SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

Additional Questions for
Mr. William R. Evanina upon his nomination to be Director of the National Counterintelligence and Security Center

Responsibilities of the Director of the National Counterintelligence and Security Center

The Director of National Intelligence (DNI) established the National Counterintelligence and Security Center (NCSC) in 2014 to integrate the Intelligence Community's (IC's) counterintelligence and security missions. The NCSC was designed to serve as the primary organization to undertake counterintelligence and security responsibilities within the Office of the Director of National Intelligence (ODNI).

QUESTION 1: What is your understanding of the unique role of the NCSC within the IC?

NCSC's unique role in the Intelligence Community (IC) arises from its unique mission set across the U.S. Government and with our allied partners. NCSC's current mission statement, as reflected in the *2018-2022 National Counterintelligence and Security Center Strategic Plan*, is to lead and support the U.S. Government's counterintelligence (CI) and security activities critical to protecting our nation; provide counterintelligence outreach to U.S. private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the U.S. Within the IC, the Director of NCSC serves as the National Intelligence Manager for Counterintelligence (NIM-CI) and the Director of National Intelligence's (DNI's) principal substantive advisor on all aspects of CI.

Additionally, as the DNI's staff support element, NCSC executes 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 13587, NCSC also serves as the co-director—along with the Federal Bureau of Investigation—of the National Insider Threat Task Force on behalf of the DNI to strengthen insider threat programs across the U.S. Government (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 is the head of national counterintelligence for the U.S. Government. In this role, the Director of NCSC is responsible for producing strategic planning assessments, developing and implementing national counterintelligence strategies, overseeing and coordinating counterintelligence analysis, developing priorities for counterintelligence investigations and functions, conducting vulnerability studies, and performing counterintelligence outreach activities. The Director of NCSC also coordinates the development of CI budgets and resource allocation plans. NCSC is responsible for the production of the *National Threat Identification and Prioritization Assessment* as well as the *National Counterintelligence Strategy*.

Additionally, under Section 119B of the National Security Act, the Director of National Intelligence designated NCSC as a National Intelligence Center to align CI and security functions. In support of its role as a National Intelligence Center, the Director of the NCSC is responsible for leading and supporting the integration of the U.S. Government's CI and security activities, providing outreach to Federal and private sector entities, and issuing public warnings regarding intelligence threats to the U.S.

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

Yes, I have discussed these issues with DNI Dan Coats. He has high expectations of me as a leader, and high expectations of NCSC as a mission center. He expects continued mission and programmatic leadership in the CI and Security community, not only within the IC, but throughout the rest of the Executive Branch. Non-IC departments are a critical part of our national security fabric, yet they are particularly vulnerable to nation state HUMINT and cyber activities. Of great concern are the protection of our critical infrastructure and mitigation of supply chain threats which impact the U.S. Government, the private sector, research and development, and academia. Additionally, Director Coats expects a larger role for NCSC in private sector outreach to deliver threat information and warning about nation state activities. He is also expecting NCSC to take a leadership role in driving security clearance modernization across the U.S. Government, in partnership with the Office of Personnel Management and the Office of Management and Budget.

QUESTION 4: You are a long-time FBI employee. How do you ensure that each of the 17 intelligence agencies is represented at NCSC and is bought into the mission? Why does it make sense for the head of NCSC to be an FBI careerist?

As the Director of NCSC, it is critically important to me that the Center's workforce represents the community and has the requisite skills and experience. NCSC currently has a government workforce comprised of approximately half cadre ODNI officers, and half detailees from other agencies. Those agencies currently include the military services, the "Big Six" IC agencies, as well as some other key agencies in the CI and security community, such as the Departments of Energy and State. We also have detailees from non-IC agencies with significant CI and security experience. The mix of cadre and detailees is a function of the need for continuity and expertise over time (cadre), and the desire to avoid an entrenched bureaucracy (detailees). These rotational detailees refresh the workforce and infuse up-to-date operational knowledge and experience from across the IC, while gaining a better appreciation for the unique role of NCSC which they bring back to their home organizations. NCSC also must maintain a stable cadre population for continuity over time and oversight of various business and infrastructure capabilities. The current NCSC leadership team is a reflection of this balance: My deputy and I are detailees, while the #3 and #4 are ODNI cadre officers.

While I am a 21-year FBI veteran, much of my experience has been in national security programs where I have consistently partnered with other IC elements to accomplish the mission. Additionally, I served as the Chief of the CIA's Counterespionage Group, leading over 200 highly dedicated men and women. I firmly believe the Director of NCSC must have two fundamental characteristics: first is the demonstrated experience and ability to lead highly motivated senior personnel from multiple agencies with disparate missions and cultures, and second is significant experience in the counterintelligence arena. Hence, although an FBI national security executive typically meets these characteristics, I do not believe it is imperative that future directors of NCSC be from the FBI.

NCSC Mission

The NCSC's 2016-2020 Strategic Plan provides that the NCSC's mission is to "lead and support the counterintelligence and security activities of the U.S. Government, the U.S. Intelligence Community, and U.S. private sector entities at risk of intelligence collection, penetration or attack by foreign and other adversaries."

QUESTION 5: Are the findings of NCSC's annual mission review reports concerning the implementation of the National Counterintelligence Strategy of the United States (National CI Strategy) socialized with NCSC mission partners?

Yes. NCSC shares its analysis of mission partner responses to the Mission Review Questionnaire and community-wide findings in feedback letters to the IC elements. I personally sign the letters and my staff coordinates drafts of these letters with appropriate CI and Security elements before they are finalized. The findings are then shared in executive sessions between the NCSC Director and Deputy Director and CI and Security leadership from the IC elements. We include a holistic approach to this process, addressing issues such as CI, security, cyber, insider threat, supply chain, operations, collection, and analysis.

QUESTION 6: Does NCSC monitor the mission partner community for subsequent action taken in response to identified implementation shortfalls?

Yes. The comprehensive IC Mission Review process ensures that previously identified shortfalls are addressed in subsequent assessment activities. When Mission Reviews are conducted, NCSC reviews the prior year's findings and assessments and revisits them as necessary. We assess the status of previously identified issues, emerging concerns, and any gaps. We then monitor actions taken to resolve areas of concern and work with the individual agencies throughout the year to monitor progress. In the next cycle, we provide tailored Mission Review questionnaires to each IC element, requesting updates to agency-specific actions cited in earlier feedback letters. Our ultimate goal is to both ensure significant progress in previous year shortfalls, and at the same time, assist in driving mission enhancement by each agency.

QUESTION 7: NCSC and Defense Security Service (DSS) have closely related missions. How do you and DSS work together to secure the larger IC/DoD enterprise?

DSS strengthens national security at home and abroad through its security oversight of 13,000 cleared defense contractor facilities and their robust education operations. Given NCSC's private sector outreach responsibilities and focus on protection of critical technologies and our supply chain, there is a natural and healthy overlap. Recognizing this, in May of 2016, NCSC assigned a senior officer to DSS to perform liaison duties between DSS, NCSC, ODNI, and select departments and agencies within the Executive Branch. Since that time, several key liaison initiatives have enhanced analytic integration, operational support, and threat and warning.

Counterintelligence analysts from DSS provide threat information collected directly from private industry that highlights foreign intelligence attempts to target national security information at defense contractor facilities, which then informs national level assessments. Joint products highlighting the threat and recommending mitigation measures are now more widely available through the use of DSS's robust dissemination network. DSS's Center for the Development of Security Excellence is partnering with the National Insider Threat Task Force (NITTF) to make online insider threat training widely available across the USG and private sector. DSS and NCSC are also in coordination concerning security clearance modernization efforts to ensure that we maintain a trusted workforce. I communicate on an almost daily basis with the Director of DSS, who is a part of every leadership effort NCSC drives across the USG and private sector.

QUESTION 8: Based on your experience at NCSC, what is your assessment of the NCSC's current strengths and weaknesses as to NCSC's stated mission?

NCSC has transformed significantly since standing up as a national center in December 2014. NCSC's current strengths are clearly embodied in the diverse group of highly qualified women and men from numerous agencies who work together every day to accomplish the mission. Additionally, NCSC's ability to successfully lead IC- and government-wide collaboration and partnerships to deliver high level products to policymakers has never been stronger.

Due to NCSC's successes over the past few years, and the ever-increasing complexity of nation state threats, insider threats, and security clearance issues, NCSC is continuously asked to take on new challenges. Successfully addressing these challenges without a corresponding increase in resources is difficult. For example, increased staffing of technically skilled professionals is essential for meeting long-term mission requirements. In addition, we will have to better leverage technology and Artificial Intelligence in our increasingly data-rich world. NCSC has developed into a CI and Security leader among our "Five Eyes" and NATO partners. I currently serve as the Chair of CI and Security in both entities, which requires a significant amount of resources as well. Additionally, it is difficult to lead CI and Security across the U.S. Government when there are insufficient directed resources for departments and agencies to follow NCSC guidelines.

QUESTION 9: What do you believe are the greatest challenges facing the NCSC?

I believe there are a few challenges which directly impact the enduring success of NCSC. First, it is hard to conduct effective and sustained outreach to Federal Partners, research labs, and the private sector. Although NCSC is building capacity for such outreach, the demand is immediate, technical, and comprehensive. Another significant obstacle is the inability to secure funding across the non-NIP funded departments and agencies, specifically for insider threat, Continuous Evaluation, supply chain risk management, and fundamental CI and Security assistance and training.

QUESTION 10: Is direct public sector outreach and threat warning contemplated in the current NCSC Strategic Plan? If not, why not?

Yes, direct public sector outreach and threat warning is in our current 2018-2022 *Strategic Plan*, and in our NCSC Mission Statement. NCSC closely coordinates with other IC agencies that also provide threat warning and have intelligence dissemination authorities. Our main mission partners in this arena are FBI and DHS. NCSC also works directly with Executive Branch agencies to ensure we share best practices in countering foreign and insider threats. We use our website and social media presence to raise awareness as well. Additionally, I have just hired a senior executive to serve as our director of communications and guide the execution of our strategic communications plan.

QUESTION 11: Would the objectives of the National CI Strategy be advanced by NCSC exercising a more direct role in communicating counterintelligence threats to the public?

Yes, the objectives of the National CI Strategy are advanced through a direct role in communicating foreign intelligence threats to the public, which is a key part of NCSC's statutory mission. In today's environment, it is more important than ever to communicate consistently with the American people, industry, and academia regarding foreign intelligence threats to our national and economic security. We are also aware that what we say in public to the American people is also heard by our adversaries, so it is a challenge to issue credible threat information without revealing too much. That said, a comprehensive and enduring narrative on foreign threats is important for transparency, to the extent we can adequately articulate the threats. Partnerships are critical in forming a consistent and sustained public narrative. In addition to FBI and DHS, the private sector has a role in attributing nation-state or criminal cyber actors publicly.

QUESTION 12: 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 for NCSC is stated in our *Strategic Plan*: To be our nation's premier source for counterintelligence and security expertise, and a trusted mission partner in protecting America

against foreign and other adversarial threats. To fulfill our vision, NCSC is currently focusing on the specific goals and underlying objectives and initiatives outlined in the *Strategic Plan*. However, as an adaptive organization, we review those priorities annually to ensure they reflect the current threat environment. I anticipate that our organization will continue evolving, and in five years, will be an even stronger voice for CI and security issues.

Following the stand-up of the Center in December 2014, we have truly achieved integration between the CI and security disciplines, and will continue to drive that model across the USG and our allied partners as a best practice. We will have domestic NCSC representatives around the country with strong links to state, local, tribal, and private sector partners. At the Federal level, NCSC will have formal, strong ties to mission partners who appreciate NCSC's unique role. NCSC will have the resources and budgetary authority to provide critically needed funding to non-IC partners at risk from foreign and other adversarial intelligence threats or the authorities to ensure that separately appropriated funds are properly aligned.

We currently spend a lot of time raising awareness of threats. I envision that in five years, we will be well past that stage, and able to provide focused, sustained leadership in key areas such as: protecting our economic security by mitigating theft of intellectual property and critical technologies; countering foreign influence operations by coordinating the activities conducted by our mission partners; hardening our critical infrastructure; harnessing and mitigating both the promise and risk posed by cutting edge technology available to both the U.S. and our adversaries; and putting personnel security and insider threat programs in place to ensure a trusted workforce.

QUESTION 13: What specific benchmarks should be used to assess the NCSC's performance?

NCSC uses many benchmarks to assess progress against the goals outlined in our *Strategic Plan*. One specific example is the impact of the guidance we promulgate. For instance, a Collection Emphasis Message we disseminated directly led to the FBI publishing 90 Intelligence Information Reports. Another benchmark is the specific actions we take to heighten awareness of, and to counter, threats to our supply chain and critical infrastructure, such as our recent briefing to State officials in preparation for the 2018 midterm elections. We track the growing number of fora where NCSC is either leading or heavily engaged, many of which are international. For example, I chair the NATO CI Panel and the Allied CI and Security Forum with our "Five Eyes" partners. NCSC's Center for Security Evaluation is a leading voice to build secure embassies and consulates overseas, and NCSC conducts countless private sector engagements through trade association groups to raise awareness and share best practices. We gauge the effectiveness of our governance by assessing the quality and quantity of engagement of the various boards we chair – the National CI Policy Board, the IC Security Directors' Board, and the CI Strategy Board.

To measure the health and welfare of NCSC internally, we can point to the successful recruitment of highly qualified CI and security officers to serve at 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 enhances expertise across the Center and allows for professional growth.

Counterintelligence Threats

QUESTION 14: What in your view are the most critical counterintelligence threats that are currently confronting the United States?

The U.S. 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 both gain sensitive U.S. information and thwart U.S. collection and operations. The three most critical CI threats cut across these threat actors: influence operations, critical infrastructure, and supply chain. 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. Advanced technology previously available mainly to leading nation-states is now increasingly available to a wide range of nation-state and non-state actors as well. For example, a growing set of threat actors are now capable of using cyber operations to remotely access traditional intelligence targets, as well as a broader set of U.S. targets including critical infrastructure and supply chains, often without attribution. Insider threats, sometimes with the encouragement of external actors, are a pernicious intelligence threat to our national security.

QUESTION 15: What would be your top priorities for the NCSC, in terms of the counterintelligence threats facing the United States?

Our top priorities include countering a range of persistent threats from intelligence actors spanning a spectrum of traditional spying, targeting of our critical infrastructure, economic espionage, cyber operations, and supply chain threats. Russia and China present global, well-resourced and technically sophisticated threats to all of these targets. However, regional and non-state actor intelligence operations are marked by increasing technical sophistication as well. Cyber operations are part of a new global "gray space" between peace and military conflict where international norms are in flux, and the protocols for countering and responding to these actions are still being established. Similarly, adversaries leverage supply chains as a threat vector to reach information technology systems and other processes or systems the supply chains support. Moreover, the U.S. government faces the difficult task of identifying insider threats before they inflict serious damage, as evinced in recent years. Another top priority is the strengthening of security safeguards for non-IC Federal Partners to enable them to effectively protect their personnel, systems, and data from hostile actors and cyber threats. Additionally, the "influence" paradigm, which cut across the greater U.S. Government, academia, media, and research and development, manifests itself in many forms and can cause insidious harm to our nation.

QUESTION 16: In your opinion, what counterintelligence threats, if any, have been overlooked or underestimated?

Technology and the capabilities of foreign intelligence threat actors have evolved so rapidly that we have underestimated certain threats. I will focus on two key examples. Until fairly recently, the efforts by China to use its intelligence services to advance its national development by undermining the economic security of the U.S. did not receive adequate attention. The U.S. has been slow in responding, in particular, to China's systematic theft of U.S. technology across broad swaths of the U.S. economy, which represents a critical national security threat.

Similarly, as a nation we underestimated Russia's intent to interfere in U.S. democratic processes and institutions. I assess that the Russian intelligence services will continue their efforts to disseminate false information via Russian state-controlled media and covert online personas to encourage anti-U.S. political views, create wedges that reduce trust and confidence in democratic processes, weaken U.S. partnerships with European allies, undermine Western sanctions, and counter efforts to bring Ukraine and other former Soviet republics into European institutions. I remain concerned that we may still be underestimating Russian capabilities and plans to influence the 2018 midterm and future elections. Furthermore, the Russians are not the only threat actor with the capability and intent for malign influence, yet that is where the focus has been. In my opinion, we also need to look at China and other adversaries' efforts to take a page from Russia's playbook.

QUESTION 17: Some agencies are very good at developing and training a cadre of counterintelligence experts; others seem to treat this discipline as an afterthought. Tell us how you have worked to develop a workforce of counterintelligence professionals at NCSC.

a. How have you encouraged each agency to do the same in-house?

Workforce development is a top priority for me at NCSC. Given the evolving nature of the intelligence threat, it is important that our workforce remains current so they have the expertise to lead the CI community. One effective strategy has been to bring in a healthy mix of detailees with recent experience working CI issues at their home agencies. To enhance our experience in-house, we have cataloged available training on CI issues, as well as key mission management skill sets such as leadership and resource management. Each employee has an Individual Development Plan and is allocated money within our budget to pursue professional development courses. Supervisors are held accountable for supporting their employee's development. We tie every employee's performance plan to the NCSC *Strategic Plan*.

To further professionalize the workforce across the community, my office, in partnership with the IC Chief Human Capital Office, issued the CI Competency Subdirectory to provide a common taxonomy for describing the job-specific capabilities of CI professionalism in the IC. These competencies serve as the basis for IC-wide and/or agency-specific qualifications, training,

career development, performance, promotion, and other standards applicable to CI professionals. This year NCSC led the IC-wide effort to develop training standards based on these competencies. In addition to training CI professionals, I advocate for cross-training other disciplines – such as acquisition, procurement, information assurance, cyber, legal, civil liberties and privacy, Inspectors General, and human resources – in CI so they better understand the intersections between their work and that of the CI community.

b. In your opinion, is the NCSC adequately staffed to address your priorities identified above?

When resources are constrained, one of the first functions to be considered for reduction is training. As the Director of NCSC, it is my role to advocate for the resource levels the community needs to be effective. Within NCSC, we have a small staff dedicated to workforce training matters. In the community-wide CI Training Work group we lead, we stress the importance of continuing to support employee education and training, and my staff is actively engaged in the resource process to ensure that funding for CI training priorities is adequate to meet the requirement.

QUESTION 18: The IC once thought of counterintelligence as being all about spy-versus-spy. Now, the "spy" could be a student in a STEM program or an IP address that appears to originate within the United States. With these aspects in mind, how are you scoping and prioritizing the counterintelligence mission?

The recently produced *National Threat Identification and Prioritization Assessment* (NTIPA), signed by the President in January 2018, provides the foundational guidance for the USG and the IC to scope and prioritize the CI threat landscape. For example, in the NTIPA, we characterize the activities of threat actors who are targeting our sensitive technology and research and development information using students, scientists, and corporate employees in addition to traditional intelligence operatives. Using the NTIPA as a blueprint, NCSC has developed the *Unifying Intelligence Strategy for Counterintelligence* and *Strategic Counterintelligence Priorities* papers for the individual threat actors, and our *Counterintelligence Production Guidance*. We also regularly examine our collection and analytic gaps. We develop collection strategies to address these gaps which are disseminated to the IC via *Collection Emphasis Messages*, and we also issue *Analytic Emphasis Messages*.

QUESTION 19: What in your view is the appropriate role of the NCSC in conducting direct informational outreach to U.S. national labs, universities, and private sector start-ups vis-a-vis is their appeal as high-value targets for economic espionage?

NCSC has a statutory responsibility to provide CI outreach to U.S. private sector entities at risk of foreign intelligence penetration, in addition to leading and supporting the USG's CI and security activities. We execute this responsibility through a variety of means, including direct engagement with entities such as the U.S. National Labs, universities, and private sector. We have ongoing initiatives, such as the "Know the Risk, Raise Your Shield" awareness campaign

and the cyber training series—both of which are available on our unclassified website. We also published the *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standard* that has been widely disseminated. We continue to expand our outreach through CI and Security working groups and conferences across all sectors of U.S. society.

QUESTION 20: Please describe the counterintelligence threat resulting from the presence of thousands of foreign nationals from adversary countries at our National Labs.

The nature of the CI threat to our National Labs has changed over the past decades. A growing list of state actors is increasingly exploiting the culture of openness and collaboration within the United States to acquire information on research and development and new technologies to advance their military capabilities, modernize their economies, and weaken U.S. global influence. The U.S. Government's CI and security resources are challenged by the presence of foreign nationals in the labs. But we also gain expertise, insight and valuable skills by maintaining our commitment to a transparent and open innovation ecosystem. The CI community's understanding of what an "intelligence collector" looks like has evolved, and we now understand that foreign adversaries are taking advantage of the access we've provided to legitimate, talented foreign scientists and academics.

Direct and discoverable ties to foreign intelligence and security services are harder and harder to discover, or don't initially exist at all. That is compounded by the collectors often being experts in fields, meaning they can identify the key pieces of information that will help their home country. Providing threat awareness information to the National Labs will assist them in making more informed decisions about how to improve security and CI awareness. NCSC works closely with the Department of Energy, the Department of Defense, and academia to facilitate robust training and threat awareness to the National Labs since they are a critical piece of the national security ecosystem.

QUESTION 21: In particular, China has a documented history of attempting to steal secret information from our National Labs, yet the United States continues to provide access to thousands of their nationals. Why?

The research community at large is committed to open science and research and does not necessarily think in terms of dual use technologies. Accordingly, they might not be aware of the national security implications of some research initiatives. The work being done at our National Labs ranges from basic, non-sensitive research, to our most prized weapons secrets. China, like other foreign countries, has a very talented academic and science base. As China becomes more capable, some of our National Labs have made great strides in partnership with Chinese nationals, for example, on the protection of nuclear materials. The United States' national and economic security has benefitted from those partnerships. NCSC partners with Department of Energy's Counterintelligence office to help understand, identify, and mitigate threats from Chinese nationals attempting to exploit our system. In addition, many of the consortiums that run the National Labs are affiliated with U.S. educational institutions. In accordance with their

educational policies, the agreements between those entities and the U.S. Government stipulate that researchers will not be discriminated against based on the country of origin.

QUESTION 22: What actions would you plan to take to ensure that each of your identified priorities is satisfied?

As the director of a national center, I use the mechanisms that NCSC has available to address my identified priorities. One mechanism is the governance structures we have in place to promote collaboration and cooperation on critical strategic CI and security issues, such as the National Counterintelligence Policy Board, the IC Security Director's Board, the Security Executive Agent Advisory Committee, and the CI Strategy Board. In addition, NCSC regularly uses regional and functional communities of practice to identify, assess, and coordinate community-wide actions, and we issue guidance to collectors and analysts across the community to ensure high-priority CI and security issues and intelligence gaps are addressed in a timely manner. Another mechanism is my mandate to advise the DNI on IC programs and budgets that support national CI and security priorities, and recommend adjustments as necessary to meet priorities established by NCSC. Finally, I have found it useful to take full advantage of my position as the Director of NCSC to raise awareness, champion our concerns, and convene the right stakeholders to take action.

Congressional Oversight

QUESTION 23: 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 to "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?

It is critical, to maintain the trust of the American people, that the IC fully comply with the Constitution and the laws of the United States.

In addition to the requirements to ensure national intelligence is provided to the Senate and House of Representatives and committees thereof under Section 102A, the DNI is also responsible under Section 502 of the Act to keep the congressional intelligence committees fully and currently informed of all U.S. intelligence activities. Such intelligence activities include "significant anticipated intelligence activities," and "significant intelligence failures."

The Director of NCSC, together with the DNI, likewise has an obligation to keep the

congressional intelligence committees abreast of all U.S. intelligence activities, and is responsible for fully complying with all IC directives related to the disclosure of information to Congress.

Furnishing information to the oversight committees is vital to Congress' role in considering legislation, determining the appropriate level of resources for NCSC, assessing the effectiveness of the Center, and gaining a better understanding of counterintelligence and security issues. If confirmed, I will remain committed to ensuring that the NCSC workforce understands the importance of congressional oversight, provides thorough and timely information to Congress, and is responsive to congressional queries.

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 National Intelligence Program (NIP) budget. The Director of NCSC is charged with providing such information as the DNI requests for determining the NIP budget. Additionally, under the Counterintelligence Enhancement Act of 2002, the Director of the NCSC, in coordination with the DNI, is responsible for coordinating the development of budgets and resource allocation plans for counterintelligence programs and activities, as well as ensuring that the budget and resource allocation plans address counterintelligence objectives and priorities.

Intelligence Community Counterintelligence Offices and Reforms

QUESTION 24: Please describe your authorities over the counterintelligence offices within the IC.

a. 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 foreign intelligence entities 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, I regularly work with the ODNI to assess whether adjustments to NCSC authorities to clarify its mission and functions are needed. I will notify Congress if NCSC identifies a need for changes to the Center's authorities.

b. How do you coordinate and deconflict with these other IC offices?

As the National Intelligence Manager for CI, we support national-level decision making by leading integrated analysis, collection, and CI initiatives to counter foreign intelligence threats. NCSC integrates CI across the IC through strategic prioritization, coordination, and deconfliction

of CI analysis, collection, and resources to address priority intelligence gaps and CI mission needs across the IC. The CI Strategy Board and various working groups and conferences serve as fora where the IC prioritizes, deconflicts, and aligns CI activities and initiatives to address priority threats and gaps. The National CI Policy Board and IC Security Director's Board are also key to helping coordinate and deconflict across the IC. These boards meet regularly and my interaction with the heads of the CI and security entities is persistent and steeped in trust and partnership.

QUESTION 25: NCSC is an organization with sweeping responsibilities but little by way of enforcement capability.

a. What tools does NCSC have to prompt IC agencies to move ahead with what may sometimes be challenging but necessary counterintelligence precautions?

Based on IC policy and directives and its statutory authorities, NCSC uses the following tools to lead and prompt the CI community:

- Strategy, Policy, Standards, and Guidance: Examples include the *National Threat Identification and Prioritization Assessment*; the *National CI Strategy*; national CI priorities for analysis, collection, and operations; Intelligence Community Directives and Standards; and NCSC contributions to legislation, Executive Orders, and Presidential Directives.
- Chairmanship of the National Counterintelligence Policy Board: NCSC convenes senior Executive Branch CI officials to drive decision making and ensure accountability on key CI issues.
- Mission Reviews: NCSC conducts annual Mission Reviews and other assessments to evaluate the IC's implementation of the *National CI Strategy*. For operational matters, this includes the annual *National Assessment of the Effectiveness of U.S. Offensive Counterintelligence Operations*, which evaluates the operational implementation of the strategy.
- Resource Advocacy: NCSC uses documents like the *National CI Strategy* and *Unifying Intelligence Strategy*, as well as *IC Major Issue Studies* and the *Consolidated Intelligence Guidance*, to communicate CI and security priorities to the IC. Using these priorities as a guide, NCSC advocates for IC element CI and security resource requests through the established budget process.

b. Are these tools sufficient to accomplish your mission?

While the NCSC can tout successes across our Center's mission areas, there are certainly challenges in enabling the IC to maximize CI capabilities towards efficient IC and whole-of-government CI support to national strategies and priorities. One specific issue is the inability for some non-NIP funded agencies outside the IC, who constitute our "soft underbelly," to properly resource their CI and security programs.

c. How might Congress and the DNI give the NCSC more authority to prompt action within the IC?

The United States faces daunting threats from foreign intelligence entities 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 counterintelligence activities across the United States Government, and greater outreach efforts to engage and disrupt FIE threats. The governance mechanisms in place now are effective and NCSC is viewed within the IC as a leader on CI and security matters.

QUESTION 26: What do you see as the most important outstanding priorities in the intelligence reform effort, as it relates to counterintelligence?

In the post-9/11 Commission Report era, one of the most important intelligence reform efforts has been increased intelligence information sharing. Within the CI discipline, which seeks to detect and deter a myriad of foreign intelligence activities against the U.S., that effort is equally as vital. By sensibly and responsibly reducing the restrictions placed on sharing sensitive data, the IC will improve its ability to collect against, analyze, and warn of important CI-related developments.

NCSC Analysis

QUESTION 27: What unique role does NCSC's strategic counterintelligence analysis play, as compared to the analysis produced by other IC components?

The Counterintelligence Enhancement Act of 2002 calls on the Director of NCSC, "in consultation with appropriate elements of the United States Government, to oversee and coordinate the production of strategic analyses of counterintelligence matters." Consistent with this authority, NCSC provides analytic production guidance to the CI analytic community that prioritizes foreign intelligence threats and identifies Key Intelligence Questions. These questions help focus limited CI analytic resources on the most important developments and trends relating to foreign intelligence entities. NCSC recently published the 2018-2019 *Counterintelligence Production Guidance* in collaboration with CI analytic elements throughout the Intelligence Community. In addition to analytic guidance, my office also produces CI risk assessments that integrate IC-coordinated threat information, vulnerability data, and mitigation strategies to assess specific CI risks to the U.S. Since many of these threats also impact our allied partners, we produce releasable versions of these products as well.

In 2014, as Director of NCSC, I advocated successfully for the establishment of the National Intelligence Officer for Counterintelligence (NIO/CI) at the National Intelligence Council. The creation of this position remedied the absence of IC-coordinated strategic CI analysis being provided to national policymakers in the Executive and Legislative branches. Since 2014, the NIO/CI in collaboration with NCSC and the CI analytic community has produced a vast range of

strategic CI analytic products that provide analytic insights on priority foreign intelligence threats. These products differ from analysis produced by other IC components in terms of analytic scope and policy impact. Also, they are estimative in nature, and are IC-coordinated representing the view of the entire CI analytic community.

QUESTION 28: What is the NCSC's role in coordinating and publishing the IC's counterintelligence assessments?

NCSC produces a range of unique risk and mission assessments for the CI community. These include the *National Threat Identification and Prioritization Assessment*, the *Foreign Economic Espionage in Cyberspace* report, and the *Counterintelligence Production Guidance*. In our role as CI mission manager, we also produce mission assessments that support collection and analytic emphasis messages to highlight high priority intelligence needs on select topics. NCSC contributes to and coordinates on CI assessments produced by other IC elements and the National Intelligence Council. The subject matter expertise that resides in NCSC's various directorates – to include supply chain risk management, technical CI threats, cyber, and the cadre of National CI Officers that support regional and functional National Intelligence Managers – serves as an important voice in the CI community's review and coordination processes.

State and Local Governments

QUESTION 29: What is the NCSC's role in producing and disseminating intelligence for state, local and tribal partners, including information as it relates to insider threats?

NCSC has a national-level role to support the flow of strategic CI and security threat assessments and mitigation strategies to state, local, and tribal partners. Foreign adversaries have demonstrated intent and capability to threaten U.S. interests at every level of our society, and state, local, and tribal partners are stakeholders and mission partners who play a vital role in identifying and mitigating CI and security threats. In the context of threats to U.S. critical infrastructure, for example, NCSC partnered with the Federal Energy Regulatory Commission, the Department of Energy, and the FBI to provide one-time access to classified information to state and local regulators to raise their threat awareness. We discussed threat actors and IC assessments as well as provided information on mitigating insider threats. In February 2018, NCSC worked with other elements of ODNI, DHS, and the FBI to provide one-time Secret level classified briefings to more than 100 Secretaries of State and state election officials from all 50 states. These threat briefings resulted in greater threat awareness on the part of the states, improved IC understanding of the needs of states, and served as the impetus to improve IC support to states to help defend against threats to the 2018 elections.

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

As a mission manager, NCSC is most often not the producer of finished intelligence products on threats, but rather provides strategic threat awareness information and collection and analytic guidance to Federal, state, and local partners. In contrast, the FBI and DHS are often best positioned to provide tactical threat information and warning to state, local, and tribal entities since they have well-established dissemination mechanisms.

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

Engagement among NCSC, FBI, and DHS is productive, collaborative, continuous, and broadens every day. As I have noted, NCSC is in the unique position, backed by statutory authority, to successfully integrate the IC and other Federal partners as well as state, local, and tribal partners to detect, understand, deter, disrupt, and defend against CI threats from foreign adversaries and insiders.

c. What priority have you assigned to this issue, and what priority do you plan to give this issue going forward?

Interacting with state, local, and tribal governments is one of NCSC's highest priorities. NCSC has detailees from the FBI and DHS to ensure we are providing the best service to the nation and leveraging authorities to best inform our state, local, and tribal partners. NCSC is deliberative in ensuring our products and publications can be shared with the broadest audience possible, including writing products at lower classifications based on the intended consumer. Furthermore, if we are able to establish Domestic NCSC Representatives, they will serve as an excellent conduit to enhance information sharing with our state, local, and tribal partners. We have requested that DHS send a detailee to NCSC to enhance our partnership in the critical infrastructure arena.

National Intelligence Manager for Counterintelligence

As the National Intelligence Manager for Counterintelligence (NIM-CI), the Director of the NCSC coordinates counterintelligence efforts to integrate collection and analytic priorities.

QUESTION 30: What is your vision of the Director of the NCSC in the role of mission manager?

As mission manager for the CI and Security community, my vision is for NCSC to lead innovative CI and security solutions, further integrate CI and security disciplines into IC business practices, and adequately resource such efforts. To do this, we will drive integrated CI activities to anticipate and advance our understanding of evolving FIE threats and U.S. security vulnerabilities. We will develop and implement 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 will 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 accomplishing these things, my goal is to create a more proactive CI and security posture in the U.S., employing all instruments of national power to prevent regional and emerging threat actors from gaining leverage over the U.S.

QUESTION 31: What is the Director of the NCSC's role in developing the National Intelligence Priorities Framework (NIPF) with regard to counterintelligence?

The Director of NCSC, through the NIPF Intelligence Topic Expert for Counterintelligence, who is an NCSC officer, guides the U.S. Government's efforts in the prioritization of collection and analysis on hostile FIEs intent on harming the United States. To collaboratively develop these priorities, NCSC, in September 2017, chaired the NIPF Focus Group on Counterintelligence. This group consisted of over 40 representatives from more than 30 agencies and departments, including CIA, DIA, FBI, NGA, NSA, and the State Department. Past NIPF changes in priority advocated by NCSC have positively shifted analysis and collection to ensure we remain focused on our highest priorities.

QUESTION 32: What is the Director of the NCSC's role in providing guidance on resource allocation with regard to particular counterintelligence capabilities and platforms?

I provide guidance on resource allocation regarding counterintelligence capabilities and platforms by developing strategic CI objectives within the *National Counterintelligence Strategy*. I also communicate CI and security priorities and guidance through the *Consolidated Intelligence Guidance*. In addition, I work within established budgetary processes to impact changes required to address CI and Security priorities in the National Intelligence Program and evaluate IC program resource allocations against *National Counterintelligence Strategy* objectives. A recent example is our successful advocacy for funding for the CITADEL program, which will position the community to collect information on CI threat actors to better mitigate threats posed to the USG.

QUESTION 33: What is the Director of the NCSC's role in providing guidance with regard to the allocation of resources among and within IC elements?

I provide guidance on the allocation of CI and security through the Intelligence, Planning Programming, Budgeting, and Evaluation process. I also advocate directly to the IC CFO and ODNI for resources across the CI and security mission space and evaluate whether IC programs are meeting their expected accomplishments. My resource allocation recommendations are informed by NCSC's annual Mission Reviews and through direct interaction with IC elements and DNI leadership.

QUESTION 34: Given resource constraints, how should the Director of the NCSC identify unnecessary or less critical programs and seek to reallocate funding?

I identify 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, I participate in the entire budget process and routinely make recommendations on strategic CI and security resource priorities, evaluate IC program requests, advocate for CI and security resources, and make recommendations on resource alignments.

While I do not have direct control over funds reallocation, I effectively communicate CI and security-related priorities through documents such as the *National Threat Identification and Prioritization Assessment*, the President's *National CI Strategy*, *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. Also, to actively shape the resource environment, NCSC routinely reviews and recommends CI and security-related resource requests as part of the budget process.

QUESTION 35: What are the most important counterintelligence gaps or shortfalls across the IC?

The IC and U.S. Government are facing important CI and security challenges today that affect our ability to perform critical mission objectives and effectively drive protection of our national security. To address these gaps, the IC must:

- Develop innovative solutions to discover, access, and exploit disparate and large data sets so the IC can use the information to enable warning and develop an agile CI and security posture.
- Advance its capabilities through the development of new, improved tradecraft, technical solutions, security clearance reform efforts, and enhanced information security. The IC must use the full spectrum of its capabilities and knowledge to deter and disrupt threats posed by foreign adversaries and insiders.
- Continue to develop and retain a highly skilled, technically proficient workforce with expertise, for example, in information technology, data science, and telecommunications, in order to develop offensive as well as defensive strategies.
- Develop an improved capacity to provide threat and warning to state, local, and tribal entities, as well as the private sector, so we are better able to connect CI and security threat information with vulnerability data to improve our understanding of and ability to mitigate risks to the U.S.

Insider Threats and Unauthorized Disclosures

QUESTION 36: What is the role of the NCSC in preventing and penalizing those who pose an insider threat to our classified intelligence information?

Executive Order 13587 established the National Insider Threat Task Force (NITTF) to assist in the development of an executive branch-wide national insider threat program. The Task Force is co-chaired by the DNI and the Attorney General, with day-to-day leadership from NCSC and the FBI. The NITTF developed the National Policy and Minimum Standards to set the basic elements necessary to establish insider threat programs, provide technical and programmatic assistance to approximately 100 departments and agencies, conduct training, disseminate best practices, and champion the push to professionalize the insider threat workforce.

The Task Force is working with DOD to extend the national program to the 13,000 facilities in the cleared defense contractor community. Finally, the NITTF is conducting independent assessments of department and agency insider threat programs to gauge their implementation of the Minimum Standards, and actively developing a model to advance programs beyond the minimum and make them more effective. The goal is not to catch malicious insiders after the compromise, but rather to proactively engage the workforce and build comprehensive and effective programs that preempt the compromise of classified information. If that fails, FBI and DOJ have the lead for investigating and imposing penalties for criminal action.

QUESTION 37: How does the NCSC work with the FBI's National Insider Threat Task Force (NITTF) to deter, detect, and mitigate insider threats?

The NITTF is co-chaired by the DNI and the Attorney General, with day-to-day leadership from NCSC and the FBI. Staffing currently comes from the NCSC, FBI, the Office of the Undersecretary of Defense for Intelligence, DIA, CIA, and the Transportation Security Administration. Agency representation is dynamic, and in the past, NSA, DOE, and others have provided their unique agency perspectives to the Task Force. The NITTF also leverages relationships with programs from the IC, DOD, and Federal Partners to champion issues of common concern and lead community working groups. Through these efforts, the NITTF works to train and assist Executive Branch departments and agencies to professionally handle insider threat matters, and, when appropriate, refers the matter to the FBI for further investigation in a manner that promotes a successful outcome.

QUESTION 38: In 2015, you were asked whether NCSC had identified OPM's security clearance database as a counterintelligence vulnerability. You responded that "[t]he statutory authorities of the National Counterintelligence Executive, which is part of NCSC, do not include either identifying information technology (IT) vulnerabilities to agencies or providing recommendations to

them on how to secure their IT systems." However, the NCSC Strategic Plan for 2016-2020 emphasizes the integration of counterintelligence with security, including the protection of networks. Please explain how you would implement that integration in terms of:

a. Assessing where government cybersecurity vulnerabilities create the greatest counterintelligence risks;

NCSC works with the IC and USG cyber community to provide the CI and security perspective on foreign adversarial cyber capabilities, intent, and attribution. We do not identify specific vulnerabilities or make targeted mitigation recommendations; rather we raise awareness of cybersecurity vulnerabilities and the impact of potential compromise or exploitation. One concrete example of this partnership is the IC Security Coordination Center, or SCC, which was a joint development effort between the IC CIO and NCSC. As part of the IC's approach to integrated risk reduction and a community-wide consolidated security risk posture, the ICC SCC operates one of the USG's seven Federal Cyber-Security Centers. It contains a fully integrated CI and Security Cell that works hand-in-hand with Information Assurance and Computer Network Defense professionals analyzing cyber security threat trends and network vulnerabilities, to include zero days, and produces warning and vulnerability mitigation reports called "Tippers" that are shared across the USG Cybersecurity Center network.

The Deputy Director for the IC SCC is a senior CI professional from NCSC whose function is to integrate into the Center such CI functions as supply chain risk management, cyber threat and vulnerability analysis, insider threat monitoring and analysis, and CI and related security liaison reach back. Plans are currently underway with the IC CIO to build greater combined capabilities in the areas of cyber security threat trends, vulnerability awareness, cyber "indications and warning," threat reporting and information sharing capabilities. Our National Counterintelligence Officer for Cyber works with the Cyber Threat Intelligence Integration Center (CTIIC) to infuse CI into CTIIC's analysis.

b. Recommending mitigation strategies; and

The IC SCC has collaborated across the USG to track known network vulnerabilities and mitigation status, such as (1) the "Heartbleed" zero day a couple of years ago and (2) more recently, the widely used web software "Apache Struts" zero day that was used to exploit Equifax and potentially could have impacted multiple USG departments and agencies. These are examples of how, through the IC SCC, we seek to help organizations understand known vulnerabilities and emerging threat trends so they can harden their network systems. We also believe that hardening the human operating system—your network users—through education and awareness is just as important.

To that end, NCSC developed a comprehensive cyber-CI awareness program called "Know the Risk, Raise Your Shield," which provides the USG, private sector, and the American public with cyber security awareness tips, cyber security hygiene tips, and educational videos on the basics and the interrelationship of counterintelligence, insider threat and supply chain risk

management.

c. Conducting damage assessments following any breaches.

NCSC, as directed by the DNI, leads and coordinates CI damage assessments to evaluate actual or potential damage to national security as a result of unauthorized disclosure of classified information. The CI concern is what our adversaries learn about our capabilities when sources and methods are publicly disclosed.

QUESTION 39: Intelligence Community Directive (ICD) 704 states: "Heads of IC Elements or designees may determine that it is in the national interest to authorize temporary access to SCI and other controlled access program information, subject to the following requirements - temporary access approvals shall be granted only during national emergencies, hostilities involving United States personnel, or in exceptional circumstances when official functions must be performed, pursuant to EO 12968. Temporary access approvals shall remain valid until the emergency(ies), hostilities, or exceptional circumstances have abated or the access is rescinded. In any case, temporary access shall not exceed one year." ICD 704 further states that "the DNI retains the authority in any case to make a determination granting or denying access to [SCI] information."

Are there any political appointees or other personnel in the Executive Office of the President who have been granted temporary access to SCI or other controlled access program information? If yes, please respond to the following:

ODNI does not routinely conduct individual access determinations, but instead establishes uniform standards and procedures for the grant of access to SCI and ensures the consistent implementation of those standards. Intelligence Community Directive 704 provides consistency in granting secure compartmented information access to the IC, but does not apply outside of the IC. Under Executive Order 12968, where official functions must be performed, temporary eligibility for access to classified information may be granted. While the DNI has oversight responsibilities of personnel security programs, agency heads are responsible for establishing and maintaining an effective program to ensure that access to classified information by personnel is clearly consistent with the interest of national security.

If yes, please respond to the following:

a. Has the DNI reviewed these cases?

See prior answer.

b. Has the DNI recommended in any of these cases that this access be denied?

See prior answer.

c. Which of the above requirements listed in ICD 704 have provided the basis for the temporary access?

See prior answer.

d. Has a temporary access been extended beyond a year?

See prior answer.

e. Who is responsible for managing these temporary accesses?

See prior answer.

QUESTION 40: What is your plan to ensure success in preventing and penalizing insider threats and unauthorized disclosures?

IC employees who misuse their access to intelligence information not only violate law and/or policy, they violate the public's trust and degrade the public's confidence in the integrity of the IC as a whole. Further, with today's technological capability for rapidly moving massive volumes of data from information systems, it is imperative that we have safeguards in place to detect such nefarious activity as close to near real time as possible.

An insider threat program is designed to focus on the central issue of human behavior: to proactively detect behavior of concern either in the physical or virtual world, place it in context, determine if a risk, threat, or vulnerability exists, and if it does, energize the appropriate agency elements to resolve the matter and mitigate the risk. Part of the solution is auditing and monitoring user activity programs in place across the IC. These are a critical piece because of the confidence we gain in knowing what is happening to information we share. Coupled with information from numerous parts of an organization—such as travel records, human resources, personnel security and data from Continuous Evaluation—these programs can develop a comprehensive view of anomalous activity and take proactive measures. Another key component is education of the workforce to instill a culture of awareness. When properly trained on insider threat indicators and reporting procedures, the workforce can become a force multiplier. NITTF assessments have shown that those departments and agencies with sound workforce and stakeholder engagement demonstrate the ability to identify not only threats to national security, but also threats to our people and mission resources. We plan to continue our ongoing public and USG awareness program about the damage caused by unauthorized disclosures that was initiated by the National Security Advisor last fall.

Acquisition and Supply Chain Risk Management

As you know, there have been recent incidents of supply chain intrusion in the U.S. government by contractors and vendors with foreign actor ties that went unnoticed - or, at least, not acted upon - by the IC.

QUESTION 41: What is the role of the NCSC in preventing and mitigating foreign state and nonstate actors from compromising the supply chains upon which the U.S. government relies for its products and services?

Impetus for securing our critical supply chains has grown in recent years given the mounting evidence that our adversaries are using our supply chain to cause us harm. This is a difficult challenge given the disparate players involved—CI, security, acquisition, procurement, information technology (IT), facilities and logistics, contracts, legal, civil liberties and privacy—with no real lead. NCSC's role has been foundational in this regard. We lead the IC in setting policy and standards to improve supply chain risk management (SCRM), creating a shared repository for SCRM-related assessments, raising awareness of supply chain risk across the USG and private sector, and advocating for the inclusion of supply chain risk into national-level decision-making processes and strategies. Specifically, in 2013, we established the first DNI policy addressing supply chain risk management.

Last year, I issued the policy standard, *Supply Chain Information Sharing*, which resolved a decade-long requirement to better share information to protect and defend our supply chains. NCSC participates in the Enduring Security Framework, a public-private partnership between the USG and key IT and Defense Industrial Base companies organized under DHS's authorities. NCSC partnered with the Federal Communications Commission to brief telecommunications representatives, and with the Federal Energy Regulatory Commission, to brief the energy sector on mitigating supply chain risk. NCSC successfully advocated for the inclusion of supply chain risk in the *National Security Strategy*, the *National CI Strategy*, and Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

QUESTION 42: What is your plan to increase the NCSC's success in preventing and mitigating foreign state and nonstate actors from compromising the supply chains upon which the U.S. government relies for its products and services? How do you measure and define "success" in this context?

NCSC's *Strategic Plan* delineates my approach to preventing and mitigating compromises to our critical supply chains. We plan to continue our whole-of-government approach by raising awareness about supply chain risk, fostering partnerships in the public and private sectors, and strengthening the exchange of threat and vulnerability assessments with mission partners. We share best practices and provide guidance on establishing and maturing SCRM programs, and advocate for the necessary resources.

I measure success by the foundational processes we establish and promulgate throughout the IC, by the continued recognition of this threat at the national level, and by the documented improvements made by individual IC elements. A recent example of a success is DHS's Binding Operational Directive requiring all federal agencies to identify the use or presence of Kaspersky Labs products and provide a plan of action to remove and discontinue present and future use. As stated in the DHS press release, "[t]he risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security."

QUESTION 43: Does NCSC conduct damage assessments relative to the licit and illicit acquisition of U.S. sensitive and advanced technology by foreign actors, to include nontraditional intelligence collectors?

Damage assessments are used to evaluate actual or potential damage to national security resulting in the unauthorized disclosure of compromise of classified national intelligence. NCSC oversees formal damage assessments and leads, when charged to do so by the DNI, or facilitates CI damage assessment teams when the unauthorized disclosure or compromise involves classified national intelligence affecting more than one IC element or USG department or agency. In the case of licit and illicit acquisition of U.S. sensitive and advanced technology at cleared defense contractors, DSS would have the lead.

QUESTION 44: 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?

Building CI threat awareness across government and our public and private sector partners must be permanent and enduring, and this is especially true regarding science and technology (S&T) partnerships. Put simply, we are going to have to make smarter, and sometimes difficult, decisions about who we partner with, and what the terms of those partnership are. This is in many ways a policy question, but the CI community's role is to highlight known vulnerabilities in our S&T infrastructure, and help identify and share best practices for security and CI awareness. We also need to be sure our partners know who to call when they identify a problem, and that we are responding to those needs effectively. Finally, we have many partners conducting outreach and briefings, and there is a leadership and coordination role for NCSC to play in making sure that those outreach materials and briefings are consistent and informative.

NCSC also has a role as a mission integrator. There are many excellent efforts already taking place from individual CI and security elements around the government, but we are up against actors that are incredibly organized and focused. Our response has to be organized and focused too, and NCSC has a role in identifying the wide variety of tools, authorities, and partners across government that should be connected to provide much more comprehensive protection for our most vital technologies and capabilities. Using our leadership of the NATO CI

Panel and the Allied Security and Counterintelligence Forum, we also need to exchange best practices with allied partners.

NCSC Personnel and Resources

QUESTION 45: Do you believe that the 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.

If confirmed, I will continuously evaluate NCSC's personnel and resource levels to ensure we are staffed to provide CI and security leadership and support to the U.S. Government, conduct CI outreach to appropriate U.S. private sector entities, and issue public warnings regarding intelligence threats to the U.S. We have recently established an NCSC Annual Planning Cycle which focuses our senior leadership team meetings on NCSC's goals, initiatives, resources, and staffing. We do this with robust input from our workforce.

We have to ensure our workforce is prepared to accomplish NCSC's growing mission requirements, especially in the areas of security clearance reform; leading, with the FBI, Executive Branch efforts to build insider threat programs; and developing national CI and Security policy to identify gaps, recommend priorities, and inform and shape resource decisions. I will utilize the ODNI planning and budgeting process to ensure NCSC has the technically trained and experienced personnel and resources to meet mission requirements. As those requirements continue to grow, I will reevaluate our staffing levels to minimize degradation to mission accomplishment.

QUESTION 46: Does the NCSC currently employ contractors?

a. If so, what is the numerical ratio of contractors to government employees?

Yes, NCSC relies on the technical skills and talents of contractors to augment those of our government staff. Currently contractors comprise 43 percent of our workforce.

b. What are NCSC's plans for employing contractors in the future, and what is the basis for those plans?

Contract personnel are part of an integrated team of professionals who bring remarkable, often rare, expertise. They support U.S. Government personnel in performing mission and mission support activities. They are an excellent source of highly qualified experts, and often provide a level of technical depth not found in government. Additionally, contracting staff can help provide surge support to tackle emerging needs as we engage in the slower (but necessary) process of workforce transformation. The staffing mix NCSC currently employs provides the right balance between cadre, detailees, and contractors to ensure NCSC is optimally postured.

Professional Experience

QUESTION 47: Please describe specifically how your experiences have enabled you to serve as the Director of the NCSC, and how these experiences would enable you to serve effectively in the future.

In serving as the Director of NCSC for more than three years, I have been fortunate to lead amazing women and men from multiple missions and cultures to accomplish critical national security objectives. My leadership and motivation skills developed over three decades of government service enable me to effectively lead and manage a diverse workforce, leverage individual and collective skill sets, and facilitate a high performing workplace where talented government employees and contractors want to work. My 21 years of experience in the FBI has placed me in numerous high stress operations, with high stake outcomes, and precarious situations, which result in a portfolio of deep and broad experience to draw upon when significant national security events and serious personnel situations arise.

My substantial experience serving as the Chair for CI and Security for our integral "Five Eyes" and NATO partners has enabled me to drive an enhanced footprint and impact on our partners, and at the same time develop new and enduring relationships with CI and Security leaders from those countries which fosters trust and enhanced collaboration. In the same context, I have built extensive trust and partnership, not only with senior leaders of CI and Security within the IC and the Federal Partner entities, but also with chief executives, information officers, and security officers from key private industry sectors critical to national security missions.

Over the past three years, I have successfully engaged with senior level leadership and policymakers in the National Security Council and developed a keen insight into the critical interlocking of intelligence and policy development. Additionally, I have successfully conducted numerous briefings and provided extensive testimony to this and other congressional committees, individual Members, and congressional staff on a broad array of CI and security issues. With such experience, I have gained an enhanced appreciation of the critical role of oversight, and the constructive relationships required to effectively enhance the CI and security mission.

The above experiences and leadership qualifications provide me a solid platform, if confirmed, to lead NCSC to the next level as a national center. In today's complex and persistent threat environment, our national security is dependent, not only upon our capabilities, but also on strong and experienced leadership to lead our dedicated women and men. I believe, if confirmed, I can continue to enhance the NCSC vision of being the nation's premier source for counterintelligence and security expertise.