SELECT COMMITTEE
ON INTELLIGENCE

UNITED STATES SENATE

Additional Questions for Mr. Michael C. Casey upon His Nomination to be Director of the National Counterintelligence and Security Center

Responsibilities of the Director of the National Counterintelligence and Security Center

QUESTION 1: What is your understanding of the unique role of the National Counterintelligence and Security Center (NCSC) within the Intelligence Community (IC)?

NCSC leads and supports the U.S. Government's (USG) counterintelligence (CI) and security activities critical to protecting our nation. This includes providing CI outreach to U.S. private sector entities at risk of foreign intelligence penetration and issuing public warnings regarding intelligence threats to the United States. Within the IC, the Director of NCSC is the mission manager for CI, serving as the National Intelligence Manager for Counterintelligence (NIM-CI) and the principal substantive advisor to the Director of National Intelligence (DNI) on all aspects of CI.

Additionally, NCSC supports the DNI's execution of her Security Executive Agent (SecEA) authorities across the Executive Branch, including the IC, to protect our national security interests by ensuring the reliability and trustworthiness of those to whom we entrust our nation's secrets and assign to sensitive positions. Pursuant to *Executive Order (EO) 13587*, NCSC also supports the National Insider Threat Task Force, on behalf of the DNI, to strengthen insider threat programs across the USG and prevent the compromise of classified information.

QUESTION 2: What is your understanding of the specific statutory responsibilities of the Director of the NCSC?

Under the *Counterintelligence Enhancement Act of 2002*, the Director of NCSC serves as the head of national CI for the USG. In this role, the Director of NCSC is responsible for leading NCSC in:

- Producing the *National Threat Identification and Prioritization Assessment*;
- Producing and implementing the *National Counterintelligence Strategy*;
- Overseeing and coordinating the production of strategic analyses of CI matters, including the production of CI damage assessments and assessments of lessons learned from CI activities;

- Developing priorities for CI investigations, operations, and collection;

- Carrying out and coordinating surveys of the vulnerabilities of the USG and the private sector to intelligence threats to identify the areas, programs, and activities that require protection from such threats;

- Advocating for research and development programs and activities of the USG and the private sector to direct attention to the needs of the CI community;

- Developing policies and standards for training and professionalizing the workforce, and developing and managing the conduct of joint training exercises; and,

- Performing CI outreach, including consulting with the private sector to identify vulnerabilities from foreign intelligence activities.

The Director also oversees NCSC's coordination of the development of CI budgets and resource allocation plans. Furthermore, under the *CI and Security Enhancements Act of 1994*, the Director of NCSC serves as the chairperson of the National CI Policy Board.

Additionally, under *Section 103F* of the *National Security Act*, the Director of NCSC is tasked to perform not only the duties set forth under the *CI Enhancement Act of 2002*, but also such duties prescribed by the Director of National Intelligence. Under *Section 119B* of the *National Security Act*, the DNI designated NCSC as a National Intelligence Center to align CI and security functions in a single organization. In support of its role as a National Intelligence Center, NCSC is responsible for leading and supporting the integration of the USG's CI and security activities, providing outreach to federal and private sector entities, and issuing public warnings regarding intelligence threats to the United States.

There are also numerous instances where NCSC supports the DNI in her execution of her statutory responsibilities. A primary example of this is NCSC's role as the primary staff element supporting the DNI's Security Executive Agent (SecEA) functions. In this role, NCSC helps to oversee many personnel security functions related to eligibility to access classified

information and to hold a sensitive position, to include: overseeing the national security background investigation and adjudication programs; developing and issuing policies and procedures, including those that support reciprocal recognition; and arbitrating and resolving disputes among agencies.

NCSC, on behalf of the DNI, is therefore required to ensure continuous performance improvement in personnel security processes. This includes building the capacity of the background investigative workforce and implementing modernized continuous vetting techniques, as appropriate.

QUESTION 3: Have you discussed with Director Haines her specific future expectations of you, and her future expectations of the NCSC as a whole? If so, please describe these expectations.

The DNI and I have spoken multiple times about the future of the NCSC. Director Haines has expressed that her key objectives for NCSC include:

- Enhancing NSCS's work on the key fundamentals that underlie the work of the IC such as completing and improving the ongoing clearance modernization and move to Trusted Workforce 2.0;
- Building on past successes in NCSC's work on understanding and helping to mitigate the supply chain vulnerabilities for the IC and the entire United States Government;
- Ensuring that the United States Government has the right CI programs needed to protect its work, particularly in the digital space; and
- Helping to continue to convey to the private sector and academia the threats posed by foreign actors, particularly China, and helping those actors grow the programs and expertise needed to protect themselves.

NCSC Mission

QUESTION 4: What do you believe are the greatest challenges facing NCSC?

The evolving CI threat landscape and the growth of NCSC's mission requirements means that NCSC must build on a number of existing efforts in order to ensure that it is effectively postured against the adapting threat

environment will be an enduring challenge.

NCSC will need to build on prior efforts to include:

- Identifying stakeholders and outlining stakeholders' USG and security roles and responsibilities, and clarifying stakeholders' relationships with NCSC.

- Ensuring that NCSC's various roles and missions are properly prioritized and not duplicating the work of other parts of the IC or other agencies who might be better postured to carry out that work.

- Leveraging the IC in protecting non-USG entities that foreign intelligence entities target for their research, technologies, data, and intellectual property.

- Assisting NT50 agencies to establish "CI awareness" and/or security programs to ensure that USG data and sensitive information are identified and protected.

QUESTION 5: Please explain your vision for the NCSC, including your views on its current and future priorities and what the organization should look like five years from now.

My vision is for NCSC to be the nation's premier source for CI and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats. NCSC is currently updating the *National CI Strategy* that focuses on prioritizing specific goals that will make America less vulnerable to foreign intelligence threats.

To implement the vision, if confirmed, I would:

- Leverage the interagency and ensure the CI community is moving in an integrated way to accomplish goals that include:

    - Detecting, understanding, and anticipating foreign intelligence threats;

    - Deterring foreign intelligence activities and capabilities;

- Protecting U.S. interests; and,

- Building CI capabilities, partnerships, and resilience.

- Advocate for resources and budgetary authority to support requirements for the IC and NT50 agencies that align resources to priorities designed to counter risks from foreign and other adversarial intelligence threats.

- Build resilience in the private sector and academia to advance outreach, education, and awareness by making resources available that assist with the development of insider threat and mitigation programs.

- Advance security priorities and support efforts to mitigate supply chain risks, issue security standards that address evolving threats, and establish technical capabilities that complement the CI and security communities to advance their missions.

NCSC currently devotes significant time and effort to raising awareness of foreign intelligence threats. I envision that in five years NCSC will continue to provide focused, sustained leadership in key areas such as: protecting our economic security by mitigating the theft of intellectual property and critical technologies; harnessing and mitigating the promise and risks posed by cutting edge technology available to both the United States and our adversaries; and, putting personnel security and insider threat programs in place to maintain a trusted workforce.

QUESTION 6: What specific benchmarks should be used to assess the NCSC's performance?

NCSC uses many benchmarks to assess progress against the following goals outlined in its *National CI Strategy* and personnel vetting performance plans.

- NCSC gauges the effectiveness of its governance by assessing progress against strategic priorities and by taking an integrated approach to CI and security. NCSC engages across the community by chairing various boards such as the National CI Policy Board, the IC Security Directors' Board, and the CI Strategy and Resource Board.

- NCSC evaluates this in the annual production of the *State of the CI Mission* which provides an assessment of the CI community's progress against priorities, initiatives, and challenges. The *State of the CI Mission* is also used to inform the CI community's prioritization of resource needs for outyears.

- NCSC also reviews benchmarks for security programs to measure their effectiveness. NCSC issued *Performance Management Guidelines* and the *Federal Personnel Vetting Performance Management Standards* to modernize outcomes for measuring efficiency and effectiveness of vetting programs. NCSC's forthcoming issuance of the *Federal Personnel Vetting Performance Management Implementation Guidance* will establish near-term and future targets for performance measures. Collectively, these security policies will facilitate uniform measurement, assessment, and reporting of key vetting processes to ensure consistency, fairness, and the protection of civil liberties.

- NCSC evaluates the effectiveness of its outreach efforts in terms of deployed capabilities, usage, and demand for upgraded capabilities, and user testimonials. NCSC also attempts to understand the extent to which outreach has changed stakeholder behaviors, increased collaboration among stakeholders, and empowered stakeholders to enhance their own security and resilience.

- To measure the health and welfare of NCSC internally, NCSC points to the successful recruitment and retention of highly qualified CI and security officers to serve in NCSC, responsible stewardship of human and financial capital, stellar employee climate survey results, and the success of groundbreaking initiatives such as our *Cross-the-Line* program that cross-fertilizes expertise across the Center and allows for professional growth.

CI Threats

QUESTION 7: What in your view are the most critical CI threats that are currently confronting the United States?

The United States faces a growing range of intelligence threats from an expanding set of actors. Russia and China represent major traditional intelligence threats to the

United States with well-resourced, technically sophisticated intelligence services determined to gain sensitive U.S. information and thwart U.S. collection and operations. Regional actors such as Iran and North Korea, and non-state actors such as terrorist groups, transnational criminal organizations, and hackers/hacktivists are growing in intent and capability. These actors also are increasing their collaboration with one another, enhancing their skills, expanding their geographic reach, and magnifying the threat to the United States.

This expanding array of Foreign Intelligence Entities (FIE) are targeting our data, technology, and talent to erode our military and economic advantage, threatening the critical infrastructure that keeps our economy and society functioning, influencing U.S. public opinion and government policies, and undermining our democracy and societal cohesion. FIE are adopting cutting-edge technologies—from advanced cyber tools to unmanned systems to enhanced technical surveillance equipment—that improve their capabilities and challenge our defenses. Much of this technology is available commercially, providing a shortcut for previously unsophisticated foreign intelligence entities to become significant threats.

U.S. adversaries also increasingly view data as a strategic resource and a collection priority. They are focused on acquiring and analyzing data—from personally identifiable information on U.S. citizens, to commercial and government data—that can make their espionage, influence, kinetic and cyber-attack operations more effective, advance their exploitation of the U.S. economy, and give them strategic advantage over the United States.

QUESTION 8: What would be your top priorities for the NCSC, in terms of the CI threats facing the United States?

NCSC's top priorities are to mitigate and counter a range of foreign intelligence threats to U.S. interests at home and abroad. Hostile intelligence services and non-state actors are becoming more capable and have access to more tools. They seek to access government systems and infrastructure, undermine the private sector through commercial espionage, infringe on the privacy of U.S. citizens through data theft, and shape U.S. policy and public opinion through influence operations.

I anticipate these priorities will be reflected in the forthcoming *National CI Strategy* and, if confirmed, I would look forward to reviewing the strategy and ensuring the Committee is kept apprised of its development. We must better anticipate foreign

intelligence threats and work together across the IC, the broader federal government, and with our partners to counter these harmful intelligence activities and degrade FIE capabilities.

Our strength as a nation rests upon a number of strategic advantages that we must help protect and defend, including our people, our democratic institutions, our critical technology, infrastructure, and supply chains. We must invest in the future to develop the capability and capacity to meet these challenges and protect America's strategic advantage. We must reinvigorate our CI community, build and enable strong partnerships, and increase collaboration to build resilience against current and future foreign intelligence threats.

QUESTION 9: What actions would you plan to take to ensure that each of your identified priorities is satisfied?

I understand through the forthcoming *National CI Strategy*, NCSC intends to drive the direction and alignment of CI priorities and activities. NCSC will leverage the strengths of each federal department or agency within their respective missions and authorities, and in coordination with the CI community, will baseline current activities and identify shortfalls and gaps. These shortfalls and gaps will then be addressed through the strategy's implementation plan to provide future direction, investment, and resource shifts needed to ensure the successful implementation of the strategy.

QUESTION 10: In your opinion, what CI threats, if any, have been overlooked or underestimated?

The top evolving and not fully understood or fully addressed challenge involves the comprehensive national security, data security, and counterespionage laws of the People's Republic of China (PRC). These laws state that the PRC government may access private information, compel PRC citizens in China and overseas to assist PRC intelligence services, and arbitrarily detain or arrest foreigners in China for suspected espionage activities. I do not believe that the United States has fully grappled with the implications of this comprehensive system.

We also cannot underestimate the threat posed by FIEs, especially China and Russia and those groups who assist them, to our critical infrastructure, particularly the financial, power, water, communications, and transportation sectors. Each of these

sectors has a large, relatively vulnerable footprint. Their supporting personnel, networks, and other infrastructure are here in the United States, posing additional legal, coordination, collection, and other challenges for the IC. Any disruption in these sectors could impact our economy, military readiness, and the U.S. population overall. FIEs will look to exploit these nodes during a time of conflict or crisis.

The convergence and disruptive potential of several advanced technologies—including AI, quantum computing, biotechnology, autonomous systems, semiconductors and telecommunications—may have unanticipated impacts across multiple critical sectors such as healthcare, energy, agriculture, and advanced manufacturing. The CI community will face numerous challenges as these technologies develop, ranging from the collection and exploitation of sensitive personal and other data to the disruption of key technical and lifeline sector supply chains to increased adversary capabilities to influence U.S. and global financial markets.

QUESTION 11: What in your view is the appropriate role of NCSC in conducting direct informational outreach to U.S. National Labs, universities, and private sector start-ups and other entities vis-à-vis their appeal as high-value targets for economic espionage?

NCSC has a critical role to play in conducting outreach to private sector, academic, and research entities. The purpose of NCSC's outreach is to educate these entities on foreign intelligence threats to their organizations, provide them with best practices for mitigation, and help them build resilience to protect their critical assets.

Working with other federal partners, NCSC has been conducting extensive outreach for years to entities in U.S. emerging technology sectors, as well as U.S. National Labs, universities, and other research institutions. NCSC conducts its outreach through both classified and unclassified threat briefings, dissemination of written products and videos, national communications campaigns, and through enduring partnerships with industry, academia, state and local entities, foreign allies, and other stakeholders.

Given its limited staff and resources, it is critical for NCSC to continue to partner

with USG agencies in its outreach efforts. I would also highlight the opportunities provided by the "China Roadshows" hosted by the Chairman and Vice Chairman of SSCI, which have allowed NCSC, with other partners, to engage with the private sector at the C-Suite level. By working together, NCSC and its partners unify messaging, deconflict engagement efforts, and broaden the scope of their outreach efforts. NCSC will continue to align its outreach activities with the goals and objectives of the *National CI Strategy of the United States* and will capture metrics on its outreach activities to measure effectiveness and achieve optimal impact for resources spent.

I would also note that over time, I expect NCSC's, and other federal entities', engagement with the private sector to evolve. As more private sector entities are aware of the threat posed by China and other actors, their questions will naturally become more focused on "what can we do" and less about the nature of the threat. NCSC is, I believe, well positioned to continue to highlight best practices to bring together government and private sector partners to combat the evolving threat.

QUESTION 12: Please describe the CI threat resulting from the presence of thousands of foreign nationals from adversary countries at our National Labs and the risks this threat poses to U.S. national security.

The nature of the foreign intelligence threat to our National Labs has changed over the past decades. State actors increasingly are exploiting our culture of openness and collaboration to acquire information on United States research and development, new technologies, and to advance their military capabilities, modernize their economies, and weaken U.S. global influence. While we gain expertise, insight, and valuable skills by maintaining our commitment to a transparent and open innovation ecosystem, we learned that foreign adversaries are taking advantage of the access we have provided to legitimate, talented foreign scientists and academics.

Congressional Oversight

QUESTION 13: *The National Security Act of 1947, Section 102A (50 U.S.C. § 3024)* provides that the DNI "…shall be responsible for ensuring that national intelligence is provided… to the Senate and House of Representatives and the committees thereof," and will "…develop and determine an annual consolidated National Intelligence Program [(NIP)] budget."

a. What do you understand to be the obligation of the DNI and the Director of the NCSC in support of the DNI to keep the congressional intelligence committees fully and currently informed about matters relating to compliance with the Constitution and laws?

As Director Haines has stated, the DNI, per Section 502 of the *National Security Act*, has a clear legal responsibility to inform the Congressional Intelligence Committees of issues of compliance with the Constitution and laws, and to report any illegal intelligence activities. As a long-time and current congressional staffer, I have a tremendous appreciation for the value and necessity of the committee's oversight responsibilities, and fully agree with Director Haines' statement. Should I be confirmed as the Director of NCSC, I commit to keeping the committees informed of any such violations that occur under my authority.

b. What are the Director of the NCSC's specific obligations under section 102A, including as to the NIP budget?

The Director of NCSC has an obligation to support the DNI's role in overseeing the programming and execution of the NIP budget. Additionally, the Director of NCSC is charged with providing such information the DNI requests for determining the NIP budget. Additionally, under the *CI Enhancement Act of 2002*, the Director of NCSC, in coordination with the DNI, is responsible for coordinating the development of budgets and resource allocation plans for CI programs and activities, as well as ensuring that the budget and resource allocation plans address CI objectives and priorities.

Intelligence Community CI Offices and Reforms

QUESTION 14: Please describe your authorities over the CI offices within the IC.

While NCSC does not have operational authority over CI offices in the IC, NCSC may promulgate guidance for IC CI programs. Additionally, by setting strategic priorities for CI investigations, operations, and collection, NCSC guides implementation of CI programs within the IC. NCSC also conducts oversight of IC CI offices through its evaluation of their implementation of the National CI

Strategy.

QUESTION 15: Do you see any need for modifications to the statutory role or authorities of the Director of the NCSC? If so, please explain.

The United States faces daunting threats from FIEs that seek to undermine our economic strength, steal our most sensitive information, and weaken our defenses. The growing impact of those activities demands knowledge repositories, strategic orchestration of CI activities across the USG, and greater outreach efforts to engage and disrupt FIE threats.

To address these issues, if confirmed, I intend to work regularly with the ODNI to identify possible adjustments in NCSC authorities to clarify its mission and functions where needed.

Finally, I would note that the Committee's Audits and Projects Team conducted a study of NCSC last year that highlighted several potential changes to the authorities of NCSC. If confirmed as the Director of the NCSC, I would look to work through those recommendations with the DNI and the committee.

NCSC Analysis

QUESTION 16: What unique role does NCSC's strategic CI analysis play as compared to the analysis produced by other IC components?

NCSC serves a unique role within the IC by producing the *National Threat Identification and Prioritization Assessment (NTIPA)*, as required in the *CI Enhancement Act of 2002*. The *NTIPA* establishes the President's national CI priorities, helps policymakers understand the principal FIE objectives and targets, and describes the intelligence threats that could harm the United States. The *NTIPA* provides a baseline for U.S. CI requirements to guide the analytic, collection, operational, and security activities of the IC, and many other NCSC products—including the *National CI Strategy and the CI Production Guidance*—flow from it. In addition, NCSC's National CI Officers lead several interagency initiatives to drive collection, analysis, and operations to identify and counter foreign intelligence entities and protect America's strategic advantage.

In addition to analytic guidance, NCSC contributes to interagency CI risk assessments that integrate IC-coordinated threat information, vulnerability data, and mitigation strategies to assess specific CI risks to the United States. These include embassy site assessments, supply chain risk assessments, and damage assessments related to unauthorized disclosures. Since many of these threats also impact our allied partners, NCSC produces releasable versions of these products, as appropriate.

QUESTION 17: What is the NCSC's role in coordinating and publishing the IC's CI assessments?

As directed by the DNI, and in consultation with appropriate elements of the departments and agencies of the USG, NCSC oversees and coordinates the production of strategic analyses of CI matters, including the production of CI damage assessments and assessments of lessons learned from CI activities. The *NTIPA* reflects the culmination of contributions from and in coordination with the IC, many USG departments and agencies, and other components within ODNI. This document reflects the greatest concerns the IC and U.S. decision makers have about the current foreign intelligence threat landscape, and focuses the CI community's efforts against a range of foreign intelligence threats. Since many of these threats also impact our allies, NCSC produces releasable versions of *NTIPA* products as well.

State and Local Governments

QUESTION 18: What is NCSC's role in producing and disseminating intelligence for state, local, and tribal partners, including information as it relates to insider threats?

a. How is that role different than that of the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS)?

b. What is your understanding of the amount and nature of cooperation among NCSC, FBI, and DHS?

NCSC does not have a direct role in producing or disseminating finished intelligence for state, local, and tribal partners, including those that may relate to insider threats. NCSC partners with IC agencies that are authorized to produce and

disseminate intelligence at this level, such as FBI and DHS, in the production of bulletins, advisories, and appropriate threat warning information designed to inform and empower partners at this level. These entities are authorized to provide threat warnings and have authorities to produce finished intelligence as well.

NCSC also works directly with Executive Branch agencies to: share best practices for countering foreign intelligence and insider threats; and develop web-based platforms to raise threat awareness by creating and disseminating unclassified advisories, bulletins, and guidance that address insider threat topics. NCSC continues to collaborate with ODNI's Federal, State, Local, Tribal, and Territorial (FSLTT) Partnerships Group to address FSLTT insider threat-related equities.

National Intelligence Manager for CI

QUESTION 19: What is your vision of the Director of the NCSC in the role of National Intelligence Manager for CI?

As mission manager for the CI community, if confirmed, my vision is for NCSC to lead innovative CI and security solutions, further integrate CI and security disciplines into IC business practices, and effectively resource such efforts. To do this, we would drive integrated CI activities to anticipate and advance our understanding of evolving FIE threats and U.S. security vulnerabilities. We would drive development and implementation of new capabilities to preempt, deter, and disrupt FIE activities and insider threats, and advance CI and security to protect our people, missions, technologies, information, and infrastructure from FIEs and insider threats. We would continue enhancing the exchange of FIE threat and security vulnerability information among key partners and stakeholders at all levels to promote and prioritize coordinated approaches to mitigation. In carrying out these activities, my goal would be to create a more proactive CI and security posture in the United States, employing all instruments of national power to prevent regional and emerging threat actors from gaining leverage over the U.S.

QUESTION 20: What is the Director of the NCSC's role in developing the *National Intelligence Priorities Framework* with regard to CI?

The Director of NCSC, as the National Intelligence Manager for CI, fulfills the duties of the NIPF Intelligence Topic Expert for CI. The Director is charged with integrating the CI community's efforts across intelligence functions, disciplines,

and activities in an attempt to achieve unity of effort and effect. One of the most important tools for accomplishing those tasks is the *NIPF*. The Director uses the *NIPF* process to prioritize collection and analysis against FIE threats against the United States and codify our approach for the coming year.

The Director of NCSC convenes the CI community and oversees the drafting of the CI *NIPF* topic's priorities to integrate, and prioritize our efforts. NCSC last completed this effort in March of this year, when the Center and subject matter experts from all relevant intelligence agencies and departments came together to review FIE threats and recommended to the DNI a reprioritization to accurately reflect the CI threat level of each foreign intelligence actor. This periodic review helps the IC determine the state of collection and analysis against FIEs, develop integrated strategies to address collection and analytic gaps, and evaluate responsiveness and success in closing those gaps.

QUESTION 21: What is the Director of the NCSC's role in providing guidance on resource allocation with regard to particular CI capabilities and platforms?

The Director of NCSC provides guidance on resource allocation regarding CI capabilities and platforms through the *National CI Strategy* and subsequent implementation plan, as well as through the broader IC's *Consolidated Intelligence Guidance*. In addition, the Director works within established budgetary processes to impact changes required to address CI and security priorities in the NIP and evaluate IC program resource allocations against the *National CI Strategy*'s goals and objectives.

QUESTION 22: What is the Director of the NCSC's role in providing guidance with regard to the allocation of resources among and within IC elements?

The Director of NCSC provides guidance on the allocation of CI and security resources through the Intelligence Planning, Programming, Budgeting, and Execution (IPPBE) process. The Director also advocates directly to the IC CFO and ODNI for resources for the CI and security mission and evaluates whether IC programs are meeting their expected accomplishments. The Director's resource allocation recommendations are informed by NCSC's continuous direct interaction with IC elements and ODNI leadership. NCSC also relies on documents such as the *National CI Strategy* and the *Unifying Intelligence Strategy for CI*, as well as the *Consolidated Intelligence*

Guidance to communicate CI and security priorities to the IC. Using these documents as a guide, NCSC advocates for IC element CI and security resource requests through the IPPBE process.

QUESTION 23: Given resource constraints, how should the Director of NCSC identify unnecessary or less critical programs and seek to reallocate funding?

The Director of NCSC identifies critical and less critical programs through evaluation of CI and security programs and by developing a clear sense of IC priorities through direct interaction with IC and ODNI leadership. Working closely with IC partners, the Director participates in the entire budget process and routinely makes recommendations on strategic CI and security resource priorities, evaluates IC program requests, advocates for CI and security resources, and makes recommendations on resource alignments.

While the Director of NCSC does not have directive authority over funds reallocation, the Director effectively communicates CI and security-related priorities through documents such as the *NTIPA*, the *National CI Strategy*, the *National Intelligence Strategy*, and other CI and security-related policies and guidance so that departments and agencies can align their resources to the identified priorities. NCSC actively shapes the resource environment by routinely reviewing and recommending CI and security-related resource requests as a part of the IPPBE process as well as leveraging its CI and Resource Strategy Board to refine enterprise mission requirements and priorities.

QUESTION 24: What are the most important CI gaps or shortfalls across the IC?

We need to better understand how FIEs exploit the increasing availability of commercial intelligence tools and services to increase their capabilities and cooperate with other state and non-state actors to exploit our vulnerabilities. To increase our understanding and pivot to a more proactive CI posture, the IC must drive integration, action, and resources across the CI community to outmaneuver and constrain FIEs, protect America's strategic advantages, and invest in the future to develop the capabilities and resilience needed to meet the current threats and challenges and those to come.

FIEs seek to collect information from virtually all USG departments and agencies, state and local governments, cleared defense contractors, commercial firms across numerous sectors, think tanks, academic institutions, and more. FIEs are pursuing not only classified information, but also vast troves of unclassified material that can support their political, economic, R&D, military, and influence goals, and their attempts to target U.S. persons, supply chains, and critical infrastructure. We must continue to build trust and increase collaboration with government partners across the federal, state, and local levels as well as in academia and private industry to sensitize these sectors to the growing threats posed by FIEs and develop practical approaches for information sharing and threat mitigation.

We face an increasingly complex technology landscape that requires the modernization of not only of our collective systems, but also requires an equally skilled workforce. We must develop a technically proficient CI workforce trained in key areas such as cyber, critical infrastructure, supply chain risk management, malign investment, and economic security.

Insider Threats and Unauthorized Disclosures

QUESTION 25: What is the role of the NCSC in preventing insider threats and unauthorized disclosures?

EO 13587 established the National Insider Threat Task Force (NITTF), which is co-chaired by the DNI and the Attorney General and is staffed by NCSC and FBI personnel.

The NITTF developed *National Policy and Minimum Standards* to establish a national baseline necessary for USG insider threat programs. The NITTF provides technical and programmatic guidance to Executive Branch departments and agencies, conducts training and workforce professionalization, and disseminates best practices across the USG.

Since its inception in 2011 the NITTF has provided independent assessments of departments and agencies insider threat programs to gauge compliance with the minimum standards and to provide policymakers with a status of the enterprise. NCSC continues to focus on evolving its NITTF framework to measure effectiveness, maturity, and efficiency.

NCSC also maintains significant roles and responsibilities within the IC to deter, detect, and report unauthorized disclosures of classified information. Pursuant to *ICD 701, Unauthorized Disclosures of Classified National Security Information*, NCSC provides guidance and oversight to IC elements on CI and security matters related to unauthorized disclosures of classified information, maintains a repository of notifications from IC elements regarding any loss or compromise of classified intelligence, and reports to the DNI on a semiannual basis data regarding the occurrence of unauthorized disclosures, trends, actions taken, and status.

QUESTION 26: How does NCSC work with the FBI's National Insider Threat Task Force to deter, detect, and mitigate insider threats?

Pursuant to *EO 13587*, the National Insider Threat Task Force is co-chaired by the U.S. Attorney General and the DNI and is staffed by NCSC and FBI. The NITTF's work impacts Executive Branch departments and agencies by deterring, detecting, and mitigating insider threats. Countering insider threats requires a collaborative effort across the government to develop effective strategies and programs. Through these efforts, the NITTF trains and assists agencies in managing insider threat programs. NITTF and the FBI continue to support the USG and partners to mature established insider threat programs.

QUESTION 27: What is your plan to ensure success in preventing insider threats and unauthorized disclosures?

NCSC is taking a multi-pronged approach to ensuring success, including through its management and oversight of implementing the *National Insider Threat Maturity Framework*, the National Operations Security Program (OPSEC), and the IC's Unauthorized Disclosure Program. The NITTF's ongoing initiative to conduct program reviews of USG insider threat programs focuses on compliance with the established Minimum Standards for Executive Branch Insider Threat Programs, and on reviewing federal programs to measure their effectiveness. The NITTF works with agencies to address vulnerabilities in their programs to further enhance program effectiveness. This initiative is designed to detect, deter, and prevent future insider threats.

NCSC continues to improve the IC's approach to protect against unauthorized disclosures as it provides guidance and oversight to IC elements on CI and security matters related to unauthorized disclosures, helping them to deter, detect, and report

unauthorized disclosures of classified information. Pursuant to *ICD 701, Unauthorized Disclosures of Classified National Security Information*, NCSC maintains a repository of notifications from IC elements regarding any loss or compromise of classified intelligence and reports to the DNI on a semiannual basis, data regarding the occurrence of unauthorized disclosures, trends, actions taken, and status.

Acquisition and Supply Chain Risk Management

QUESTION 28: What is the role of the NCSC in preventing and mitigating foreign state and non-state actors from compromising the supply chains upon which the USG relies for its products and services?

NCSC works with USG Supply Chain Risk Management and cyber offices to help them assess and mitigate efforts to compromise USG and industry supply chains. NCSC also collaborates with the USG cyber community and the IC to provide CI and security perspectives on foreign intelligence and other threat actors' cyber capabilities. NCSC facilitates interagency fora and platforms for the sharing of risk information and best practices.

QUESTION 29: What is your plan to increase NCSC's success in preventing and mitigating foreign state and non-state actors from compromising the supply chains upon which the USG relies for its products and services? How do you measure and define "success" in this context?

NCSC intends to expand industry outreach on CI supply chain threats and risk management best practices to further enhance understanding and acceptance of the shared risk environment of modern global supply chains.

Feedback from stakeholders and demand for new capabilities from academia, private industry, allies, and the USG informs NCSC's measurements for success. Success would be bolstered by the introduction of stronger contractual language during USG acquisitions, proactive engagement that identifies vulnerabilities and mitigations up-front, and increased investment in CONUS-based manufacturing of critical technology components.

QUESTION 30: How do you intend to use NCSC's resources and organizational mandate to fight against the licit and illicit acquisition of U.S. sensitive and advanced technology by foreign actors?

NCSC's role in the whole-of-government effort against the licit and illicit acquisition of U.S. sensitive and advanced technology by foreign actors is to integrate, deconflict, educate, and champion the CI community's efforts. Further, NCSC has a role in identifying the variety of tools, capabilities, and partners across government that should be connected to provide much more comprehensive protection for our most vital technologies and capabilities. Additionally, the CI community will continue expanding outreach efforts to highlight the known vulnerabilities in the U.S. science and technology (S&T) infrastructure to industry, government labs, and others developing cutting-edge technologies. The CI community will continue to identify and share best practices for security and espionage awareness.

Providing threat awareness information to our partners and allies helps them make informed decisions about how to improve their security and CI postures. NCSC works closely with the National Labs to facilitate robust training and threat awareness. For example, NCSC recently introduced the "Safeguarding Science" toolkit on its public-facing website. The initiative is designed to raise awareness of the spectrum of risk in emerging technologies and to help our stakeholders in these fields—such as semiconductor and quantum—develop their own programs to protect research and innovation. NCSC partnered in this initiative with several USG organizations—including the National Science Foundation, Office of Science and Technology Policy, and National Institute of Standards and Technology—to provide tangible mitigation options against theft, abuse, misuse, and exploitation of U.S. scientific, academic, and emerging technology sectors. NCSC is also addressing these issues in the forthcoming *National CI Strategy*.

NCSC's outreach and engagement will foster the development of an informed, empowered scientific community that will be best positioned to assess emerging, advanced technologies and their applications (such as AI and quantum computing), design measures to guard against the potential misuse or theft of these technologies, and encourage information exchanges with the national security community. As a result, the IC will be better postured to proactively identify security challenges. NCSC is also addressing this issue in the forthcoming *National CI*

Strategy.

NCSC Personnel and Resources

QUESTION 31: Do you believe that NCSC currently has an appropriate level of personnel and resources? If not, please specify the areas that are lacking and NCSC's current plans to address those areas.

At this time I do not know. If confirmed, I will evaluate NCSC's personnel and resource levels to ensure NCSC is staffed to provide CI and security leadership and support to the USG, conduct outreach to appropriate U.S. private sector entities, and issue public warnings regarding intelligence threats to the United States.

As the threat environment evolves, I will leverage the ODNI planning and budgeting process to ensure NCSC has the technically trained and experienced personnel and resources to meet mission requirements.

Professional Experience

QUESTION 32: Please describe specifically how your experiences would enable you to serve as the Director of NCSC.

I have spent the last 28 years working in Congress overseeing departments and agencies of the United States government that are involved in national security. For the last seven and a half years, I have served first as the Minority Staff Director and then the Staff Director for the Senate Select Committee on Intelligence. In these roles, I helped, with my counterpart, to lead the staff of the committee in overseeing all aspects of the USIC. I also, again, with my counterpart at the time, helped direct the staff of the committee's investigation into Russia's attempt to interfere in the 2016 election. This three and a half year effort involved considerable exposure to, and engagement with, all the various CI elements of the USIC. Further, as part of my daily job responsibilities as the SSCI staff director, I have personal and direct engagement with multiple CI entities in the IC on issues of concern.

Prior to joining the SSCI staff, I was employed for 9 years at the House Armed Services Committee, where I oversaw multiple areas of DOD operations. While not as directly as involved in CI, I was frequently exposed to CI, insider threat, and supply chain risks and programs of the Department of Defense.

To be clear, I am not, unlike the past acting and confirmed Director of the NCSC, an FBI agent. However, and with all due respect to those individuals, each of whom I believe did an excellent job in that role, I believe that my background suits me for this new role, if I am fortunate enough to be confirmed. I have had a broad exposure to the IC and the entire USG national security operations. I have had long, and often in depth, engagement with CI professionals across the IC. As the Staff Director of the SSCI, I have experience in running a staff of over 40 people. Additionally, the role of Staff Director of the committee has frequently required the ability to navigate multiple competing interests, among members, other committees of the Senate, HPSCI, the IC, and the White House, among others, to enact legislation and complete projects, which has direct parallels to how NCSC must navigate the IC and multiple agencies involved in the CI mission. And, as evident by my professional experience, I have a deep appreciation for the oversight responsibilities of the committee and the necessity for partnering with the committee to ensure NCSC meets its mission requirements.