, NCSC ***lacks an outreach plan.*** [redacted]

(U) Second, despite the enormous need for outreach and general education, [redacted] Several private sector and academic officials told the Committee, for instance, that they had not received sufficient threat awareness briefings from the IC.[557] Industry and academic officials told the Committee that many people working in areas such as life sciences or biotech or energy often lack even basic awareness of FIE threats.[558] Officials from one large financial company told the Committee that smaller financial firms "do not have as much of an appreciation for the strategic risks posed by China."[559] Officials from an energy company similarly told the Committee that most businesses probably do not understand that they are targets of foreign adversaries.[560] [redacted] Even then, many individuals both within and outside the CI community told the Committee they had never heard of NCSC or recalled seeing its outreach materials.[562]

(U) Finally, various other USG entities with a bigger geographic footprint and more resources already conduct outreach to industry and academia. Most notably, FBI conducts extensive outreach and is poised to do more through the new NCITF.[563] Most academic and industry officials told the Committee that USG

[redacted]

555 [redacted]

556 [redacted]

557 **(U)** Interview with U.S. Investment Firm 1 (Dec. 7, 2021); Interview with U.S. Energy Company 1 (Jan. 10, 2022); Interview with U.S. University 2 (Dec. 9, 2021). Officials from one energy company noted that they have received several general cybersecurity briefings from the FBI. Teleconference with U.S. Energy Company 1.

558 **(U)** Interview with U.S. Investment Firm 1 (Dec. 7, 2021); Interview with U.S. Energy Company 1 (Jan. 10, 2022); Interview with U.S. Research Institutions (Jan. 11, 2022).

559 **(U)** Interview with U.S. Investment Firm 1 (Dec. 7, 2021).

560 **(U)** Interview with U.S. Energy Company 1 (Jan. 10, 2022).

561 [redacted]

562 **(U)** Interview with Fed. Bureau of Investigation, New York City Field Office (Dec. 6, 2021); Interview with Fed. Bureau of Investigation, Houston Field Office (Jan. 11, 2022).

563 **(U)** Interview with Fed. Bureau of Investigation, Nat'l Counterintelligence Task Force (Feb. 3, 2022).

[redacted]

[redacted]

outreach in general was very limited, but that whatever outreach they were familiar with came from the FBI. [redacted] As another example, DCSA—an NT-50 entity in the federal government dedicated to protecting the United States' trusted workforce and trusted workspaces—also conducts outreach to the defense industrial base.[566] NIH conducts outreach to academic institutions involved in medical research.[567]

(U) It is therefore important to consider whether NCSC should be attending roadshows and conferences, reaching out to non-IC entities directly, and using social media to share threat warnings to the public or whether it should be more narrowly focused on developing strategic communications products that other USG entities could then distribute. [redacted] Mr. Evanina noted that NCSC could both develop the strategic communications products ***and*** conduct certain in-person outreach, depending on the circumstances.[570]

vii. **(U)** *Research and Development*

(U) The 2002 Counterintelligence Enhancement Act directs NCSC to "ensure that [R&D] programs and activities of the [USG], as well as the private sector, direct attention to the needs of the [CI] community for technologies, products, and services."[571] However, NCSC is not currently doing much work in this area. NCSC

---

564 [redacted]

565 [redacted]

566 **(U)** Interview with U.S. Dep't of Def., Def. Counterintelligence & Sec. Agency (May 14, 2021).

567 **(U)** Interview with U.S. Research Institutions (Jan. 11, 2022).

568 [redacted]

569 [redacted]

570 **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).

571 **(U)** 50 U.S.C. § 3383 (d)(7)(C).

[redacted]

[redacted]

has a chief scientist and a Community of Practice on CI countermeasures,[572] but its *2019 Year in Review* report did not include any R&D efforts.[573]

(U) There is a long-recognized need for R&D in the CI space. In 2005, the Iraq WMD Commission recommended that NCIX identify and direct the development and deployment of new and advanced CI methodologies and technologies.[574] In 2009, INSA called for advancing technological applications for CI among national agencies, law enforcement bodies, and military services.[575] INSA recommended that the IC collaborate with outside experts on issues such as cyber, advanced information technology, biotechnology, neuroscience, nanotechnology, materials science, and robotics, as well as in behavioral, social, and cultural sciences.[576]

[redacted]

[redacted] The need for new countermeasures is particularly acute given the emerging technologies described earlier in the report. [redacted]

---

[572] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[573] **(U)** *See also* 2019 YEAR IN REVIEW. The 2019 Year in Review report is the most recent available. NCSC has not yet issued its reports for 2020 or 2021.

[574] **(U)** 2005 WMD FINAL REPORT at 491.

[575] **(U)** 2009 INSA CI REPORT at 3.

[576] **(U)** 2009 INSA CI REPORT at 11.

[577] [redacted]

[578] [redacted]

[579] [redacted]

[580] [redacted]

[581] [redacted]

[redacted]

[redacted]

[redacted] NCSC believes that it must continue to develop expertise to identify vulnerabilities and propose countermeasures to protect sensitive information and facilities.[583]

[redacted]

viii. **(U)** *Training and Professional Development*

(U) The 2002 Counterintelligence Enhancement Act directs NCSC to "develop policies and standards for training and professional development of individuals engaged in [CI] activities and to manage the conduct of joining training exercises for such personnel."[590] Although ONCIX had a training branch, NCSC no longer sees training as a core mission function.[591] Although NCSC has undertaken one-off training events—such as convening forums or participating in table-top

---

[582] **(U)** *Id.*

[583] [redacted] NAT'L COUNTERINTELLIGENCE & SEC. CTR., NCSC 2024: A VISION OF THE FUTURE 4 (2021).

[584] [redacted]

[585] **(U)** *Id.*

[586] **(U)** *Id.*

[587] **(U)** *Id.*

[588] [redacted]

[589] [redacted]

[590] **(U)** 50 U.S.C. § 3383 (d)(7)(D).

[591] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

[redacted]

[redacted]

exercises[592]—NCSC officials explained that being a standing training provider was not a good use of limited resources.[593]

(U) Given its position, NCSC has not developed standardized CI training for the IC or NT-50s.[594] NCSC officials told the Committee that they are actively working to develop "competency standards" and a training compendium to highlight CI courses offered elsewhere.[595] [redacted]

(U) INSA identified a need for new CI tradecraft and training standards back in 2009.[597] Their *Counterintelligence for the 21st Century* report called for building a comprehensive, IC-wide training program that involves rigorous, formal CI courses for senior leadership, extensive training for CI personnel, and high-quality indoctrination for non-CI personnel. Such an effort should include partnerships with universities to develop credit courses, and should professionalize the CI cadre and train non-CI personnel by establishing policies and standards for CI training and education. "Even with the leading CI agencies today, CI training is outsourced in part because the most skilled insiders do not see conducting such training as career enhancing."[598]

(U) Several current and former NCSC officials added that centralized and standardized CI training is great in theory, but hard to do in reality, because the institutional culture at each agency is very strong and no one wants NCSC telling them how to conduct CI.[599] One NCSC official said that it may be possible to inject ***strategic CI*** training into all CI training curriculums across the community because there is less institutional attachment to that discipline.

(U) Finally, NCSC could also play an important role in training non-IC entities. One former NCSC official told the Committee that NCSC has provided some CI training to other USG agencies,[600] but more could be done. [redacted]

---

[592] **(U)** *See also* 2019 YEAR IN REVIEW.
[593] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).
[594] **(U)** *Id.*
[595] **(U)** *Id.*
[596] **(U)** *Id.*
[597] **(U)** 2009 INSA CI REPORT at 3.
[598] **(U)** *Id.* at 11.
[599] **(U)** Interview with Former Nat'l Counterintelligence & Sec. Ctr. Official (Oct. 9, 2020); Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).
[600] **(U)** Document provided by Former Deputy Director Interview, Nat'l Counterintelligence & Sec. Ctr., 2 (Oct. 8, 2020).

[redacted]

[redacted]

[redacted]

2. (U) NCSC Conducts Several Duties Not Assigned in Statute due to Perceived IC Need

(U) In addition to the statutorily-required duties mentioned above, NCSC engages in several activities that are not explicitly assigned in statute. Officials had differing perspectives on the extent to which NCSC should be operating in these areas.

i. (U) *Facilitating Collaboration and Coordination*

(U) The 2002 Counterintelligence Enhancement Act does not explicitly direct NCSC to facilitate collaboration and coordination across the IC, USG, and academia and private sector; the only statutory requirement to facilitate collaboration is for the NACIPB.[604] However, NCSC officials said that this was an important "gap" that needed to be filled, and they now see this as a core mission.[605] Several other CI officials agreed that NCSC has a vital role to play in this space.[606]

(U) Mr. Evanina told the Committee that establishing systematic two-way information sharing capabilities between the IC, NT-50 agencies, state and local governments, the private sector, and academia is a key role. He added that NCSC also coordinates national efforts and, where appropriate, participates in efforts to counter FIE threats.[607] One CI official told the Committee that NCSC is like a "central brain" for CI.[608] Another NCSC official told the Committee that NCSC is

---

601 [redacted]

602 **(U)** *Id.*

603 [redacted]

604 **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021).

605 **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022); *see also* Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020).

606 [redacted]

607 **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 5 (June 3, 2020).

608 [redacted]

[redacted]

[redacted]

the "connective tissue" between IC components,[609] which enables NCSC to identify trends and shape reporting[610] and to be the "voice of the IC" for CI.[611] [redacted]

(U) Multiple previous CI reviews have also identified the need for better collaboration and coordination across the IC and USG on the CI mission. The 2005 Iraq WMD Commission recommended that the NCIX de-conflict and coordinate operational CI activities both inside and outside the United States.[615] The 2009 CI Review Group found that, while individual components of the IC may have vigorous CI programs focused primarily on their unique missions, there is inadequate attention to "horizontal" or cross-cutting aspects of CI within the IC.[616]

(U) NCSC can also bring NT-50 agencies, acquisition professionals, state and local leadership, contractors, and others together to try to solve a problem.[617] NCSC highlighted efforts to enhance engagement with federal, state, local, tribal, and territorial partners beyond the IC who need assistance strengthening their protective posture.[618] One NCSC official noted, for example, that NCSC's convening abilities are particularly important for "non-traditional" CI activities such as protecting the supply chain from FIE exploitation. NCSC highlighted its efforts to establish SCRM capabilities across the IC and to serve as a leading voice in USG-wide SCRM policy and programs to protect key U.S. supply chains for critical technologies.[619] [redacted]

---

609 **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).
610 **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).
611 **(U)** Interview with Former Nat'l Counterintelligence & Sec. Ctr. Official (Oct. 9, 2020).
612 [redacted]
613 **(U)** *Id.*
614 **(U)** *Id.*
615 **(U)** 2005 WMD FINAL REPORT at 491.
616 **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 2-3).
617 **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).
618 [redacted] NAT'L COUNTERINTELLIGENCE & SEC. CTR., NCSC 2024: A VISION OF THE FUTURE 1 (May 26, 2021).
619 **(U)** *Id.*
620 [redacted]

[redacted]

[redacted]

(U) Another example of NCSC bridging the divide between IC entities, NT-50s, and industry is critical infrastructure. One NCSC official cited NCSC's work to establish a Critical Infrastructure Task Force, comprised of USG and industry leaders across 17 critical infrastructure sectors,[621] as vital for pulling together related activities into one coherent effort.[622] [redacted]

[redacted] Despite the importance of this role, NCSC faces several challenges. [redacted]

[redacted] Due to the lack of clear authorities to convene campaigns and ensure appropriate IC participation, NCSC officials told the Committee that Congress should consider clarifying NCSC's "convening authority" provisions. [redacted]

---

[621] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Deputy Dir. (Oct. 29, 2020).

[622] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).

[623] [redacted]

[624] [redacted]

[625] [redacted]

[626] [redacted]

[627] **(U)** *Id.*

[redacted]

[redacted]

Second, several officials have argued that the newly-established NCITF may obviate some of the need for NCSC to convene inter-agency CI or security working groups or initiatives going forward. [redacted] Thus, NCITF would benefit from a firmer legislative foundation in order to lead CI campaigns.[634]

(U) Third, some IC entities actively or passively oppose NCSC playing a convening role. [redacted] This has resulted in NCSC being less productive than it could be on certain topics.[635]

ii. **(U)** *Developing and Maintaining Databases*

(U) Another duty not spelled out in statute is NCSC's development and maintenance of CI databases. Currently, NCSC maintains several IC databases and recently established a database directorate to house its various database projects.

---

628 [redacted]

629 [redacted]

630 **(U)** *Id.*

631 **(U)** *Id.*

632 [redacted]

633 [redacted]

634 **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

635 **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021).

[redacted]

[redacted]

However, NCSC and the CI community more broadly do not have a clear vision of which databases NCSC should be responsible for developing and maintaining. [redacted] The inverse is also true; other IC agencies have likely developed databases that NCSC may be better positioned to manage.

[redacted]

(U) Other CI officials have pointed out that NCSC plays an important role in this space. One former NCSC official told the Committee that when there is a need for information sharing and no single agency is willing to do it, NCSC can step in and fulfill that function.[640]

[redacted]

636 [redacted]
637 [redacted]
638 [redacted]
639 **(U)** *Id.*
640 **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr.; Former Nat'l Intelligence Officer (Dec. 18, 2020).
641 [redacted]
642 [redacted]

[redacted]

[redacted]

[redacted] NCSC also manages the USG's Continuous Evaluation system for security clearances as part of its security mission.[644]

[redacted]

[643] [redacted]

[644] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 6 (June 3, 2020).

[645] [redacted]

[redacted]

[redacted]

C. (U) RESOURCES AND STAFFING

Staffing and resource constraints impact NCSC's ability [redacted]

(U) The Committee acknowledges that budget constraints are an issue across the IC and the USG; this section simply highlights what NCSC officials and others have described as a limiting factor in effectively addressing and mitigating the FIE threats identified earlier in the report.

1. (U) Key NCSC Duties are Limited due to Staffing and Resource Constraints

[redacted]

While NCSC's outreach efforts have grown over the past several years, [redacted]

---

646 [redacted]

647 [redacted]

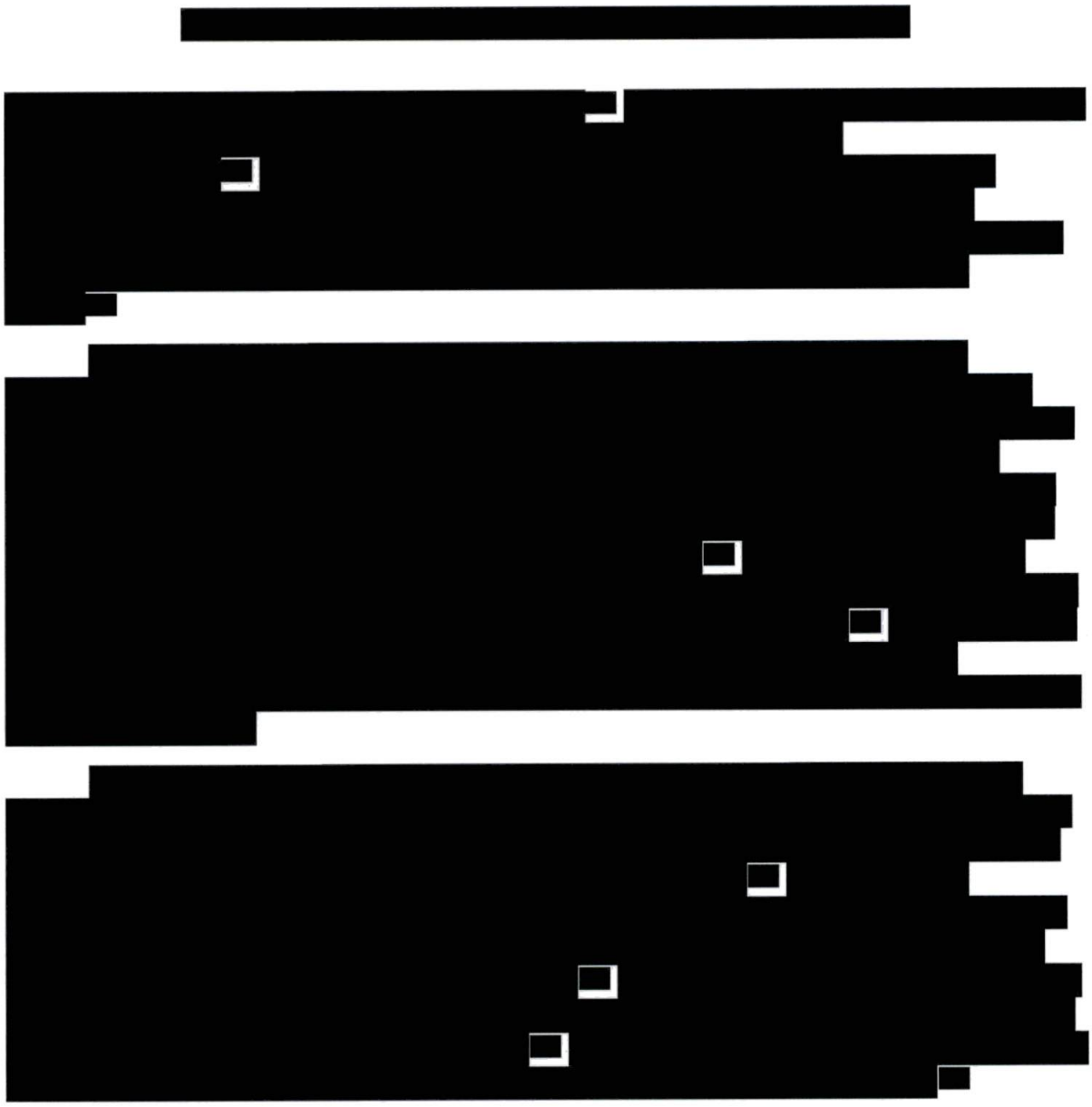
648 [redacted]

649 [redacted]

650 **(U)** *Id.*

651 [redacted]

[redacted]



[redacted]

652 [redacted]

653 [redacted]

654 [redacted]

655 [redacted]

656 **(U)** *Id.*

657 [redacted]

658 **(U)** *Id.*

659 **(U)** *Id.*

660 **(U)** *Id.*

[redacted]

[redacted]

2. (U) NCSC's Staff Composition is Appropriate

[redacted] NCSC officials indicated that its current mix of permanent staff (cadres), joint-duty staff (detailees), and contractors was appropriate; however, the NCSC staff is comprised entirely of IC employees, [redacted] Those same officials indicated that the mix of staff from the various IC agencies was also appropriate—although they noted that has not always been the case.[662] [redacted]

[redacted] One NCSC official told the Committee that NCSC does not want to "stack" personnel from any one agency and that it is important to have broad representation from across the IC.[665] The NCSC chart on the next page shows the joint-duty breakdown by IC agency as of November 2021.[666]

---

[661] [redacted]

[662] **(U)** *Id.*

[663] [redacted]

[664] **(U)** *Id.* at 6.

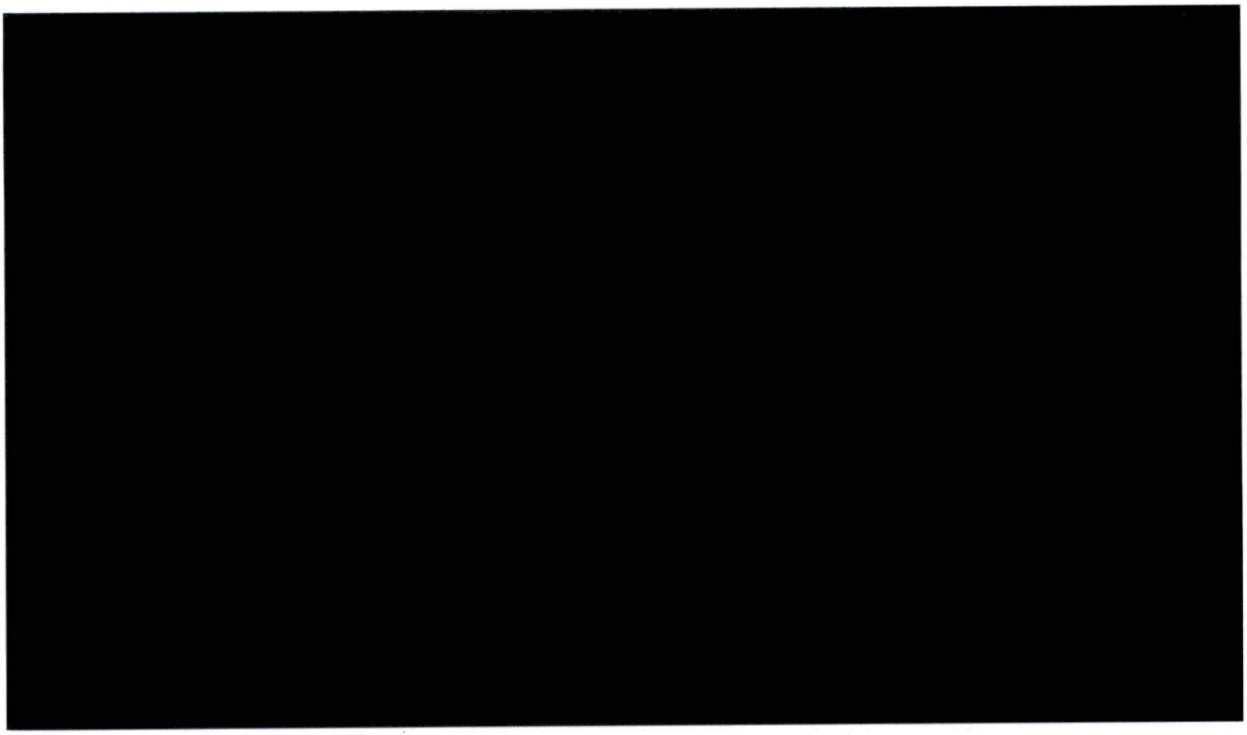
[665] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Deputy Dir. (Oct. 29, 2020).

[666] **(U)** Email from Office of Legislative Affairs, Nat'l Counterintelligence & Sec. Ctr., Office of the Dir. of Nat'l Intelligence to Staff, S. Select Comm. on Intelligence (Nov. 23, 2021).

[redacted]

[redacted]

(U) Graphic G: NCSC Joint-Duty Staff, by Agency (as of 23 Nov 2021)



3. (U) Change in NCSC Staffing Over Time

[redacted] The Committee also reviewed ODNI Congressional Budget Justification Books to analyze trends of full time employees (FTEs) per fiscal year, from FY 2012 to the present. In FY 2012, ODNI data indicated that NCSC [redacted]. In FY 2022, ODNI [redacted]. Then-Vice Chairman Warner asked then-NCSC Director Evanina, "What do you need personnel-wise or asset-wise to be able to more effectively take on [the CI] challenge?"[667] Mr. Evanina responded, "Prefacing that, Senator, with the big picture that, as the governance person of counterintelligence resources across the government, no resources have moved. We've been flat across every agency. . . . My agency specifically, I'm not even flat. I'm significantly reduced."[668]

---

[667] [redacted] *Closed Oversight Hearing on Counterintelligence with NCSC, FBI, and CIA, Before the Senate Select Committee on Intelligence*, 116th Cong. (Dec. 1, 2020) (testimony of William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr.).

[668] (U) *Id.*

[redacted]

[redacted]

(U) Graphic H: FTE Staffing Levels for NCSC, NCTC, and NCPC, Fiscal Years 2012-2022



4. (U) NCSC's Hiring Procedures Take Time

[redacted] NCSC, like every other IC agency, has to deal with staffing challenges, such as hiring and maintaining a workforce with security clearances, that hinder its ability to bring on staff. NCSC, however, faces several unique staffing challenges owing to its position as a Center within ODNI. For instance, several NCSC officials described how the approval process for cadres and detailees is time consuming—it is a "nonstop challenge."[669] One NCSC official told the Committee that it can take more than two months to bring on a detailee and between 12 and 18 months to hire an external candidate, leading some candidates to seek a position elsewhere.[670] The bureaucratic hurdles to staffing include having ODNI approve Memorandums of Understanding between NCSC and other IC agencies.[671]

[redacted] Mr. Evanina and other NCSC officials explained that NCSC does not have hiring authority separate from ODNI, thus requiring NCSC to get ODNI's approval for each hire. Mr. Evanina also mentioned [redacted] that NCSC could use

---

[669] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Deputy Dir. (Oct. 29, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[670] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).
[671] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).

[redacted]

[redacted]

additional legal support.[672] Additional legal support could both decrease the time it takes to usher people through the staffing approval process and assist NCSC with other aspects of its work.

5. (U) NCSC's Budget is Small Relative to its Mission

[redacted] NCSC's budget is small relative to its mission and is controlled by ODNI. Yet ODNI has not requested any substantial growth for NCSC's budget or FTEs, nor has Congress provided it. The Committee reviewed ODNI's Congressional Budget Justification Books to analyze budget trends over the past 10 years for the three ODNI centers: NCSC, NCTC, and NCPC. While NCSC's budget submissions during this time period reflect an overall increase in NCSC spending, some of the increases are directed for specific programs [redacted] do not reflect a true NCSC budget increase.[673] Mr. Evanina, for example, told the Committee that while NCSC's budget has increased over the past few years, [redacted]

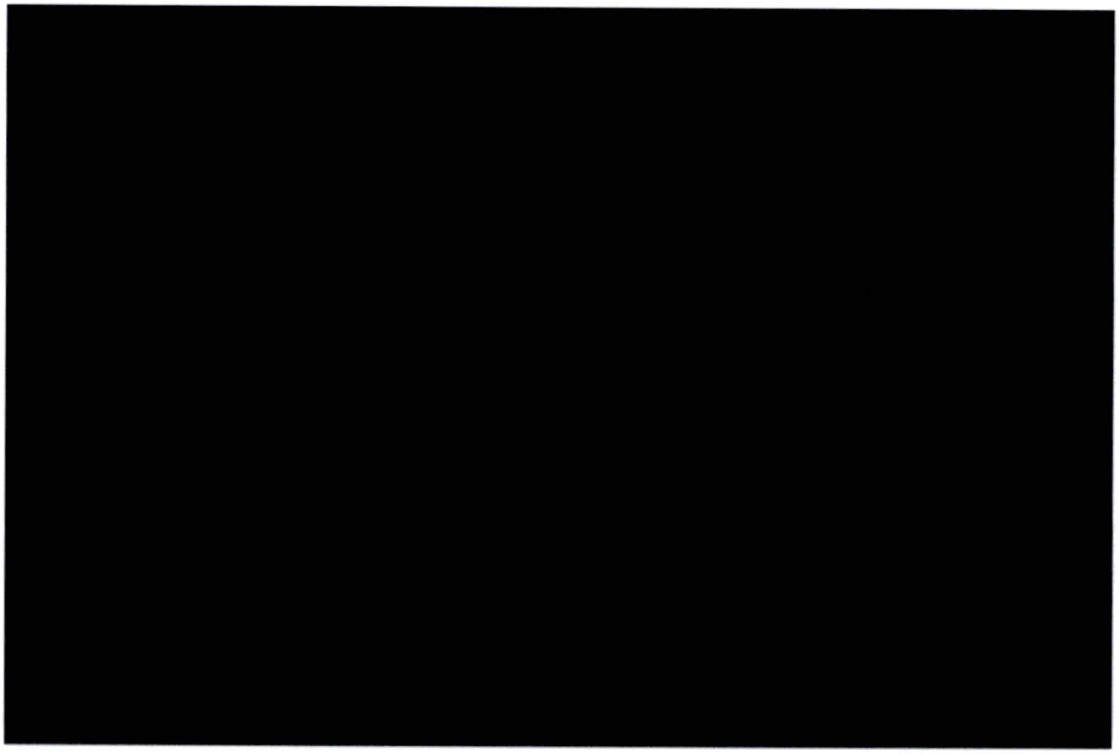
[redacted]

[672] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020).
[673] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020); Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021).
[674] [redacted]
[675] **(U)** *Id.*
[676] [redacted]

[redacted]

[redacted]

[redacted] **Graphic I: ODNI Centers' Budgets, Fiscal Years 2012-2022**



(U) Mr. Evanina, during testimony at a 2020 Committee hearing on CI issues, also noted the disparity in CI and CT spending:

> [redacted] Congress was very instrumental in surging resources subsequent to 9/11. . . . [redacted]

[redacted] He ended by saying: "What we are looking for as we are seeing enlightenment to the counterintelligence threat, we have not seen the same tide come in with new resources."

[redacted] Finally, ODNI controls NCSC's budget because NCSC is a Center rather than an independent agency or department. [redacted]

677 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

678 [redacted]

[redacted]

[redacted]

D. (U) LOCATION AND STRUCTURE

(U) As an ODNI center, NCSC is exclusively part of the IC: its authorities stem from Title 50 and it is funded entirely through the NIP. However, as previously explained, NCSC's mission is not entirely clear; NCSC conducts activities pertaining to both the traditional CI and the strategic CI mission sets and serves stakeholders throughout the IC, NT-50 agencies, and in academia and the private sector. This section highlights the positives and negatives of NCSC's location within ODNI and its structure as an IC-based, NIP-funded entity. This section also highlights several USG entities that officials have suggested may fit well within an independent National Counterintelligence and Security Agency focused on the strategic CI mission.

1. (U) NCSC Experiences Drawbacks and Benefits as an ODNI Center

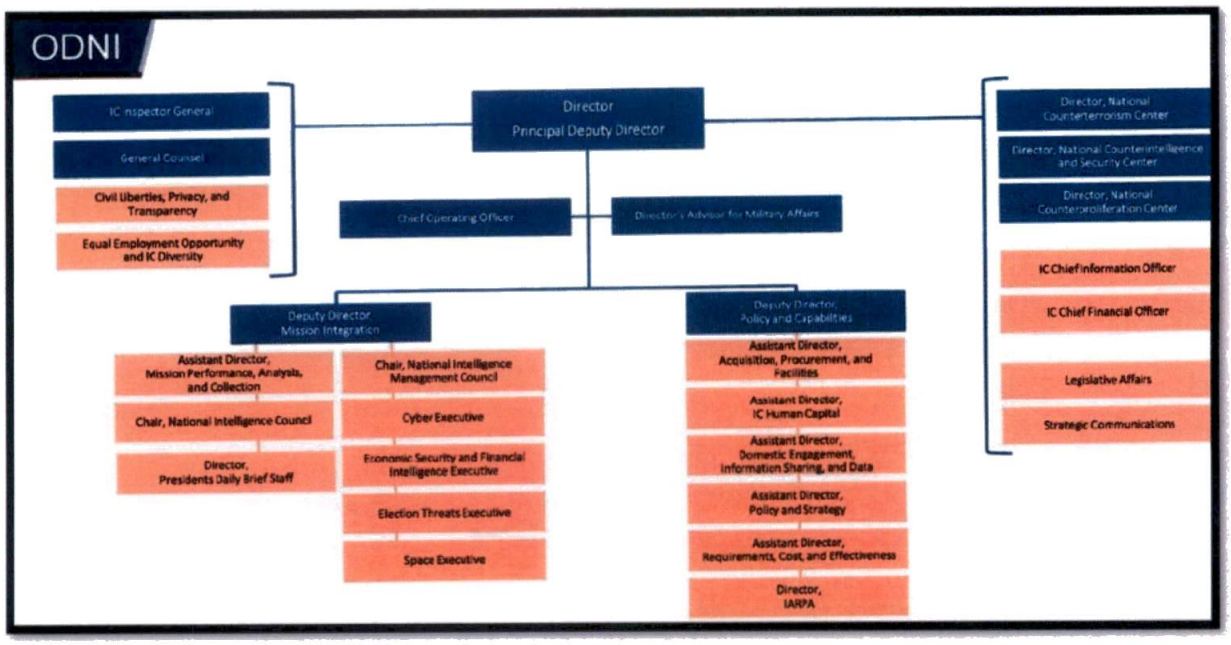
(U) As explained in Appendix A, Congress originally established ONCIX, NCSC's precursor, as an independent entity within the IC.[679] Congress later incorporated ONCIX into ODNI after ODNI's establishment in 2004.[680] When NCSC was established in 2014, DNI Clapper left NCSC under direct ODNI control. NCSC, as shown in the graphic below, is now one of three mission centers nested under ODNI, along with NCTC and NCPC. As a mission center, NCSC serves both as the functional National Intelligence Manager for CI (NIM-CI) and as a mission integrator for CI.[681]

[679] **(U)** *See* the "Evolution of CI" section of this report.
[680] **(U)** *Id.*
[681] **(U)** *Who We Are*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE (Feb. 21, 2020).

[redacted]

[redacted]

(U) Graphic J: ODNI Organizational Chart as of January 2022



(U) Various NCSC officials have noted that NCSC's organizational location within ODNI impacts its ability to carry out the strategic CI mission and to support entities outside the IC. Consequently, several current NCSC officials believe that NCSC should possibly become independent of ODNI.[682] Mr. Evanina stated that "it's the only way we survive."[683] He attributed his success as Director of NCSC to the trust, partnerships, and value-add that he and his team provided to the rest of the IC over time, but noted that this is perishable and relationship-dependent.[684] In contrast, other officials feel that NCSC's current placement as a center under ODNI is manageable and comes with positive aspects.

(U) *Drawbacks of Remaining within ODNI*

(U) First, multiple NCSC officials and other CI experts believe that ODNI has historically not valued CI and does not truly understand the strategic CI mission. In 2005, the Iraq WMD Commission considered ONCIX's placement within ODNI to be a "useful step."[685] However, the Commission also noted that ONCIX would need "all of the DNI's authorities for counterintelligence—particularly authority over the FBI's counterintelligence operations"—for this move to be more

---

[682] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[683] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[684] **(U)** *Id.*
[685] **(U)** 2005 WMD FINAL REPORT at 490.

[redacted]

[redacted]

than "window dressing."[686] Yet, such change never came to pass.[687] According to the 2009 INSA review *Counterintelligence for the 21st Century*, "CI—with the exception of cyber security aspects—was, quite frankly, not a priority for the first two Directors of National Intelligence."[688] The INSA review noted that the ability of NCSC's precursor to influence IC policy and resources "to any appreciable degree" was highly dependent on support from ODNI—and as of 2009 "this support ha[d] been inadequate."[689] The report added that locating NCSC within ODNI could have been a constructive change had the DNI "chosen to use his authorities to exert greater leverage over CI elements of the IC."[690] However, NCSC leadership and that of its precursor have "largely been disconnected from DNI, both physically and bureaucratically, which has further complicated its efforts to exert influence over CI policy across the agencies."[691]

[redacted] The situation has not changed much since ODNI's creation. Mr. Evanina told the Committee [redacted]

(U) Several current and former NCSC officials largely concurred with Mr. Evanina's assessment. [redacted]

---

[686] **(U)** *Id.* at 491.
[687] **(U)** *See* "Duties and Authorities" section of this report.
[688] **(U)** 2009 INSA CI REPORT at 5.
[689] **(U)** *Id.*
[690] **(U)** *Id.*
[691] **(U)** *Id.*
[692] [redacted]
[693] **(U)** *Id.*
[694] [redacted]
[695] [redacted]
(The Committee was unable to corroborate this claim).
[696] [redacted]
[697] **(U)** *Id.*

[redacted]

[redacted]

[redacted] Second, NCSC's location within ODNI may hinder its freedom of maneuver. [redacted]

[redacted] Third, as noted in the prior section, NCSC's placement within ODNI has hampered its ability to quickly and efficiently bring in staff. A large portion of NCSC's workforce consists of detailees, and NCSC does not have hiring authority separate from ODNI.[703] Mr. Evanina told the Committee that NCSC is not able to hire anyone without ODNI's approval, and NCSC once struggled [redacted]

---

698 [redacted]
699 **(U)** *Id.*
700 [redacted]
701 [redacted]
702 [redacted]
703 **(U)** *Id.*
704 **(U)** *Id.*
705 **(U)** *Id.*
706 **(U)** *Id.*
707 **(U)** *Id.* [redacted]
708 [redacted]
709 **(U)** *Id.*

[redacted]

[redacted]

(U) *Benefits of Remaining within ODNI*

(U) Officials also noted several benefits of remaining part of ODNI. First, being part of ODNI provides NCSC with prestige and access that NCSC may not otherwise enjoy. [redacted]

(U) Second, as part of ODNI, NCSC can use ODNI's administrative systems—namely its human resources systems—which would be expensive and time consuming to develop and maintain on its own.[717] Mr. Evanina emphasized that this would be a major drawback.[718]

(U) Finally, NCSC officials noted that NCSC's status as an ODNI Center gives it access to highly sensitive classified intelligence through classified IC

---

[710] [redacted]
[711] [redacted]
[712] [redacted]
[713] [redacted]
[714] [redacted]
[715] [redacted]
[716] [redacted]

[717] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Nov. 13, 2020); Interview with Nat'l Counterintelligence & Sec. Ctr., Counterintelligence Directorate (Nov. 17, 2020).

[718] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[redacted]

[redacted]

holdings. [redacted]

2. (U) Officials Disagree Over Whether NCSC Should Remain Exclusively Within the IC

(U) As noted previously in this report, there is debate about whether strategic CI is an IC-only responsibility, a whole-of-government responsibility, or a whole-of-society responsibility. As a result, there is a parallel debate about the proper placement of NCSC: Should NCSC be located entirely within the IC, entirely outside the IC, or straddled across both worlds?

(U) At the moment, CI remains predominantly an IC responsibility.[720] Only IC entities have operational CI authorities,[721] and few NT-50 agencies or non-USG entities have "CI awareness" programs.[722] Moreover, NCSC is entirely NIP-funded and, as a result, is located entirely within the IC.[723]

(U) Some former and current IC officials consider CI to be primarily an IC responsibility and therefore believe that NCSC should remain a Center at ODNI. Ms. Van Cleave believes that CI is an inherently IC responsibility and should remain exclusively within the purview of the IC, although she recognizes that NT-50s, state and local governments, academia, and the private sector have an important role to play in ***security***.[724] Several officials within ODNI, including Mr. Orlando,[725] also take the view that CI is an inherently IC function.[726]

(U) Other officials disagree that strategic CI should remain an IC-only responsibility. Mr. Evanina, for example, believes that strategic CI is a whole-of-society responsibility.[727] He also believes that his successors should think of NCSC as a government-wide national security organization and not as an IC-only entity.[728] Mr. Bryant, in testimony before this Committee in 2010, said that CI "must become the practice of the entire USG—not just the IC—as well as those elements of the public and private sectors charged with holding and protecting

---

719 [redacted]

720 **(U)** *See* Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities (June 3, 2020).

721 **(U)** *Id.*

722 **(U)** *Id.*

723 **(U)** *Id.*

724 **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Oct. 6, 2020).

725 **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022).

726 **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020); Interview with Office of the Dir. of Nat'l Intelligence (Oct. 5, 2021).

727 **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

728 **(U)** *Id.*

[redacted]

[redacted]

sensitive information and leading-edge technologies."[729] Several current NCSC officials have also repeatedly told the Committee that NT-50s, academia, and the private sector should be considered part of the CI community, and noted that several NT-50s, particularly HHS, already have robust CI programs.[730]

(U) The question of whether strategic CI is an IC-only responsibility or whether it is a whole-of-government responsibility has implications for the optimal placement of NCSC. If strategic CI is an IC-only responsibility, then various officials believe that NCSC should probably remain within the IC. On the other hand, if strategic CI is a whole-of-government responsibility—that is, if NT-50s are expected to have CI roles and responsibilities—then other officials believe that NCSC may be better structured partially or entirely outside the IC. This question must be answered first, before any decision about NCSC's optimal location can be made.

3. (U) Several Officials Have Called for the Establishment of an Independent National Counterintelligence and Security Agency

(U) Similarly, there is no consensus on NCSC's ideal structure given the ongoing debate about its mission, duties and authorities, and resources; various models could work. However, in conversations with this Committee, Mr. Evanina has proposed establishing an independent National Counterintelligence and Security Agency (NCSA) responsible for the strategic CI mission and focused on protecting the United States as a whole.[731] While an exhaustive framework for a potential NCSA is beyond the scope of this review, Mr. Evanina and several other officials have identified several key elements an NCSA could have.

(U) *Potential Elements of an Independent NCSA*

[redacted] Members of this Committee have asked whether the United States should establish a CI entity similar to the United Kingdom's MI5.[732] No one who spoke with the Committee during this review believed that MI5 was the appropriate model for the U.S. CI enterprise as a whole—although the Committee believes that MI5 may have more applicability to an independent NCSA focused more narrowly on the strategic CI mission.

(U) Officials cited two main reasons why MI5 may not be a good model for the CI mission as a whole. First, MI5 is tasked with both the traditional and

---

[729] **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 2).

[730] **(U)** Interview with Nat'l Counterintelligence & Sec. Ctr., Office of the Exec. Dir. (Feb 4, 2022).

[731] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[732] [redacted] *Closed Oversight Hearing on Counterintelligence with NCSC, FBI, & CIA Before the Senate Select Comm. on Intelligence*, 116th Cong. (Dec. 1, 2020).

[redacted]

[redacted]

strategic CI missions.[733] Yet, given the decentralized nature of the IC in the United States, several officials emphasized that traditional CI activities should remain within individual IC or NT-50 entities to protect their operations.[734] As Mr. Evanina noted in his written response to this Committee, traditional CI "has resided and should remain within the separate cognizance and competence of units within the elements of the IC and the Department of Defense, which have well-established and effective programs, processes, and objectives."[735]

(U) Second, MI5 lacks law enforcement authorities. That is, MI5 cannot arrest, detain, or charge any individual accused of a crime.[736] Instead, MI5 has established strong relationships with national and regional police units and has a representative embedded in every police unit in the United Kingdom. MI5 conducts investigations collaboratively with police partners, who make independent decisions to use their authorities to arrest, detain, or charge.[737] NCSA could similarly establish relationships with the FBI and state and local law enforcement entities to arrest, detain, and charge individuals when necessary. [redacted] Mr. Orlando told the Committee that if Congress were to establish an MI5-type entity consolidating both traditional and strategic CI, it would need to include law enforcement authorities "or the fundamental problem would not be addressed."[739]

(U) Although this Committee does not believe that MI5 is a good fit for U.S. CI broadly, several officials have indicated that it may be instructive for the strategic CI mission more narrowly.[740] That is, all strategic CI duties, authorities, and resources could be consolidated within an independent NCSA to include collection, analysis, production, and dissemination of strategic CI intelligence, as well as conducting strategic CI activities (i.e., defensive and offensive CI

---

[733] **(U)** Briefing with U.K., Security Service (June 22, 2021).

[734] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021); Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 3 (June 3, 2020).

[735] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 3 (June 3, 2020).

[736] **(U)** Briefing with U.K., Security Service (June 22, 2021).

[737] **(U)** *Id.*

[738] [redacted]

[739] **(U)** *Id.*

[740] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (Feb. 15, 2022); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).

[redacted]

[redacted]

operations).[741] This consolidation could be beneficial because strategic CI "does not fit comfortably within the existing architecture and [traditional CI] approach to counterintelligence as it has developed within the United States."[742]

(U) To carry out the strategic CI mission, officials have suggested that an NCSA, should it be established, may need to incorporate several other existing USG entities that play an important role in this space. Although not an exhaustive or definitive list, officials have proposed various contenders for consideration to include[743]:

- **(U) NCITF.** NCITF is an FBI Headquarters element, co-chaired by the FBI, [redacted]

[redacted]

[741] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022). (Mr. Evanina told that Committee that an independent NCSA should still rely on other IC elements to collect original intelligence, but that NCSA should be given full access to that intelligence—similar to the levels of access enjoyed by the NIC—which it could then use to conduct in-depth strategic analysis and interagency damage assessments).

[742] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 1 (2007).

[743] **(U)** This is not a definitive or complete list of USG entities that could or should be incorporated into an independent NCSA responsible for the strategic CI mission; they are simply the ones highlighted by NCSC officials as possible contenders.

[744] [redacted]

[745] [redacted]

[746] **(U)** *Id.*

[747] **(U)** *Id.*

[748] [redacted]

[redacted]

[redacted]

[redacted] the FBI owns domestic operational CI per EO 12333.[758]

- **(U) DCSA.** DCSA is a DOD entity that, despite its name, is not part of the IC.[759] DCSA officials said that they do not have any CI operational or

[749] [redacted]

[750] **(U)** *Id.*

[751] **(U)** *Id.*

[752] [redacted]

[753] [redacted]

[754] [redacted]

[755] [redacted]

[756] [redacted]

[757] [redacted]

[758] **(U)** *Id.*

[759] **(U)** Interview with U.S. Dep't of Def., Def. Counterintelligence & Sec. Agency (May 14, 2021).

[redacted]

[redacted]

investigative authorities, but they engage in CI collection, analysis, and production, as well as functional services.[760]

(U) Through its National Industrial Security Program (NISP), DCSA has sole oversight over the nation's "cleared industrial base"—comprised of 12,500 cleared facilities (approximately 100 of which are universities).[761] Specifically, DCSA works to ensure the trustworthiness of the USG's workforce and the integrity of its cleared contractor support through vetting, industry engagement, CI support, and education.[762] DCSA is also responsible for ensuring the uncompromised nature of the nation's technologies, services, and supply chains.[763]

(U) DCSA's CI Directorate identifies threats to U.S. technology and programs resident in cleared industry and articulates those threats to stakeholders.[764] In some cases, DCSA knows that foreign actors have access to companies in the cleared industrial base, so DCSA works with cleared industry to identify and mitigate these threats. DCSA believes it is the best positioned entity in the USG to do this because of its relationships with cleared companies and its broad network of field offices and field agents.[765] [redacted]

(U) Mr. Evanina said that DCSA could be a good fit for the proposed NCSA because DCSA works on many of the same strategic CI and security issues.[767] [redacted]

---

[760] [redacted]
[761] **(U)** *Id.*
[762] **(U)** *About Us*, DEF. COUNTERINTELLIGENCE & SEC. AGENCY, U.S. DEP'T OF DEF., dcsa.mil/about.
[763] **(U)** Interview with U.S. Dep't of Def., Def. Counterintelligence & Sec. Agency (May 14, 2021.
[764] **(U)** *About Us*, DEF. COUNTERINTELLIGENCE & SEC. AGENCY, U.S. DEP'T OF DEF., dcsa.mil/about.
[765] **(U)** Interview with U.S. Dep't of Def., Def. Counterintelligence & Sec. Agency (May 14, 2021.
[766] **(U)** *Id.*
[767] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[768] [redacted]
[769] [redacted]
[770] [redacted]

[redacted]

[redacted]

- **(U) FMIC.** In its FY 2022 Congressional Justification Book, ODNI noted that it intends to establish a Foreign Malign Influence Center, in accordance with Section 5322 of the National Defense Authorization Act for FY 2020, to serve as the central USG organization for producing coordinated analysis and integrating intelligence pertaining to foreign malign influence. Specifically, ODNI envisions FMIC serving as the key functional and collaboration hub by which to organize, prioritize, and optimize IC activities on foreign malign influence.[771]

  (U) The FMIC would be responsible for establishing analytic production lines based upon defined national priorities as established by policy officials; proposing priorities across the IC for areas of focus related to foreign malign influence; building upon existing partnerships with other agencies, domestic customers, and allied partners by developing releasable information standards and enhancing sharing opportunities by establishing formal protocols; and assessing opportunities to leverage existing or proposed technology solutions that can provide intelligence insight or influence operations.[772]

  (U) If Congress and ODNI determine that CI includes foreign malign influence activities, then there is a case for incorporating the FMIC into an independent NCSA focused on strategic CI. As previously noted, Mr. Evanina and Mr. Orlando argued that foreign malign influence should be part of NCSC's/NCSA's mission set.[773] Mr. Evanina noted that only NCSC/NCSA is poised to truly tackle the foreign malign influence problem set.[774] Mr. Orlando did not oppose the idea of including FMIC.[775]

- **(U) State Department's Global Engagement Center (GEC).** Similarly, if Congress and ODNI determine that CI includes foreign malign influence, there is also a case for incorporating GEC into an independent NCSA focused on the strategic CI mission. Although not part of the IC, GEC's mission is to "direct, lead, synchronize, integrate, and coordinate efforts of the federal government to recognize, understand, expose, and counter foreign state an non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations."[776]

---

[771] **(U)** ODNI FY 2021 CBJB at 5.
[772] **(U)** *Id.*
[773] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr. (May 12, 2021); Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[774] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[775] **(U)** Interview with Mike Orlando, Acting Dir., Nat'l Counterintelligence & Sec. Ctr., (Feb. 15, 2022).
[776] **(U)** *Core Mission & Vision*, GLOBAL ENGAGEMENT CTR., U.S. STATE DEP'T (Feb. 2022).

[redacted]

[redacted]

(U) The Committee did not meet with State officials during this review to get their perspective on a potential merger with NCSC. However, Mr. Evanina explicitly mentioned GEC as a potential contender given its mission.[777]

- **(U) CISA.** If Congress and ODNI determine that CI includes national security cyber responsibilities, there is a case for incorporating CISA into a future independent NCSA focused on strategic CI. Although not part of the IC, CISA's mission is to lead "the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services,"[778] as well as to work with "businesses, communities, and government at every level to help make the nation's critical infrastructure more resilient to cyber and physical threats."[779]

  (U) Current and former CISA officials did not respond to the Committee's repeated requests for an interview, so the Committee does not know their position on this issue. [redacted]

[777] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Nov. 17, 2020).
[778] **(U)** *About CISA*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC.
[779] **(U)** *Id.*
[780] [redacted]
[781] [redacted]
[782] [redacted]

[redacted]

[redacted]

(U) CONCLUSION AND RECOMMENDATIONS

(U) The U.S. CI enterprise is not postured to confront the whole-of-society FIE threat landscape facing the country today. CI as a mission first arose throughout the IC after World War II to defend IC operations, and the United States is still living with the legacy of that structure. Although that structure may have been appropriate when FIEs were primarily targeting information held by the IC and other national security entities, today's FIEs dedicate enormous energy and resources to acquiring not only sensitive state secrets, but also information from NT-50s and non-USG entities—which are significantly more vulnerable targets than the IC. There is thus a "disconnect" between the location of valuable information relevant to U.S. national security interests and what the U.S. CI enterprise is tasked with protecting.

(U) As more and more sensitive information has moved outside the protective walls of the IC, CI as a mission has struggled to adapt. The very definition of CI—both in terms of the types of activities FIEs conduct to target the United States, as well as the types of U.S. efforts to counter those activities—is now murky and no longer clearly reflects the reality on the ground. For instance, various non-IC entities have established or are establishing "CI programs," but their CI activities conceptually overlap in many ways with the security mission and do not conform to the traditional understanding of CI activities—namely efforts to identify, deceive, exploit, disrupt, or protect against espionage. The USG must determine which FIE and USG activities fall within the CI mission set today, draw clear boundaries between the CI and security missions and clarify where "CI awareness" activities fall, and clarify the roles and responsibilities of USG and non-USG entities tasked with carrying out the CI and/or security missions.

(U) This distinction is important because it implies different national security models; CI measures deal directly with FIE activities, whereas security programs indirectly defend against FIE actions by minimizing vulnerabilities. Thus, under an expansive CI enterprise model, the entire USG and potentially non-USG entities would bear responsibility for dealing directly with FIE activities. On the other hand, a more traditional CI enterprise model would be based exclusively on the IC—but could nevertheless require non-IC entities to be responsible for defensive security measures to identify and mitigate vulnerabilities.

[redacted] In either case, tactical, one-off responses are no longer sufficient to address the current FIE threat landscape; a strategic response is required. Yet, the U.S. CI enterprise has not fully pivoted to confront this new reality. [redacted]

[redacted]

[redacted]

[redacted]

(U) Moreover, CI as a discipline has traditionally been undervalued in the USG. Back in 2005, the Iraq WMD Commission, for example, noted that CI has been "plagued by a lack of policy attention and national leadership" and is largely neglected by policymakers and the IC. The Commission also stated that CI actually lost stature after September 11, as the USG turned its attention to CT.[784] The 2009 INSA report *Counterintelligence for the 21st Century* noted that CI was not a priority for their first two DNIs.[785] Mr. Evanina added that agency heads often assign lower priority to CI divisions and programs than to offensive mission requirements.[786] As of July 2022, the Administration has not yet officially nominated a permanent NCSC Director, despite the position being vacant for over a year.

(U) The impact of all these challenges is clear: foreign adversaries compromise U.S. assets across the globe, acquire billions of dollars a year in U.S. research and technology, jeopardize the competitiveness of U.S. companies and the economic dominance of the United States, steal sensitive PII on USG employees and U.S. citizens, and interfere in domestic affairs. The USG cannot allow this situation to continue without serious repercussions for U.S. national security.

(U) Congress last tried to seriously reform CI statutes in 2002, when it passed the Counterintelligence Enhancement Act and created NCSC's precursor to try to better integrate the CI silos scattered across the IC. The Committee believes that NCSC has made progress in achieving that goal. However, NCSC lacks the necessary clarity of mission, sufficient authorities and resources, and an optimal location/structure to truly lead U.S. CI and to execute the strategic CI mission.

[redacted] It is time for Congress to take another hard look at the ability of the U.S. CI enterprise in general and NCSC in particular to confront today's FIE threat landscape. As Vice Chairman Rubio noted during a hearing on CI in 2020: "the IC may need a fundamental rethink of its counterintelligence enterprise."[787] As Ms. Van Cleave told the Committee: "the USG does not have the right 'business model' for CI; rather than being strategic, forward-looking, and proactive, U.S. CI is tactical, reactive, and defensive."[788] Mr. Evanina has similarly

---

[783] [redacted]

[784] **(U)** 2005 WMD FINAL REPORT at 487.

[785] **(U)** 2009 INSA CI REPORT at 5.

[786] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020).

[787] [redacted] *Closed Oversight Hearing on Counterintelligence with NCSC, FBI, and CIA Before the S. Select Comm. on Intelligence* (Dec. 1, 2020).

[788] **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Oct. 6, 2020).

[redacted]

called for "a dramatic new construct to ensure adequate and enhanced coordination of a holistic CI program for the United States."[789]

(U) There is no easy "fix" to U.S. CI, nor is there one single way in which NCSC could be reformed to better serve as head of national CI. If Congress and ODNI determine that NCSC should focus exclusively on better operationalizing traditional CI activities, then NCSC may not need additional authorities or resources, and a structural change to the Center may not be necessary. ***Yet, there must be an "owner" for strategic CI to address the FIE landscape facing the nation today, and NCSC is currently the only USG entity positioned to lead this mission.*** If Congress and ODNI assign the strategic CI mission to NCSC, then bigger changes to the Center may be warranted. Owning strategic CI would require sufficient authorities and resources to enable NCSC to successfully develop a strategic CI program to bring together all the means of execution for strategic CI priorities. In addition, Congress may want to consider whether NCSC can best carry out the strategic CI mission as a Center within ODNI, or whether such a mission requires the establishment of an independent NCSA spanning the IC and NT-50s universe.

(U) These are not new challenges or debates. Various CI experts have been calling for such reforms for almost 20 years. For example, in 2005 the Iraq WMD Commission noted that:

> **(U)** Organizational change is not a panacea for counterintelligence, but it is necessary. Today there is no individual or office that can impose Community-wide counterintelligence reform or hold individual agencies accountable for fulfilling national counterintelligence requirements. This should change, and we believe that the obvious candidate for leadership is an empowered [NCSC].[790]

(U) This Committee recognizes that any major change to the CI enterprise will be difficult and time consuming, and that various members of the USG may fiercely resist such changes. However, the USG has made big, bold changes before. After the terrorist attacks of September 11, 2001, Congress reorganized the U.S. national security enterprise to better confront terrorism. But more importantly, Congress helped to reorient the CT mission away from reactive, defensive efforts focused on figuring out who conducted a specific terrorist attack towards a proactive, offensive posture focused on stopping terrorists before they strike.[791] It is

---

[789] **(U)** Letter from William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr., to Sen. Marco Rubio, Acting Chairman, S. Select Comm. on Intelligence, and Sen. Mark Warner, Vice Chairman, S. Select Comm. on Intelligence, regarding Unclassified Response to Questions on CI Capabilities 2 (June 3, 2020).

[790] **(U)** 2005 WMD FINAL REPORT at 491.

[791] **(U)** Michelle Van Cleave, *The Question of Strategic Counterintelligence: What Is It, and What Should We Do About It*, 51 STUDIES IN INTELLIGENCE 1, 4 (2007).

[redacted]

time for CI to undergo a similar revolution and to receive the national-level attention it deserves.

(U) SSCI Recommendations

Definitions

1. The Executive Branch should develop and adopt, and Congress should codify, a consistent USG-wide definition of CI that:
    a. Reflects today's FIE threat landscape; and
    b. Delineates CI and security.
2. The Executive Branch should develop and adopt, and Congress should codify, related definitions to include strategic CI and offensive CI.

The CI Enterprise

1. NCSC, in consultation with ODNI, should identify the conceptual boundaries of the CI enterprise, including by identifying key stakeholders (e.g., which entities are members, partners, beneficiaries, etc.); outline stakeholders' CI and security roles and responsibilities; and clarify their relationship with NCSC.
2. NCSC, in consultation with ODNI, should determine what role each element of the IC should play in protecting non-USG entities that FIEs target for their research, technologies, data, and IP.
3. NT-50s should consistently establish "CI awareness" and/or security programs to ensure that USG data and sensitive information are identified and protected.

NCSC's Mission and Structure

4. Congress, in consultation with the Executive Branch, should clarify NCSC's mission and determine what, if any, role it should play in:
    a. Traditional CI;
    b. Strategic CI; and
    c. Offensive CI operations.
5. Congress, in consultation with the Executive Branch, should determine whether NCSC should remain a Center within ODNI or should be established as an independent agency.
6. Congress, in consultation with the Executive Branch, should determine which aspects of the security mission NCSC should retain.
7. Congress, in consultation with the Executive Branch, should consider whether the Director of NCSC/NCSA should be the official Sec/EA.

NCSC's Duties

[redacted]

8. NCSC should develop a strategic plan to conduct vulnerability assessments within the IC, NT-50s, and selected non-USG entities or sectors, and should request resources and authorities necessary to conduct those assessments.
9. NCSC should develop a plan for IC CI outreach to non-IC entities, including:
    a. Identifying IC outreach roles and responsibilities for each element of the IC; and
    b. Identifying and requesting resources and authorities necessary to implement this plan.
10. The USG should consider establishing a dedicated CI R&D fund and a CI R&D board to fund and oversee R&D efforts.
11. NCSC should develop a strategic plan, in consultation with relevant stakeholders, for CI R&D efforts.
12. NCSC should develop a plan for strategic CI training across the IC as well as for NT-50s and non-USG entities.
13. NCSC should establish a clear vision of what, if any, role it should play in developing and maintaining IC databases that support the CI mission.

NCSC's Authorities and Resources

14. Congress or the Executive Branch should provide NCSC with explicit authorities to ensure that NCSC can require appropriate CI entities to participate in NCSC-led efforts in support of the National CI Strategy.
15. If Congress determines that NCSC should own the strategic CI mission, then Congress should provide NCSC with the appropriate authorities and resources necessary to develop and execute a strategic CI program including:
    a. Strengthening NCSC's authorities to determine IC strategic CI budgets.
    b. Considering the establishment of a separate appropriation for NCSC to support NT-50 and non-USG CI programs with strategic CI and/or security objectives and/or clarifying ODNI's ability to transfer NIP resources to NT-50s.
    c. Providing NCSC with authorities to task CI entities with carrying out specific elements of a strategic CI program.

(U) APPENDIX A: EVOLUTION OF CI AUTHORITIES

(U) U.S. CI legal authorities have evolved over time, nearly always in response to public CI failures such as breaches of classified information. From theft of nuclear secrets at the DOE in the 1990s, to the Aldrich Ames and Robert Hanssen arrests, to the OPM breach, to WikiLeaks and Edward Snowden, the USG has responded to these incidents with limited reforms to the CI enterprise. These reforms typically followed after-action reviews and generally targeted the specific CI issue or breach.

(U) In addition, while the USG has conducted several major CI reviews over the past 20 years, those reviews have yet to result in significant reforms necessary to effectively confront the threat landscape facing the United States today. This section outlines key CI authorities and the evolution of those authorities over time. This section also details the findings of key USG-wide CI studies or reviews.

a. (U) National Security Act of 1947 (1947)

(U) The National Security Act of 1947 laid the foundation of the IC by establishing the NSC, the CIA, and the National Security Resources Board. This Act did not explicitly assign to the Director of Central Intelligence (DCI) the responsibility of protecting the United States against foreign intelligence threats.[792] Some national security practitioners indicated that this responsibility, however, was inferred and said that "they regard counterintelligence as a subordinate discipline to intelligence, and therefore inherently a part of the DCI's responsibilities."[793]

b. (U) Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs—U.S. Senate Select Committee on Intelligence Report (1986)

(U) This Committee initiated a "comprehensive review of the capabilities of U.S. CI and security programs for dealing with the threat to the United States from Soviet espionage and other hostile intelligence activities" in 1986.[794] The report underscored the fundamental challenge of the time: "The hostile intelligence threat is more serious than anyone in the Government has yet acknowledged publicly. The combination of human espionage and sophisticated technical collection has done immense damage to the national security."[795] The Committee found that:

- **(U)** "Foreign intelligence services have exploited human and technical vulnerabilities to penetrate some of the most vital parts of our defense,

---

[792] **(U)** National Security Act of 1947, 50 U.S.C. § 3001 et seq. (2018).
[793] **(U)** Michelle Van Cleave, *The NCIX and the National Counterintelligence Mission: What has Worked, What has Not, and Why*, PROJECT ON NATIONAL SECURITY REFORM: CASE STUDIES VOL. 1 (2008).
[794] **(U)** 1986 SSCI REPORT.
[795] **(U)** *Id.* at 3.

[redacted]

intelligence and foreign policy structure, including many Executive Branch agencies and the Congress."[796]

- **(U)** "Authorized (but uncontrolled) disclosures and unauthorized leaks of classified information are so commonplace as to imperil many sensitive programs and operations."[797]
- **(U)** "The classification system is unduly complicated and it breeds cynicism and confusion in those who create and use classified information."[798]

(U) The Committee's report included recommendations for improvements that the Executive Branch had the authority to accomplish. The Committee recognized that the report's recommendations would not be "cost free" but believed that "the U.S. Government has suffered for years from inadequate investment in security countermeasures."[799] The additional expenditures recommended by the Committee for the fiscal year following the publication of the report "would [have] amount to an increase in annual spending for counterintelligence and security of at least $500 million. ... This commitment must continue in the years ahead, when further increases may well be required because of the growing technical, communications and computer security vulnerabilities."[800] At that time, these increases were viewed as "investments" because "the costs of improved security [would] be offset by the gains to the United States in overall U.S.-Soviet balance of military, intelligence, economic, and political capabilities."[801]

(U) Despite the report's findings and recommendations, the Committee later found that the Executive Branch did not implement many of the recommendations for two basic reasons: "Counterintelligence and security had failed to receive sustained attention; and the ideas [recommended in the report] frequently challenged established ways of doing things, cut across bureaucratic lines of responsibility, or required substantial changes in resource allocations."[802]

c. (U) Presidential Decision Directive 24 (1994)

(U) In 1994, the FBI arrested Aldrich Ames, a CIA CI chief who had been spying for the Soviets for nine years. Ames provided comprehensive blueprints of U.S. collection operations against the Soviets, including the identities of clandestine agents he had sworn to protect. At least nine people lost their lives due to his spying.[803] At the time, there was no such job as "head of U.S. counterintelligence";

---

[796] **(U)** *Id.* at 12.
[797] **(U)** *Id.* at 7.
[798] **(U)** *Id.*
[799] **(U)** *Id.* at 9.
[800] **(U)** *Id.*
[801] **(U)** *Id.*
[802] **(U)** *Id.*
[803] **(U)** Michelle Van Cleave, *Foreign Spies are Serious, Are We?*, WASH. POST (Feb. 8, 2009).

[redacted]

[redacted]

no one person was responsible for identifying and responding to FIE threats to U.S. national security or economic well-being. Instead, CI responsibilities were divided among the FBI, the CIA, and the three military services, with no central leadership or overarching structure to unite them. This construct created seams that adversaries could, and did, exploit.[804]

(U) The Ames case sparked a reexamination of U.S. CI, leading the Clinton Administration to issue Presidential Decision Directive (PDD) 24—"U.S. Counterintelligence Effectiveness."[805] PDD 24 noted that threats to the national security of the United States had been significantly reduced by the break-up of the Soviet Union and the end of the Cold War, but that numerous threats to U.S. national interests—such as terrorism, proliferating weapons of mass destruction (WMD), ethnic conflicts, and sluggish economic growth—remained.[806]

[redacted] President Clinton argued that the United States needed to improve coordination of its CI activities. Specifically, President Clinton noted that the IC and Law Enforcement community needed to "improve their understanding of their respective needs and operating practices…to cooperate earlier, more closely, and more consistently on matters in which they both have a separate but parallel interest."[807] Towards that aim, PDD 24 directed the creation of a new national CI policy structure under the auspices of the NSC to coordinate CI policy matters.[808]

(U) This new structure was designed to ensure that all relevant departments and agencies had a full and free exchange of information necessary to achieve maximum effectiveness of the U.S. CI effort and included a National Counterintelligence Policy Board and a National Counterintelligence Operations Board.[809] PDD 24 is the origin of a central government entity responsible for a consolidated inter-agency approach to CI policy, programs, and oversight.[810]

(U) PDD 24 also directed the creation of a new National CI Center to be established by the National CI Policy Board (which replaced the National Advisory Group for CI) with assistance from the DCI, the Director of the FBI, the Secretary of Defense, and the Secretary of State.[811] This Center was to implement interagency CI activities, report to the National CI Policy Board, and serve as the interagency forum for complementary activities among CI agencies. Finally, PDD 24 also

---

[804] **(U)** *Id.*
[805] **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Oct. 6, 2020).
[806] **(U)** Press Release, Pres. William Clinton, White House, U.S. Counterintelligence Effectiveness (May 3, 1994).
[807] **(U)** *Id.*
[808] **(U)** *Id.*
[809] **(U)** *Id.*
[810] **(U)** CONG. RES. SERV., EVOLUTION OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER 4 (2020).
[811] **(U)** *Id.*

[redacted]

[redacted]

required the CIA and FBI to exchange senior managers to "ensure timely and close coordination between the intelligence and law enforcement communities."[812]

d. (U) CI and Security Enhancements Act (1994)

(U) Later the same year, Congress passed the CI and Security Enhancements Act of 1994. This Act was focused primarily on identifying and preventing insider threats posed by individuals such as Ames. For instance, the Act established procedures to govern access to classified information, such as requiring a background investigation for employees wanting to access classified information and establishing minimum requirements governing the scope and frequency of background investigations.[813]

(U) The Act also permitted any authorized investigative agency to request financial records and other financial information from financial agencies and institutions to conduct law enforcement investigations, CI inquiries, or security determinations. The Act also permitted rewards for information concerning espionage and permitted the USG to deny annuities or retired pay to persons convicted of espionage in foreign courts involving U.S. information.[814]

e. (U) The Cox Commission (1998)

(U) In June 1998, after a *New York Times* article reported on China stealing U.S. nuclear secrets, the U.S. House of Representatives created the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China (the Cox Commission).[815] The Cox Commission conducted a six-month investigation examining whether U.S. export controls failed to stop missile technology and nuclear weapon technology transfers to China. According to the Cox Commission, China stole classified information on the most advanced U.S. thermonuclear weapons, giving China "design information on thermonuclear weapons on par with our own."[816] The classified design information included "every currently deployed thermonuclear warhead in the U.S. ballistic missile arsenal," on the neutron bomb, and on a number of U.S. re-entry vehicles.[817]

(U) The Cox Commission made 38 recommendations for actions by Congress and the Clinton Administration,[818] including that:

---

[812] **(U)** Press Release, Pres. William Clinton, White House, U.S. Counterintelligence Effectiveness (May 3, 1994).
[813] **(U)** Counterintelligence & Security Enhancements Act of 1994, 50 U.S.C. § 3381 (2018) (as amended).
[814] **(U)** *Id.*
[815] **(U)** H.R. Rep. No. 105-851, Vol. 1 (1999).
[816] **(U)** *Id.* at ii.
[817] **(U)** *Id.* at iii.
[818] **(U)** *Id.* at 166-77.

[redacted]

[redacted]

1. **(U)** DOE must implement as quickly as possible, and then sustain, an effective CI program;
2. **(U)** Appropriate congressional committees review Executive Branch action on strengthening CI at DOE labs and determine if the Administration was devoting sufficient resources to such efforts; and
3. **(U)** Appropriate departments and agencies conduct comprehensive damage assessments of the strategic implications of the security breaches that have taken place at the national laboratories since the late 1970s.

f. (U) Counterintelligence for the 21st Century and PDD 75 (2000)

(U) In 2000, the USG conducted another CI review which led to PDD 75—U.S. Counterintelligence Effectiveness for the 21st Century, signed on January 5, 2001.[819] This review recognized the changing nature of CI; President Clinton explained that the United States faced a more complex set of threats from a variety of countries, non-state actors, and traditional adversaries.[820] He also noted that the CI system that worked well in the Cold War would not be successful in the threat environment of that time, and indicated his intention to have a U.S. CI system that was predictive and would provide integration and oversight of CI issues across the national security agencies.[821]

(U) PDD 75 outlined specific steps that "will enable the U.S. CI community to better fulfill its mission of identifying, understanding, prioritizing and counteracting the intelligence threats faced by the United States."[822] Specifically, the PDD directed the following:

1. **(U)** The establishment of a CI Board of Directors to select, oversee, and evaluate the NCIX and promulgate the mission, role, and responsibilities of the NCIX. The Board was to also approve the National CI Strategy and work with Congress, OMB, and other Executive Branch agencies to ensure the NCIX has adequate resources to carry out their responsibilities.
2. **(U)** The NSC Deputies Committee to review the annual NTIPA and meet at least semiannually to review progress in implementing the National CI Strategy. The Deputies Committee was to also ensure that the strategy, priorities, and activities of the CI community were grounded in national policy goals and objectives, and to ensure that CI analysis and information

---

[819] **(U)** WHITE HOUSE, FACT SHEET: THE PDD ON CI-21: COUNTERINTELLIGENCE FOR THE 21ST CENTURY (Jan. 5, 2001).
[820] **(U)** *Id.*
[821] **(U)** *Time-line of CI Milestones*, OFFICE OF THE DIR. OF NAT. INTELLIGENCE, dni.gov/index.php/ncsc-who-we-are/ncsc-history/ncsc-time-line-of-ci-milestones.
[822] **(U)** WHITE HOUSE, FACT SHEET: THE PDD ON CI-21: COUNTERINTELLIGENCE FOR THE 21ST CENTURY (Jan. 5, 2001).

[redacted]

[redacted]

would be provided to assist national policy deliberations as appropriate. The CI Board of Directors was to be responsible for ensuring the implementation.

3. **(U)** The establishment of the NCIX position to execute certain responsibilities on behalf of the Board of Directors and to serve as the substantive leader of national-level CI. The NCIX was to report to the FBI director as Chairman of the Board of Directors. The NCIX was also directed to advise the members of the Board on CI programs and policies.

4. **(U)** The NCIX to chair the CI Policy Board. Senior CI officials from State, DOD, DOJ, DOE, Joint Chiefs of Staff, the CIA, the FBI and NSC were to serve on the Board.

5. **(U)** The NCIX to head an ONCIX.

6. **(U)** ONCIX, in consultation with USG agencies and the private sector, was to produce the annual NTIPA for review by the Deputies Committee. Based on this assessment, ONCIX was to formulate and publish the National CI Strategy. ONCIX was also to oversee and coordinate the production of strategic national CI analysis and be supported in this endeavor by all components of the Executive Branch.

7. **(U)** ONCIX was to review, evaluate, and coordinate the integration of the CI budget and resources of DOD, CIA, and FBI and report to the Board and Deputies Committee on how those plans meet the objectives and priorities of the National CI Strategy, as well as evaluate the implementation of the National CI Strategy. ONCIX was to identify shortfalls, gaps, and weaknesses in agency programs and recommend remedies.

8. **(U)** ONCIX was to develop strategic CI investigative, operational, and collection objectives and priorities that implement the National CI Strategy. ONCIX was not to have an operational role in CI operations and investigations and was to have no independent contacts or activities with foreign intelligence services.[823]

g. Counterintelligence Enhancement Act (2002)

(U) In February 2001, one month after PDD 75, the DOJ arrested FBI special agent Robert Hanssen on charges of spying for the Russians for more than 20 years. Hanssen had handed over more than 6,000 pages of classified documents on some of the United States' most sensitive national security programs, including details on

[823] **(U)** Press Release, Pres. William Clinton, White House, U.S. Counterintelligence Effectiveness (May 3, 1994).

[redacted]

[redacted]

U.S. nuclear-war defenses.[824] Furthermore, he revealed the identities of Russian agents working for the United States, two of whom were tried and executed.[825] Hanssen's treason cost the United States billions of dollars and numerous human sources.[826]

(U) In 2002, Congress passed the Counterintelligence Enhancement Act. This Act codified key PDD 75 provisions and aimed to make structural changes to the CI enterprise. Specifically, this Act sought to facilitate the enhancement of CI activities by enabling the CI community to fulfill better its mission of identifying, assessing, prioritizing, and countering intelligence threats to the United States; ensure that the CI community act in an efficient and effective manner; and integrate all USG CI activities.[827]

(U) The Act also sought to clarify the roles and responsibilities of the National CI and Security Board. The Act directed the Board to serve as the principal mechanism for developing policies and procedures to govern the conduct of CI activities; resolve conflicts that arise between USG elements conducting such activities; act as an interagency working group to ensure the discussion and review of matters related to the implementation of the Act; and provide advice to the NCIX on priorities in the implementation of the National CI Strategy.[828]

(U) Most importantly, and for the first time, the Act created a ***national head of U.S. CI***. Specifically, the Act codified the establishment of the NCIX to serve as the head of national CI for the USG, the head of ONCIX, and the chairperson of the National CI Policy Board established by the 1994 CI and Security Enhancements Act. The NCIX was placed within the Executive Office of the President[829] and was also directed to participate as an observer on such boards, committees, and entities appropriate for the discharge of the mission and functions of ONCIX.[830] The purpose was twofold: (1) to close the seams that existed between the fiefdoms of the several operating agencies, which were being exploited by spies seeking a way to access U.S. national security secrets and (2) to develop and execute a national CI strategy to protect the United States against FIE threats targeting the U.S. economy and the openness of U.S. society.[831]

---

[824] **(U)** *Famous Cases & Criminals: Robert Hanssen*, FED. BUREAU OF INVESTIGATION, fbi.gov/history/famous-cases/robert-hanssen.
[825] **(U)** *Id.*
[826] **(U)** 2005 WMD FINAL REPORT at 486.
[827] **(U)** Counterintelligence Enhancement Act of 2002, 50 U.S.C. § 3382 (2018) (as amended).
[828] **(U)** *Id.*
[829] **(U)** *Time-line of CI Milestones*, OFFICE OF THE DIR. OF NAT. INTELLIGENCE, dni.gov/index.php/ncsc-who-we-are/ncsc-history/ncsc-time-line-of-ci-milestones.
[830] **(U)** Counterintelligence Enhancement Act of 2002, 50 U.S.C. § 3382 (2018) (as amended).
[831] **(U)** *Scholars or Spies: Foreign Plots Targeting America's Research and Development: Joint Hearing Before the Subcomm. On Oversight and Subcomm. on Research & Tech of the H. Comm. on Sci., Space, & Tech.*, 115th Cong. (2018) (statement of Michelle Van Cleave).

[redacted]

[redacted]

(U) When President Bush appointed Michelle Van Cleave to the post, Ms. Van Cleave conducted a review of the U.S. CI landscape and concluded that "tinkering around the edges wouldn't do."[832] Ms. Van Cleave testified that "[t]he national CI enterprise needed to be reconfigured to go on the offense, exploit where we can, and interdict where we must, with the purpose of degrading adversary intelligence services and their ability to work against us."[833] The first National CI Strategy, issued in 2005, had this proactive reorientation as its central goal: "Each member of the CI community must be prepared to assume new responsibilities, and join together in a unity of effort."[834]

h. (U) The Intelligence Reform and Terrorism Prevention Act (2004)

(U) President Bush signed the Intelligence Reform and Terrorism Prevention Act (IRTPA) into law in December 2004. This Act was the largest reorganization of the IC since the Truman Administration. IRTPA modified many aspects of federal intelligence and terrorism-prevention organizations. Specifically, it reorganized the IC, established the position of the DNI to serve as the President's chief intelligence advisor and the head of the IC and to ensure closer coordination and integration of the 16 agencies that then made up the IC. It also established the NCTC to serve as a multiagency center analyzing and integrating all intelligence pertaining to terrorism, including threats to U.S. interests at home and abroad.[835] The IRTPA, however, did little to materially reorganize the CI enterprise, although it did fold the NCIX under the new ODNI.[836]

i. (U) The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005)

(U) In February 2004, President Bush issued EO 13328 establishing the Iraq WMD Commission.[837] President Bush charged the Iraq WMD Commission with assessing whether the IC was sufficiently authorized, organized, equipped, trained, and resourced to identify and warn in a timely manner of, and to support USG efforts to respond to, the development and transfer of knowledge, expertise, materials, and resources associated with the proliferation of WMD, related means of delivery, and other related threats of the 21st Century and their employment by

---

[832] **(U)** *Id.*
[833] **(U)** *Id.*
[834] **(U)** *Id.*
[835] **(U)** Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 3341 (2018).
[836] **(U)** *Id.*
[837] **(U)** Press Release, White House, President Bush Administration Actions to Implement WMD Commission Recommendations (June 29, 2005).

[redacted]

foreign powers.[838] The Iraq WMD Commission issued a report with its findings and recommendations to the President in March 2005.[839]

(U) Chapter 11 of this report focused on CI and its findings were scathing. The report noted that U.S. CI efforts "***remain fractured, myopic, and marginally effective***. Our counterintelligence philosophy and practices need dramatic change, starting with centralizing counterintelligence leadership, bringing order to the bureaucratic disarray, and taking our counterintelligence fight overseas to adversaries currently safe from scrutiny."[840] The report also noted that the current CI posture resulted in the loss of offensive opportunities to manipulate foreign intelligence activities to the United States' strategic advantage.[841] The report found that U.S. CI had been plagued by a lack of policy attention and national leadership, although it expressed hope that that would change with the establishment of ONCIX and the issuance of the first National CI Strategy in 2005.[842]

(U) The report issued five recommendations for reforming CI, including two for the NCIX: (1) NCIX should become the DNI's Mission Manager for CI, providing strategic direction for the whole range of CI activities across the USG; and (2) NCIX should work closely with agencies responsible for protecting U.S. information infrastructure to enhance the United States' technical CI capabilities. The report explained that these recommendations were intended to ensure that the NCIX serve as the planner, manager, and supervisor for all United States CI efforts.[843]

(U) Regarding the first recommendation, the Iraq WMD Commission recommended that the NCIX assume the power and responsibility to:

1. **(U)** Prepare the National Intelligence Program's (NIP) CI budget and approve, oversee, and evaluate how agencies execute the budget;
2. **(U)** Produce national CI requirements and assign operational responsibilities to agencies for meeting those requirements;
3. **(U)** Evaluate the effectiveness of agencies within the IC in meeting national CI requirements;
4. **(U)** Direct and oversee the integration of CI tradecraft throughout the IC;
5. **(U)** Establish common training and education requirements for CI officers across the IC and expand cross-agency training;

---

[838] **(U)** *Id.*
[839] **(U)** *See* 2005 WMD FINAL REPORT at Chapter 11.
[840] **(U)** *Id.* (emphasis added).
[841] **(U)** *Id.* at 485.
[842] **(U)** *Id.* at 486 (emphasis added).
[843] **(U)** *Id.* at 487.

[redacted]

6. **(U)** Identify and direct the development and deployment of new and advanced CI methodologies and technologies;
7. **(U)** Ensure that recommendations emerging from CI damage assessments are incorporated into agency policies and procedures;
8. **(U)** Deconflict and coordinate operational CI activities both inside and outside the United States; and
9. **(U)** Produce strategic CI analysis for policymakers.[844]

(U) The Iraq WMD Commission said that at the "heart" of its recommendations was the belief that an integrated and directed U.S. CI effort would take advantage of intelligence collection opportunities; protect billions of dollars of defense and intelligence-related investments, sources, and methods; and defend our country against surprise attack.[845]

(U) Also in 2005, the NCIX published the first National CI Strategy, which included an enhanced focus on offensive CI. The 2005 Iraq WMD Commission applauded the issuance of this strategy, but noted that "***a new strategy alone will not do the job***. As in the old—and clearly unsuccessful—approach to Homeland Security, U.S. counterintelligence is bureaucratically fractured, passive (i.e., focusing on the defense rather than going on the offense), and too often simply ineffective." The report continued: "But unlike homeland security, counterintelligence is still largely neglected by policymakers and the Intelligence Community. In fact, counterintelligence has generally ***lost*** stature since September 11, eclipsed by more immediate counterterrorism needs."[846]

(U) At that time, momentum for reform seemed strong. The first National CI Strategy directed that the national CI enterprise be reconfigured to be able to work together to go on offense. A national team would do the centralized strategic planning; execution would be distributed to the FBI, CIA, and DOD. The goal was to "exploit where we can, and interdict where we must," to degrade adversary intelligence services and their ability to operate against the United States.[847]

(U) However, efforts to substantially reform CI were derailed.[848] According to Ms. Van Cleave, the realignment of U.S. CI was put on hold as the Bush and Obama Administrations concentrated their attention and resources against the War on Terror.[849] As national security resources were directed toward CT efforts, the

---

[844] **(U)** *Id.* at 491-92.
[845] **(U)** *Id.* at 487-88
[846] **(U)** *Id.* at 487 (emphasis added).
[847] **(U)** Michelle Van Cleave, *Want to Stop Russia from Messing with our Democracy? Rethink U.S. Counterintelligence*, POLITICO (Oct. 8, 2019).
[848] **(U)** Interview with Michelle Van Cleave, Nat'l Counterintelligence & Sec. Ctr., Former ONCIX Director (Oct. 6, 2020).
[849] **(U)** Michelle Van Cleave, *Want to Stop Russia from Messing with our Democracy? Rethink U.S. Counterintelligence*, POLITICO (Oct. 8, 2019).

[redacted]

[redacted]

NCIX was hard-pressed to obtain staff or contractors to fill positions needed to meet PDD 75 responsibilities.[850] For instance, the prototype CI program that Ms. Van Cleave designed was stripped of funding and never renewed.[851]

(U) Shortly after the passage of the CI Enhancement Act, the new office of the DNI was established, along with a new bureaucracy and new priorities that steered policy and funding away from ONCIX's nascent efforts to create a strategic CI capability.[852] Ms. Van Cleave later wrote that when the NCIX was placed under DNI John Negroponte, he delegated authority for much of ONCIX's work to his own newly created deputies. She stated that despite DNI Negroponte naming the NCIX as the CI "mission manager," there was little authority to propel change and reform. Mr. Evanina, a former NCSC Director, similarly noted that making the NCIX the mission manager was a "demotion" from its previous statutory role as the executive lead for the CI mission.[853] With no central leadership in the fight against FIE threats, Ms. Van Cleave noted that the FBI, CIA, and the military services tended to go their separate ways, and the NCIX became "just another layer of the weighty bureaucracy of the ODNI."[854]

j. (U) Executive Order 13467 (2008)

(U) On June 30, 2008, President Bush issued EO 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information." One of its provisions designated the DNI as Security Executive Agent (SecEA). As SecEA, the DNI became responsible for providing oversight for background personnel security investigations and determinations of eligibility for access to classified information; developing policies and procedures related to security clearance determinations; and issuing guidelines to heads of agencies promoting security investigation timeliness, uniformity, efficiency, and centralization. The SecEA also serves as the final authority to designate agencies to conduct investigations and determine eligibility for access to classified information in accordance with government standards for eligibility.[855]

---

[850] **(U)** *Time-line of CI Milestones*, OFFICE OF THE DIR. OF NAT. INTELLIGENCE, dni.gov/index.php/ncsc-who-we-are/ncsc-history/ncsc-time-line-of-ci-milestones.
[851] **(U)** Michelle Van Cleave, *Want to Stop Russia from Messing with our Democracy? Rethink U.S. Counterintelligence*, POLITICO (Oct. 8, 2019).
[852] **(U)** *Scholars or Spies: Foreign Plots Targeting America's Research and Development: Joint Hearing Before the Subcomm. On Oversight and Subcomm. on Research & Tech of the H. Comm. on Sci., Space, & Tech.*, 115th Cong. (2018) (statement of Michelle Van Cleave).
[853] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).
[854] **(U)** Michelle Van Cleave, *Foreign Spies are Serious, Are We?*, WASH. POST (Feb 8. 2009).
[855] **(U)** CONG. RES. SERV., EVOLUTION OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER 3 (2020).

[redacted]

[redacted]

k. (U) The National Counterintelligence Review Group (2009)

(U) In 2009, the DNI created the Review Group to review the role, mission, capabilities, and resources of all national CI activities within the IC, with a specific focus on the ability of the NCIX and the ONCIX to carry out the provisions of the CI Enhancement Act of 2002. Mr. Evanina noted that this group focused primarily on identifying prospective spies in the federal government.[856] The Review Group was composed of CI and intelligence professionals and chaired by former FBI Director Louis Freeh.

(U) The review group had three key findings:

1. [redacted] CI is one of three pillars, along with Collection and Analysis, of the Intelligence Enterprise. In this fashion, the Review Group recognized that no matter how threats to national security may change, CI would remain a core element.

2. [redacted] The ubiquity of networks and access to sensitive information in the modern cyber-centered environment constitutes an extraordinary change to the landscape upon which CI operates. The Review Group predicted that the damage done by the most notorious spies of the past will one day be viewed as minor compared to the damage that is being done to U.S. national security interests now and in the future.

3. [redacted] While the individual components of the IC have vigorous CI programs of varying effectiveness, focused primarily on their unique missions, [redacted] The Review Group recognized a need for a strategic CI program—but such a strategic CI program was never established.[857]

(U) The DNI accepted the Review Group's findings and subsequently approved a set of 15 recommendations concerning CI activities within the IC. These recommendations centered around four principal themes:

1. **(U)** Embed CI throughout the IC structure;

2. **(U)** Enhance integration of the core intelligence missions—that is, provide strategic CI analysis that supports warning, mission planning, and operations;

---

[856] **(U)** Interview with William Evanina, Dir., Nat'l Counterintelligence & Sec. Ctr. (Apr. 7, 2022).
[857] **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 2).

[redacted]

[redacted]

3. **(U)** Facilitate the full exercise of NCIX authorities; and
4. **(U)** Engage on cyber—specifically, the NCIX needs to assemble the capability to perform cyber threat analysis, educate the public and private workforce about cyber threats, and provide a forum for de-confliction and tradecraft development.[858]

[redacted]

(U) Additionally, to better support NCIX's statutory authorities, the DNI approved several Review Group recommendations:

1. **(U)** The NCIX be more fully integrated into the DNI's budget process by requiring NCIX approval on CI-related budget recommendations to the DNI.
2. **(U)** The NCIX have full and complete access to all information that the NCIX determines necessary to perform the Cl mission.
3. **(U)** The NCIX, as Chairman of the National Counterintelligence Policy Board (NACIPB), utilize fully the Board to foster collaboration and develop a unified approach to CI; this includes establishing a subcommittee on cyber issues and other subcommittees as appropriate.
4. **(U)** The NCIX develop, in coordination with the Cl community, a long-term, multi-year CI strategy with both defensive and [offensive] elements.
5. **(U)** The NCIX build a staff sized for the mission, including an appropriate senior grade structure and recommend to the DNI incentives to attract detailees of the appropriate grade and expertise.

[redacted] After the Review Group finished its work, President Obama appointed Robert Bryant (who also served on the Review Group) as the NCIX in September 2009. When Mr. Bryant arrived at the NCIX, he testified to this Committee that the office was [redacted]

---

858 **(U)** *Id.* at 3-4.

859 [redacted]

860 [redacted]

[redacted]

[redacted]

[redacted] He established four new directorates: mission integration, acquisition risk (supply chain), analysis and collection (which included damage assessments), and technical cyber CI. He also brought in new leadership and instructed ONCIX to develop overarching CI strategies for [redacted]

[redacted] Mr. Bryant noted several additional ways in which he and the DNI began addressing the Review Group's recommendations. For instance, the DNI directed that the NCIX undertake appropriate measures to initiate, oversee, and coordinate strategic analysis in accordance with existing statutory authority. [redacted] the NCIX was to have full and complete access to all information that the NCIX determines is necessary to perform the CI mission.[865] [redacted]

(U) Finally, in 2009, the DNI elevated CI for the first time as a mission objective in the National Intelligence Strategy. According to Mr. Bryant, this elevation:

> **(U)** Highlighted the necessity of integrating CI into all facets of national intelligence. The DNI's goal in elevating CI to a mission objective was to ensure that ONCIX was positioned to lead a national CI effort that provides a counterintelligence perspective in all IC support to policymakers and enables government departments and agencies

---

[redacted]

[861] **(U)** *Id.*

[862] **(U)** *Id.*

[863] **(U)** *Id.*

[864] **(U)** *Id.*

[865] **(U)** *Counterintelligence Issues: NCIX and FBI: Closed Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. (2010) (prepared statement of Robert Bryant, Nat'l Counterintelligence Executive, Office of the Dir. of Nat'l Intelligence, at 4).

[866] [redacted]

[redacted]

[redacted]

outside the IC to understand and meet enduring and emerging CI challenges.[867]

l. (U) ICD 750 and the "Security" Mission (2010)

(U) In September 2010, the DNI announced the merger of ONCIX with the DNI's Special Security Center (SSC)[868] and the Center for Security Evaluation (CSE).[869] In unifying the formerly-distinct disciplines of CI and security, the DNI adopted a new, layered response to foreign intelligence threats. The merger of these entities with ONCIX was intended to enhance IC mission integration, strengthen the protection of national intelligence, and save resources by consolidating common functions.[870] DNI Clapper also oversaw the build-up of the NITTF[871], directed by EO 13587, to implement a government-wide program to detect, deter, and mitigate insider threats. Finally, Clapper also oversaw the development of Continuous Evaluation and the IC Information Technology Enterprise, and signed Intelligence Community Directive (ICD) 750, Counterintelligence Programs—the first IC-wide CI policy.[872] A year later, the President signed the "National Insider Threat Policy & Minimum Standards," which mandated that every Executive Branch department/agency with access to classified information establish a formal insider threat program and meet all twenty-six minimum standards.

m. (U) Intelligence Community Directive 750 (2013)

(U) In February 2012, DNI Clapper appointed Frank Montoya as the NCIX.[873] Mr. Montoya realigned ONCIX to reflect its functional mission within the IC by focusing on his role as the NIM-CI and establishing a directorate to manage the broad accompanying responsibilities of that role. He also established the first CI Operations Coordination Directorate—the first time CI operations were coordinated

---

[867] **(U)** *Id.*

[868] **(U)** CONG. RES. SERV., EVOLUTION OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER 4 (2020). The mission of the SSC—now the Special Security Director (SSD)—was to provide support staff of the NICX in its role as Security Executive Assistant.

[869] **(U)** *Id.* The CSE was established by former FBI Director William Webster in 1988 as the Security Evaluation Office in the aftermath of Soviet compromises of U.S. diplomatic facilities. CSE supports the Department of State in establishing and monitoring standards for security for U.S. diplomatic facilities abroad to include major construction projects.

[870] **(U)** *Time-line of CI Milestones*, OFFICE OF THE DIR. OF NAT. INTELLIGENCE, dni.gov/index.php/ncsc-who-we-are/ncsc-history/ncsc-time-line-of-ci-milestones.

[871] **(U)** Exec. Order No. 13,587, 3 C.F.R. 13587. The NITTF was established by EO 13587 on October 7, 2011 in the wake of the WikiLeaks scandal involving the release of thousands of pages of classified documents. NITTF's purpose is to establish policy, guidance, standards, and training for the protection of classified information, and to deter, detect, and mitigate potential actions by employees of the USG who may seek to compromise U.S. national security.

[872] **(U)** *Time-line of CI Milestones*, OFFICE OF THE DIR. OF NAT. INTELLIGENCE, dni.gov/index.php/ncsc-who-we-are/ncsc-history/ncsc-time-line-of-ci-milestones.

[873] **(U)** *Id.*

[redacted]

[redacted]

across the community.[874] He was also instrumental in establishing the National Cyber CI Division.[875]

(U) Despite this, other IC reforms around the same time may have hindered broader CI reform. Most notably, DNI Clapper signed ICD 750 in 2013, which explicitly devolved authority and responsibility for all CI programs down to the department/agency level. As Ms. Van Cleave testified in 2018:

> **(U)** The national head of counterintelligence was rebranded director of a security and counterintelligence center, his duties further dissipated by the fixation on leaks and insider threats driven by the grievous harm done by Snowden, Manning, *et al.* ***Gone was any dedicated strategic CI program***, while elite pockets of proactive capabilities died of neglect.[876]

(U) Ms. Van Cleave concluded of the impact of these reforms: "Read between the lines of existing CI guidance and you will not find a whiff of a national-level effort left, other than caretaker duties such as taking inventory and writing reports."[877]

n. (U) Creation of the National Counterintelligence and Security Center (2014)

(U) On December 1, 2014, DNI Clapper established the NCSC as a component of ODNI. The NCSC integrated into one organization the functions of the ONCIX, the CSE, the SSC, and the NITTF.

m. (U) Intelligence Authorization Act for Fiscal Year 2017

(U) The IAA for FY 2017 amended the Counterintelligence Enhancement Act of 2002 by codifying a number of the DNI-driven reforms from 2010 and 2014. It created the presidentially-appointed, Senate-confirmed position of the Director of the NCSC, abolishing the position of the NCIX. The mission of the Director of the NCSC is to "serve as the head of national counterintelligence for the United States Government," which includes chairing the NACIPB. The IAA for FY 2017 also abolished the ONCIX. Its functions were assumed by the NCSC, which the Act codified as a mission center within the ODNI.[878] Congress has not materially changed NCSC's authorizing statute or functions since the creation of the Center.

---

[874] **(U)** *Id.*

[875] **(U)** *Id.*

[876] **(U)** *Scholars or Spies: Foreign Plots Targeting America's Research and Development: Joint Hearing Before the Subcomm. On Oversight and Subcomm. on Research & Tech of the H. Comm. on Sci., Space, & Tech.*, 115th Cong. (2018) (statement of Michelle Van Cleave).

[877] **(U)** *Id.*

[878] **(U)** CONG. RES. SERV., EVOLUTION OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER 5 (2020).

[redacted]

[redacted]

o. (U) Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020

(U) The IAA for FYs 2018, 2019, and 2020, enacted on December 20, 2019, codified provisions of EO 13467 designating the DNI as SecEA: "The Director of National Intelligence or such other officers of the United States as the President may designate" serves as the SecEA "for all departments and agencies of the United States."[879]

p. The National Counterintelligence Task Force (2019)

[redacted] In October 2019, the FBI established the NCITF to "provide management and support for the newly established CITFS throughout the FBI's field offices."[880] [redacted]

[879] **(U)** *Id.*
[880] [redacted] FED. BUREAU OF INVESTIGATION, CONGRESSIONAL NOTIFICATION: FBI POSITIONED TO COMBAT COUNTERINTELLIGENCE THREATS MORE EFFECTIVELY THROUGH NEW ORGANIZATIONAL STRUCTURE (Oct. 1, 2019).
[881] **(U)** *Id.*
[882] **(U)** *Id.*

[redacted]