

UNCLASSIFIED

**SELECT COMMITTEE ON
INTELLIGENCE**

UNITED STATES SENATE



**Additional Questions for
George Wesley Street upon his nomination to be
Director of the National Counterintelligence and Security Center**

UNCLASSIFIED

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)?

The NCSC mission is to lead and support U.S. Government (USG) counterintelligence and security activities critical to protecting the nation, providing outreach to the public sector, and issuing public warnings regarding intelligence threats to the U.S. Broader than just the Intelligence Community (IC), the NCSC can and should serve as the center of gravity for the whole of Government “Counterintelligence Fight” and a leader for the security community. The NCSC has the potential to serve as the nerve center to enable USG agencies with the authorities and mission to execute operational activities that achieve counterintelligence effects. The NCSC can act as a fusion point for the USG counterintelligence and security communities as well as a critical touch point for private industry, academia, state, local, tribal and territorial governments. The NCSC can also serve as a key bridge between the federal IC and law enforcement (LE) communities.

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

My understanding of the specific statutory requirements of the NCSC are as follows:

- Lead the NCSC, and serve as the head of national counterintelligence for the USG
- Chair of the Counterintelligence Policy Board
- Production of the National Threat Identification and Prioritization Assessment
- Production of the National Counterintelligence Strategy
- Evaluate on an ongoing basis the implementation of the National Counterintelligence Strategy
- Coordinate the development of budgets and resource allocation plans for counterintelligence programs (at the direction of the DNI)
- National Counterintelligence Collection and Targeting Coordination, including the development of priorities for counterintelligence investigations, operations, and collection
- National Counterintelligence outreach, watch and warning, including outreach to private/public sectors, research and development, development of

policies and standards for training and professional development for counterintelligence personnel

- Developing standards and criteria for Counterintelligence Risk Assessments and Vulnerability Surveys and identifying vulnerabilities from foreign commercial spyware
- The NCSC also supports the DNIs role as the Security Executive Agent, providing expertise to support DNI decision making and policy guidance

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

If confirmed, Director Gabbard expects me to provide a return on investment of the American taxpayer; achieve substantive results; optimize NCSC structure; impose cost on adversaries; and be transparent with the U.S. Congress. She also expects that I will lead the U.S. counterintelligence and security communities, protect classified information, the defense industrial base, critical infrastructure, academia, private industry, state/local governments from foreign exploitation.

NCSC Mission

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

In my view there are several challenges currently facing the NCSC. There is a perception in the field that the NCSC is a “think tank” type entity that doesn’t provide significant value to field elements executing counterintelligence and security mission sets. This is likely due to a lack of understanding of the statutory mission of the NCSC. The NCSC is meeting key national security needs and has unique capabilities that support the entire IC and beyond. However, the NCSC lacks solid linkages to the field elements that are executing counterintelligence and security mission sets. The NCSC must enhance its partnership with field elements, provide value to its consumer base, and ensure DNI/Congressional awareness of its unique functions. It must also be responsive to DNI requirements and focus on the defined mission: “organizing and leading strategic planning for counterintelligence activities of the USG by integrating instruments of national power as needed to counter foreign intelligence activities.”

The NCSC must be more representative of all elements of “national power,” including partnership with the interagency, ideally through partnership with the National Counterintelligence Task Force (NCITF) to better implement the National

Counterintelligence Strategy across the interagency.

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.

If confirmed, I envision the NCSC as the central hub for U.S. counterintelligence and security, supporting the government, private and public sectors as an agile center of gravity for all counterintelligence and security topics related to nefarious foreign intelligence entity activities. The NCSC can provide the linkages between these U.S. partners and the appropriate USG entity that can take action against adversarial entities.

The NCSC doesn't have to lead or include all of these diverse entities in its structure, but should serve as the mechanism to connect the right provider with the right consumer. The NCSC should not replicate or compete with activities being executed by other entities in the IC, but enhance centers of excellence that provide results effectively.

The NCSC should be agile to emerging threats, shifting techniques, and economic environments. The NCSC should spearhead whole-of-government and whole-of-nation solutions to complex counterintelligence challenges. For example, if foreign students represent a potential non-traditional collection threat to U.S. research, development, and technological leadership – the NCSC should be working to address that challenge, in coordination with stakeholders, to find legal, ethical and effective solutions to minimize that risk.

The NCSC should tirelessly explore opportunities to strengthen our overall security posture to protect classified information and national equities. Interoperability, reciprocity, and common standards for access to classified information should continue to evolve to keep pace with emerging challenges.

The NCSC should counter the exploitation of U.S. society and counter foreign malign influence through effective outreach and enabling operational activities of field elements. We must be agile and adaptable to counter the innovative techniques of foreign intelligence and adversarial elements. We should identify areas of redundancy, streamline and optimize our structure.

The NCSC should be valued by the elements of the interagency conducting the

investigative and operational activities of counterintelligence and security – these are key customers for the NCSC.

Any proposed changes to statutory requirements to make the NCSC more effective should be addressed under the leadership of the DNI, through applicable OMB processes, and in partnership with Congress.

Five years from now, I would envision an optimized, agile NCSC, that is respected and valued throughout the counterintelligence and security communities, providing unparalleled value to the nation.

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

The NCSC should be assessed on multiple benchmarks:

- Meeting Statutory Requirements. The NCSC is responsible to meet statutory requirements. It must do so in accordance with the law and in order to maintain credibility with the Executive Branch, the DNI, and the U.S. Congress.
- Providing a Return on U.S. Taxpayer Investment in Counterintelligence. The NCSC must be valued by its consumer base. It must effectively inform the private/public sectors of foreign intelligence threats/exploitation, enhance counterintelligence awareness, enable and empower effective counterintelligence investigations and operations by operational elements which achieve results and impose cost on adversarial elements.
- Strengthen the Security Enterprise. The NCSC must further strengthen the security enterprise through increased standardization of security standards, personnel security, operational security, polygraph, technical security, physical security, and reciprocity.
- Expanded Support to Non-Title (NT)-50s. The NCSC, in partnership with the NCITF, must expand support to NT-50s, the often targeted and hard to protect entities of the USG which provide gateways for nefarious foreign intelligence efforts.
- Value. The NCSC must be valued by the DNI, interagency and public/private sectors. In order to be valued, we must meet the needs of our consumers.

Counterintelligence Threats

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

There are numerous emerging critical counterintelligence threats. Foreign entities are exploiting our critical infrastructure, targeting our economic base, infiltrating our academic/defense research and technology development, and targeting all aspects of our society. China uses a whole-of-society approach to exploit the U.S. with non-traditional collectors, third country national co-optees, and exploitation of our business communities with near impunity in the U.S. homeland. While traditional and technical collection is still a constant activity, non-traditional collection is frequently harder to detect, deter, and counter. Non-traditional collection is often not illegal or pursued for prosecution given the difficulty in proving a legal offense. Areas traditionally not associated with being counterintelligence risks, such as biotech and agriculture are also impacted. Foreign intelligence services relentlessly target emerging technologies such as artificial intelligence and quantum computing in the defense, academic, and private sector environments. Unmanned vehicles also pose new risks which we are not well postured to address. Numerous foreign nationals have been identified flying drones near critical U.S. infrastructure and defense facilities. Innovative approaches to collect agricultural data are underway by foreign companies using legitimate business models. While it is not necessarily illegal, they present a vulnerability and potential advantage to adversarial powers.

Most at risk for non-traditional collection and hardest to defend include:

- Academia (key hubs for research and development)
- Non-Title 50 USG elements
- Information management systems, including cyber systems
- Critical infrastructure
- Private sector businesses (economic exploitation)

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

If confirmed by the Senate, my priorities for the NCSC would be:

- Establish the NCSC as the center of gravity for the whole-of-government /whole-of-nation “Counterintelligence Fight.” I would look to ensure that the NCSC enables interagency collaboration and leverages agencies’ respective authorities/mission areas to achieve counterintelligence effects.
- Enable interagency action by the whole-of-government, using agencies’ unique expertise and authorities to achieve counterintelligence effects against adversarial activity. The intent is to impose cost on the adversary for insidious

exploitation of the United States.

- Bridge the federal law enforcement/IC gap. Frequently there is a gap in the information flow, operating systems, and shared understanding of the federal law enforcement community and the IC. Law enforcement elements frequently have information of value to the IC and vice versa. Enhanced collaboration between these elements will improve our national capabilities to fully identify and take action against emerging threats.
- Establish partnership with the National Counterintelligence Task Force (NCITF) in full coordination with the Federal Bureau of Investigation (FBI), Department of Defense (DoD) and interagency partners.
- Advocate for the establishment of a formal counterintelligence professional career field. There is currently no Office of Personnel Management (OPM) recognized job series for counterintelligence professionals. Organizations across the USG use varying job series to execute counterintelligence activities, including 1811 (Criminal Investigator); 0132 (Intelligence Specialist) and 0080 (Security Specialist). This leads to disparate training, execution and understanding of counterintelligence across the IC and whole-of-government.
- Advance security efforts, specifically continuous evaluation, Trusted Workforce 2.0, reciprocity, ensuring consistent polygraph use for access to sensitive compartmented information (SCI).
- Expand partnerships with state, local, tribal, territorial governments, as well as private industry and U.S. academia.
- Enhance reporting of counterintelligence incidents across the whole-of-government and ensure that actionable leads are appropriately passed to the USG entities who have the expertise and authority to action those leads.
- Solve hard counterintelligence and security issues challenges by utilizing a whole-of-government, interagency approach.

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

If confirmed by the U.S. Senate, I would immediately conduct a review of the structure, personnel, and budget of the NCSC to ensure that it meets statutory obligations and priorities of the DNI to achieve results. I will identify areas where the NCSC can improve its performance to achieve substantive results. As needed, and under the direction of the DNI, I will optimize the structure, skill sets, and

manning of the NCSC to best meet its organizational mission.

I will collaborate with the FBI and DoD to immediately expand partnership with the NCITF to better link the NCSC with the whole-of-government counterintelligence effort and more effectively bridge the gap between the IC and federal law enforcement entities. This will also enhance the flow of counterintelligence leads and enable IC/LE elements to further their engagement/liaison with foreign partners regarding counterintelligence threats.

I will work with OPM and interagency partners to establish a formally recognized counterintelligence professional career field and designator.

NCSC will conduct a review regarding the health of the security enterprise and identify areas that require additional attention. As issues are identified, I will coordinate with the DNI (who serves as the Security Executive Agent) to address any issues or challenges.

I will explore opportunities to refocus NCSC's "engagement team" to enhance not only private/public sector engagements, but opportunities to increase awareness for the American public of the nefarious and sinister threats posed by adversarial intelligence/foreign malign influence.

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

There are numerous counterintelligence threats that have been underestimated by the U.S. counterintelligence community for too long. In many cases adversarial entities work with impunity in the U.S. homeland, exploiting the seams and varying definitions/understanding of "counterintelligence" across the USG. China uses a whole-of-society approach to exploit all aspects of U.S. society.

Non-traditional collectors exploit the U.S. academic community, research and development efforts, and economic entities of our nation. In many cases, these non-traditional collectors are not committing crimes associated with traditional counter-espionage activities and fall below the level of interest of federal law enforcement entities due to no "known affiliation" with foreign intelligence entities. Numerous examples include the operation of drones over military bases/critical infrastructure by Chinese nationals in the U.S. on student/tourist visas, and exploitation of

academic/defense research to the benefit of the People's Republic of China defense industrial base. This is particularly concerning in the areas of emerging disruptive technologies such as artificial intelligence, with both economic and national security implications. This situation is exacerbated by a lack of robust vetting of foreign nationals working/studying in Science, Technology, Engineering and Mathematics (STEM) fields at U.S. universities and private/public sectors. Foreign intelligence entities also exploit unexpected sectors such as biotech and agriculture, with the specific goal of undercutting the U.S. agricultural economic advantage. Foreign malign influence, executed through social media platforms to enflame social divisions in the U.S., downplay negative actions by adversarial elements, and encourage inaccurate favorable views of dictatorial regimes, represents an underappreciated threat to the U.S. population.

China takes a whole-of-government and whole-of-society approach to exploiting the United States. The NCSC must evolve and adapt to the non-traditional techniques used by China to effectively lead the U.S. whole-of-nation "Counterintelligence Fight."

QUESTION 11: 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 and other entities vis-à-vis their appeal as high-value targets for economic espionage?

The NCSC is statutorily directed to carry out and coordinate outreach efforts with elements of the USG and the private sector to provide awareness and warnings of counterintelligence threats (section 904 of the Counterintelligence Enhancement Act of 2002). Ideally, these outreach efforts would be conducted in partnership with local FBI Counterintelligence Task Force (CITF) elements, DoD, and Department of Energy counterintelligence elements, as appropriate. Doing combined outreach ensures relationships are established between action elements and consumers of the threat data. The NCSC should be coordinating across the IC to develop releasable products to support these outreach engagements and empower investigative and operational elements of interagency partners in support of the USG and private sector. The NCSC can also proactively work to identify the needs of the private sector and local governments to identify elements of information that will facilitate their ability to protect themselves and enhance reporting of suspicious counterintelligence or security issues to USG agencies that have the authority to take action.

QUESTION 12: If confirmed, how will you expand and institutionalize NCSC outreach to private sector entities whose technology and supply chains are of high interest to adversaries like the People's Republic of China?

If confirmed by the Senate, I would look to expand outreach to the private sector, not only on cyber, technology, and supply chains, but in all areas that are susceptible to foreign intelligence exploitation or foreign malign influence. I would pursue every opportunity to provide releasable data from the IC to "at risk" private/public entities in a timely, relevant manner and in conjunction with local FBI CITF, Department of Homeland Security (DHS), and DoD counterintelligence organizations, as appropriate. I will explore the opportunity to refocus NCSC's engagement team, to engage with private sector/state/local government entities with releasable data, in full coordination with local FBI CITFs and DHS partners, as soon as nefarious intentions are identified by the IC. While difficult to quantify, detecting, countering, and preventing adversarial exploitation before it happens is more effective than reacting.

QUESTION 13: Please describe the counterintelligence 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 presence of foreign nationals from adversarial nations at U.S. National Labs represent a long-standing threat to the long-term national security of the United States. This technique of foreign collection and exploitation of the U.S. is representative of the challenge of non-traditional foreign collection. In many cases, these personnel are participating in critical research then returning to adversarial nations to advance their defense industries and/or economic enterprises. In short, we are funding, training, and educating adversarial actors for the benefit of our adversaries and competitors. In many cases, these personnel are not committing any crime that can be prosecuted, but represent a vulnerability in our National Lab system. I do not view this as a linear China, Russia, Iran, North Korea problem set, but from a broader perspective. Frequently, the Talent Programs of the Chinese Communist Party fund the education of third country nationals and co-optees with an expectation of return for China. The USG should explore legally viable options to expand the vetting of foreign nationals working in U.S. National Labs to reduce the threats posed by this insidious exploitation of our nation.

Congressional Oversight

QUESTION 14: The National Security Act of 1947, Section 102A (50 U.S.C. § 3024) provides that the Director of National Intelligence (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?
- B. What are the Director of the NCSC’s specific obligations under Section 102A (50 U.S.C. § 3024), including as to the NIP budget?

My understanding of section 102A of the National Security Act is that the Director of the NCSC, in support of the DNI, is obligated to ensure that the congressional intelligence committees are informed of all matters relating to compliance with the Constitution and U.S. laws. As I understand it, the Director of the NCSC is also responsible to submit annual budget requests that meet the resourcing needs of NCSC for inclusion in the overall NIP Budget. Director, NCSC is also responsible to answer any additional requests from the DNI for the purpose of determining the annual consolidated NIP budget.

NCSC Authorities, Personnel, and Resources

QUESTION 15: Section 7305 of the *Intelligence Authorization Act for Fiscal Year 2024* (P.L. 118-31, Div. G) established that NCSC’s mission “shall include organizing and leading strategic planning for counterintelligence activities of the United States Government by integrating instruments of national power as needed to counter foreign intelligence activities.” If confirmed, how would you ensure that NCSC’s mission is executed according to this statutory requirement?

While the NCSC is statutorily prohibited from conducting counterintelligence investigations or operations, the NCSC can play a key role in enabling effective counterintelligence investigations, operations, and activities. By identifying emerging threats to specific sectors, the NCSC can work directly with interagency partners who have the authority, mission and ability to take action on those threats. A significant part of this effort will be a strong partnership with the NCITF, which has participants from over 50 USG organizations. The NCITF represents the most effective bridge to

action elements available to the interagency. The NCSC is not able to direct action against specific target sets at the tactical level, vulnerabilities, or threats, but it does have the capability to synergize interagency efforts that result in action by individual agencies and partners. Counterintelligence threats and foreign influence challenges remain complex and ever-evolving. No single agency in the USG has the expertise or authorities to address adversarial efforts to exploit all aspects of U.S. society. Agile, whole-of-government interagency solutions are needed to address complicated counterintelligence problems. If confirmed, I intend for the NCSC to lead those efforts in a collaborative manner that achieves results and imposes cost on nefarious adversarial activity.

QUESTION 16: Please describe your authorities over the counterintelligence offices within the IC.

The NCSC does not exercise direct authority over the counterintelligence entities of the IC or other government entities that work in the counterintelligence space. However, the NCSC does have the statutory authority to evaluate the counterintelligence community's implementation of the National Counterintelligence Strategy. In addition, the National Intelligence Manager – Counterintelligence (NIM-CI) participates in the DNI National Intelligence Priorities Framework (NIPF) and the DNI Intelligence Planning Programming, Budgeting and Execution (IPBBE) process and strongly influences counterintelligence priorities, funding decisions, and counterintelligence results achieved by the counterintelligence elements of the IC.

QUESTION 17: Do you see any need for modifications to the statutory role or authorities of the Director of the NCSC? If so, please explain.

Not at this time. If confirmed, I will look to complete a holistic review of the NCSC (budget, personnel, mission function areas). This review will enable me to identify any updates needed to the statutory roles and authorities of the NCSC. If updates are needed, I will work with the Senate Select Committee on Intelligence and House Permanent Select Committee for Intelligence on any proposed changes, after consultation with DNI Gabbard, and through OMBs legislative proposal processes. Of note, the NCSC does not need the authority to execute investigations or operations; the NCSC should serve as the nerve center of the U.S. counterintelligence and security communities, synchronizing the unique expertise/authorities of the whole-of- government to achieve counterintelligence effects.

QUESTION 18: What is your view of the NCSC's size and function?

While I have not yet had the opportunity to execute a complete review of the NCSC structure and mission focus, I assess that the current size of the NCSC is adequate to satisfy current statutory and DNI requirements. However, I believe that that current structure must be optimized and the focus areas improved to ensure that the NCSC is not duplicating other activity being conducted in the USG. If confirmed by the Senate, one of my top priorities will be to conduct a line-by-line review (budget, personnel, and function) to identify areas of redundancy gaps in the national counterintelligence and security communities, and efficiencies.

QUESTION 19: Do you believe that the NCSC has sufficient personnel resources to carry out its statutory responsibilities effectively? If not, where does NCSC require additional personnel resources? If so, where should NCSC streamline its personnel?

As I am not currently in the role of Director, I look forward to having the opportunity to fully assess the NCSC and ensure alignment with statute, the National Counterintelligence Strategy, the President's priorities, DNI priorities, and Congressional priorities.

QUESTION 20: In your view, what are the competing values and interests at issue in determining to what degree there should be a permanent cadre of personnel at the NCSC, or at any of its components, and to what degree the NCSC should utilize detailees from the IC elements?

Detailees from across the IC are critical to refresh the currency of expertise and bring the most recent, relevant experience to the NCSC. The threats posed by our adversaries are constantly changing and require an agile, adaptable enterprise to counter them. While IC detailees are of significant value, the modern "Counterintelligence Fight" requires collaboration across the whole-of-government to leverage the unique perspectives, expertise, capabilities and authorities of the entire USG enterprise. This includes organizations that have not traditionally had many representatives at the NCSC, such as DHS, NT-50s, and federal law enforcement organizations. Both detailees, working under the authorities and management of NCSC, and assignees, collaborating with the NCSC but working on behalf of and under the authorities of their home organizations, are of value to a collaborative effort. Detailees should be of exceptional quality, in place for a set period of time, and work to advance the organizational mission of the NCSC vice influencing the NCSC on behalf of their home organization. Assignees can provide critical linkages to home agencies to forward the shared goals of the NCSC and partner organizations. Cadre positions ensure NCSC continuity and synchronization with the business practices of

the ODNI. If confirmed by the U.S. Senate, I will review the current structure to maximize the impact of cadre, detailee, assignee, and contractor manning of the NCSC, with the intent to maximize efficiency.

QUESTION 21: What are your views on the NCSC's intelligence budget in the short-, medium-, and long-term? In what areas should the intelligence budget be modified, and how?

If confirmed by the U.S. Senate, I am committed to initiating a line-by-line review of the NCSC budget to ensure that funding is achieving results for the American taxpayers as envisioned by the U.S. Congress. Upon review, I will look to address areas that require improvement under the direction of DNI Gabbard and in full collaboration with the U.S. Congress. If I identify budget shortfalls or areas that require additional investment due to evolving techniques of adversarial actors, I would first look to address these shortfalls internally, in accordance with specific Congressional allocations for NCSC, before highlighting the need for additional budget resources. Of note, a significant portion of the NCSC budget is apportioned towards the security portfolio, which reduces the risks posed by potential insider threats and secures classified information for the IC and greater government enterprise.

QUESTION 22: What reforms are required to ensure that NCSC's personnel and resources are in line with NCSC's value to the ODNI and the larger IC? Have you discussed these reforms with Director Gabbard?

If confirmed by the U.S. Senate, I will look to optimize the NCSC structure, manning, and budget to achieve results for the DNI, whole-of-government and nation writ large. I will establish the NCSC as the center of gravity for the whole-of-government "Counterintelligence Fight," I will expand NCSC partnership with the NCITF, which should serve as a key linkage for the NCSC to field elements. I will enable field elements to be more effective in conducting investigations and operations that achieve effects and impose cost on adversaries. I will review the current manning/expertise at the NCSC to ensure we have the right skill sets/expertise applied against the right problem sets. I will explore cost saving solutions for the management of the U.S. counterintelligence community. I will continue to strengthen security practices across the IC and whole-of-government (Trusted Workforce 2.0, polygraph, protection against technical collection, National Operations Security Program Office), identify and address supply chain threats, and secure U.S. innovation. If confirmed, DNI Gabbard expects me to provide a return on investment for the American taxpayer;

achieve substantive results; optimize NCSC structure; impose cost on adversaries; and be transparent with the U.S. Congress.

NCSC Analysis

QUESTION 23: What unique role does NCSC's strategic counterintelligence analysis play, as compared to the analysis produced by other IC components?

All source analysis of counterintelligence related information is generally done by the IC writ large, vice the NCSC directly.

As directed by the DNI, the NCSC conducts damage assessments of significant compromises of national security information and assessments of lessons learned from counterintelligence activities. Damage assessments provide key insights into foreign intelligence collection techniques, may provide additional leads for counterintelligence law enforcement investigation referral, identify mitigation measures, and identify potential avenues to prevent future compromises.

NCSC should also play a key role in federating the disparate counterintelligence analytical enterprise to cross-pollinate best practices, synergize analytical partnerships, track new developments, and ensure the community's analysis is focused on national counterintelligence priorities. Collaborative counterintelligence analysis across interagency/organizational boundaries can better enable holistic action by field elements.

The NCSC is also statutorily required to produce the National Threat Identification and Prioritization Assessment (NTIPA) and the National Counterintelligence Strategy (NCS) under the Counterintelligence Act of 2002 (section 904 of the Counterintelligence Enhancement Act of 2002). The NTIPA effectively fuses input regarding emerging threats identified across the IC into a consolidated assessment that identifies the most significant issues. The NTIPA enables the production of the NCS, which is used by the IC and interagency partners to focus their respective counterintelligence activities. Additionally, the NCS is published at the unclassified level for public release, allowing for sharing with private industry, academia and local elements to expand public awareness of counterintelligence issues. These documents represent interagency analysis.

QUESTION 24: What is the NCSC's role in coordinating and publishing the IC's counterintelligence assessments?

As directed by the DNI, and in consultation with the appropriate agencies and departments of the USG, NCSC oversees and coordinates the production of strategic counterintelligence analysis. The NCSC is directly responsible for the National Threat Identification and Prioritization Assessment (NTIPA). The NTIPA identifies the most current trends in adversarial collection against the U.S. and partner nations. It is produced in coordination with the IC and other federal partners. It reflects the most current concerns of the IC and U.S. decision makers regarding the full range of foreign intelligence threats to the U.S. and partner nations. Given that collaboration with foreign partners is critical to successful counterintelligence activities, the NCSC also produces releasable versions of the NTIPA for use by the appropriate LE and IC elements in counterintelligence liaison activities. The NCSC should also play a role in federating the whole-of-government counterintelligence analytical enterprise, specifically through hosting collaborative forums to enhance counterintelligence analysis, investigations, and operational activity from a broader perspective that includes the IC and other government elements impacted by or taking action against foreign collection efforts.

State and Local Governments

QUESTION 25: 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?

- 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?

The NCSC does not have a role in directly producing or disseminating finished intelligence for distribution to state, local and tribal partners. However, the NCSC should play a role in identifying threats to these elements, coordinating releasable products to these organizations from within the IC, ensuring awareness by these entities of the threats, and empowering them to defend their own equities. The NCSC can accomplish this by sharing best practices that raise awareness and explain the

risk, in full partnership with FBI field Counterintelligence Task Forces and DHS field entities. NCSC should look to expand partnership and collaboration with both DHS and FBI field offices as the action elements closest to the problem set. While these linkages do exist, they are uneven and often based on personal relationships vice institutionalized relationships. FBI and DHS entities are frequently focused on law enforcement/counterterrorism activities vice vulnerabilities and awareness of broader counterintelligence threats. Effective, institutionalized collaboration between FBI, DHS, and NCSC will enhance the mission of all three organizations, expanding reported incidents and allowing for both criminal investigations and counterintelligence operational potential for field elements. Many of the vulnerabilities encountered by state, local, and tribal entities fall below the cut line for DHS/FBI action, but can be of interest to the greater counterintelligence community, interagency partners, and the IC. Exploring co-location of the National Counterintelligence Task Force with NCSC would assist in the ability to address complex challenges from an interagency perspective and bridge organizational culture and mission gaps. The NCSC also participates in the ODNI's Federal, State, Local, Tribal and Territorial (FSLTT) Partnerships Group in order to support the whole-of-nation effort.

National Intelligence Manager for Counterintelligence

QUESTION 26: What is your vision of the Director of the NCSC in the role of National Intelligence Manager for Counterintelligence?

As the National Intelligence Manager for Counterintelligence (NIM-CI), the Director of NCSC should set priorities for counterintelligence analysis, and collection requirements and integrate the community's activities to support counterintelligence priorities. These priorities should be based on our holistic understanding of current foreign intelligence entity activities, target areas, target technologies, and analysis from across the IC. The NCSC does this through the National Counterintelligence Strategy, the NTIPA, and supporting the DNI's budgeting process through the Intelligence Planning, Programing, Budgeting, and Evaluation (IPPBE) system as outlined in Intelligence Community Directive 116. As the NIM-CI, the IPPBE allows the NCSC to ensure resources are dedicated against the most current priorities.

QUESTION 27: What is the Director of the NCSC's role in developing the National Intelligence Priorities Framework with regard to counterintelligence?

In accordance with the DNI's statutory authorities and ICD 204, the National

Intelligence Priorities Framework (NIPF) serves as the primary mechanism to focus the IC on national intelligence priorities for collection and analysis. As the NIM-CI, the Director, NCSC, is responsible for supporting the DNI updates to the NIPF from a counterintelligence perspective.

QUESTION 28: What is the Director of the NCSC's role in providing guidance on resource allocation with regard to particular counterintelligence capabilities and platforms?

As the NIM-CI, the Director, NCSC, is responsible to support the DNI IPPBE process to ensure resource allocation through the National Intelligence Program budget (in accordance with ICD 104) and supports the DNI's participation in the development of the Military Intelligence Program (ICD 900) for specific areas of counterintelligence focused capabilities, platforms and focus areas.

QUESTION 29: What is the Director of the NCSC's role in providing guidance with regard to the allocation of resources among and within IC elements?

As noted in the responses to questions 26, 27 and 28, the Director, NCSC provides guidance to the allocation of resources regarding security and counterintelligence by acting as the NIM-CI, participating in the DNI IPPBE process, and the DNI NIPF process. The Director, NCSC, continuously assesses the performance of the counterintelligence and security efforts across the IC, identifies areas that need additional resources, and identifies areas that are not producing the expected results (as identified by the NIPF requirements). NCSC does not directly allocate resources to IC elements, but influences resourcing decisions of the DNI through the IPPBE.

QUESTION 30: Given resource constraints, how should the Director of the NCSC identify unnecessary or less critical programs and seek to reallocate funding?

The Director of the NCSC is responsible to identify unnecessary or low priority programs through evaluation of the counterintelligence and security executors, collaboration with IC partners, the NCSC-led National Counterintelligence Policy Board and National Counterintelligence Strategy and Resources Board, and direction from the DNI. Given the constantly evolving nature of the counterintelligence landscape and threats posed by adversarial entities, consistent evaluation of the current state of play is necessary. While the National Counterintelligence Strategy and the National Threat Identification and Prioritization Assessment are helpful tools,

we must be mindful of the agility and creativity of adversarial actors. Specifically, the Chinese Communist Party has shown their ability to react to ongoing events and capitalize on perceived vulnerabilities in the U.S. While security related efforts often have more continuity, we must ensure that our security efforts are keeping pace with emerging technical threats and cyber threats. The Director, NCSC does not directly allocate/reallocate funds, but participates in the DNI's Intelligence Planning, Programming, Budgeting and Execution (IPPBE) process to focus resources on higher priority requirements.

QUESTION 31: What are the most important counterintelligence gaps and shortfalls across the IC? If confirmed, how would you address these gaps and shortfalls?

The U.S. counterintelligence community lacks a defined center of gravity, a central touch point, and a shared understanding of exactly what constitutes counterintelligence. A patchwork of authorities and responsibilities in both counterintelligence and security across the U.S. government further complicates this challenge. In addition to these challenges, there is no formally designated job series for counterintelligence professionals recognized by the Office of Personnel Management in the U.S.G. There are no recognized standards for the conduct of sensitive counterintelligence activities, with each organization establishing varying standards for executing and classifying sensitive counterintelligence activities. Our adversaries are consistently innovative, and exploiting the seams between USG organizational responsibilities to exploit our research, development, academia, and private and public sectors to their advantage. In many cases this insidious exploitation of our nation is executed using non-traditional means which are not illegal or readily identifiable as traditional espionage activities. In many cases, our adversaries act with impunity in our homeland, exploiting our critical infrastructure (VOLT TYPHOON, SALT TYPHOON). China has even brazenly flown a spy balloon over the U.S. heartland. These actions will continue by adversarial elements until we impose a cost on the adversary for their nefarious activities.

If confirmed by the U.S. Senate, I will look to empower and enable the whole-of-government enterprise, using the unique authorities/expertise of each organization to impose cost on the adversary. I will pursue the establishment of a formal counterintelligence job series, explore avenues to better support NT-50 organizations and enhance partnerships with private industry, academia and local governments – all of which represent the most targeted, vulnerable areas to our adversaries. Closer partnership with the National Counterintelligence Task Force will provide a key avenue to bring the NCSC closer to the operational organizations which can take

action on emerging threats.

Insider Threats and Unauthorized Disclosures

QUESTION 32: What is the role of the NCSC in preventing insider threats and unauthorized disclosures?

The NCSC currently hosts the National Insider Threat Task Force (NITTF). Further, countering insider threats is the inherent mission set of both the counterintelligence and security communities within the USG. Adversarial elements seek to collect information, both classified and unclassified from the whole of the U.S. government, academia, private industry, state, local and tribal governments, the agriculture, and biomedical sectors. Insider threats pose a threat across the full spectrum of these sectors to the benefit of adversary intelligence services and economic competition. While the NITTF is a helpful tool within U.S. federal government structures, the outreach conducted by the NCSC is key to supporting the threats to the entire nation.

QUESTION 33: How does the NCSC work with the FBI's National Insider Threat Task Force to deter, detect, and mitigate insider threats?

In accordance with Executive Order 13587, the NITTF is co-chaired by the Attorney General and Director of National Intelligence (or their designees). The NITTF is currently hosted at the NCSC and staffed by NCSC personnel. The NITTF works to enhance and assess the Insider Threat programs of executive branch entities. The collaborative assistance of the NITTF is particularly important to NT-50 agencies, for which insider threat guidance frequently comes with limited (if any) resources to detect, deter and mitigate insider threats. The NCSC, under the leadership of the DNI, continues to support USG partners to solidify their current insider threat efforts.

QUESTION 34: What is your plan to ensure success in preventing insider threats and unauthorized disclosures?

Preventing insider threats and unauthorized disclosures fits squarely in the center of the NCSC mission set. The insider threat problem is inherent to both the security and counterintelligence enterprises. Current NCSC activities addressing this problem set include the National Operations Security Program, continued implementation of the security continuous evaluation program, and polygraph program. I would look to expand the polygraph requirement for personnel with access to sensitive compartmented information (SCI) information, close gaps between differing

information systems and classified information access requirements for IC organizations, and ensure the appropriate, written referrals to the Department of Justice and Federal Bureau of Investigation in support of DNI Gabbard's initiative to address unauthorized disclosures. While written referrals to the DOJ and FBI are important from a law enforcement perspective, written referrals regarding unauthorized disclosures to home organizations that fall below prosecutorial benchmarks can result in administrative actions and/or security clearance revocations for perpetrators. In regards to the threats in the cyber domain, expanding detection mechanisms to ensure the protection of classified information is a critical aspect that I would look to expand. Also of note are the damage assessments conducted by the NCSC in support of the DNI; these damage assessments can identify investigative leads for referral to law enforcement, enhance our awareness of foreign intelligence techniques, serve as a deterrent to potential insider threats, identify trends to inform the security/continuous evaluation process, and identify mitigation measures when compromises do occur.

Acquisition and Supply Chain Risk Management

QUESTION 35: 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?

The NCSC should set priorities for counterintelligence collection against threats, analysis of threats, and advocacy for security of critical U.S. supply chains. This is particularly relevant in emerging and previously underappreciated areas of the supply chain such as rare earth minerals, which have the potential for national security and economic impacts. Through the DNI enterprise, the NCSC should be tracking all emerging counterintelligence threats to key U.S. supply chains, keeping the DNI, executive branch and U.S. Congress informed of emerging trends and vulnerabilities to current and future supply chain equities at both the classified and unclassified level. The NCSC can share unclassified information with private industry and academia to inform these entities of adversarial intentions vis-à-vis the supply chain. The NCSC can also serve as the connective tissue between supply chain centers of excellence in the IC, the acquisition community, the federal law enforcement community and consumers to enable real action by field elements to confound nefarious efforts to exploit the U.S. supply chain.

Question 36: 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?

Preventing and mitigating threats to the U.S. supply chain starts with effective analysis to identify emerging counterintelligence threats and federating the USG Supply Chain Risk Management (SCRM). There are silos of excellence regarding SCRM across the IC, which are frequently disconnected from elements that can actually take action on identified threats. Adversarial actors are and will continue to be innovative in their approaches to compromise U.S. supply chains, particularly for foreign sourced products and services. Adversaries will use all available means (both legal and illegal) to obfuscate their nefarious activities. While the NCSC does not and should not conduct redundant SCRM activities, the NCSC can play a key role in establishing priorities for collection against counterintelligence threats to the supply chain, prioritize IC analysis on vulnerabilities in the supply chain and the provision of actionable information to the acquisition community, federal law enforcement elements, and IC elements. This will enable law enforcement actions, acquisition actions, and law enforcement/intelligence liaison with foreign partners to mitigate and disrupt emerging threats. If confirmed by the Senate, I will look to enhance the NCSC’s role as a nerve center for SCRM prioritization/collaboration from a counterintelligence perspective, enabling action by field elements. I would define success in this regard as investigations by federal law enforcement, disruptions of adversarial efforts to exploit our supply chain, counterintelligence operations to exploit adversarial efforts, disruption of adversarial activities by partner nations, contract debarments, and stronger security of our supply chain from the research and development phase through acquisition.

QUESTION 37: 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?

While the NCSC is statutorily prohibited from carrying out CI investigations or operations (section 904 of the Counterintelligence Enhancement Act of 2002), NCSC may leverage the analytical elements of the IC to provide actionable information to partners in the federal law enforcement/whole-of-government enterprise for further action. Establishing strong partnerships and collaboration with action elements such as the FBI, DHS (Customs and Border Protection, Homeland Security Investigations), Department of Commerce, DOD, NSF, HHS, and other USG partners enable measurable action. In addition to actual action on current threats by the entities with

the appropriate authorities, enhanced outreach with private industry, academia, partner nations (in full coordination with local federal partner organizations) at the unclassified/releasable level regarding emerging threats by adversarial actors provides an opportunity to enhance reporting, disrupt adversarial collection, and enable private entities to protect themselves to a greater extent.

Professional Experience

QUESTION 38: Please describe specifically how your experiences would enable you to serve as the Director of the NCSC.

I have nearly 30 years of full spectrum counterintelligence experience in nearly every aspect of the mission as both an active duty and U.S. Army Civilian Counterintelligence Special Agent. I have conducted, led, and managed the full spectrum of counterintelligence investigations and operations from the tactical level in peacekeeping and combat operations to the strategic level in partnership with interagency partners. I have conducted activities in both the United States and globally with the U.S. Intelligence Community, foreign partner nations, federal law enforcement partners, state and local partners, private industry, and NT-50 organizations. I have represented the DoD as the Deputy Director of the FBI-led interagency National Counterintelligence Task Force. I have led, managed, and coordinated counterintelligence/security technical services including technical security countermeasures, polygraph, cyber efforts, research and technology protection, and interagency task forces for cyber, counterintelligence, and counterterrorism. I have led large scale damage assessments regarding significant compromises of classified information. I have established new partnerships to evolve the understanding of, and action against, emerging counterintelligence/security threats including non-traditional collection and exploitation of U.S. research. I have conceived, coordinated, and implemented sensitive interagency activities to impose cost on and neutralize adversarial collection efforts. I have a unique understanding of the gap between the federal law enforcement community and the IC – I know how to bridge that gap in a collaborative manner that utilizes the unique authorities and expertise of interagency partners, which achieves substantive results. The breadth and depth of my unique experience is rare in the whole-of-government counterintelligence/security community.

FBI Background Investigations

QUESTION 39: Should the FBI conduct background investigations of all

Presidential nominees for positions within the executive branch of the federal government to ensure that those under consideration for positions of significant authority and responsibility will not misuse the power of their offices and do not have vulnerabilities that make them susceptible to coercion by our adversaries?

Yes, all Presidential nominees should undergo background investigations.

QUESTION 40: Have you undergone, or will you undergo, an FBI background investigation as part of the process associated with your nomination?

Yes, I have. I also most recently completed a polygraph examination on 10 April 2025. I have held a TS/SCI clearance for over 30 years, completed several polygraph investigations and undergone numerous background investigations in order to meet all security and special access requirements.

QUESTION 41: Do you agree to provide the results of your FBI background investigation to the Chairman and Vice Chairman of this Committee for review?

Yes.

Workforce Protection

QUESTION 42: Will you commit that, if confirmed, you will seek to recruit, attract, and retain a workforce based on principles of fairness and merit, and without consideration of personal political preferences?

Yes.

QUESTION 43: Do you commit to consider professional qualifications in personnel decisions exclusively, without consideration of partisan or political factors?

Yes.

QUESTION 44: Would you ever consider an individual's personal political preferences, to include "loyalty" to the President, in making personnel decisions, such as to hire, fire, or promote an individual?

If confirmed by the U.S. Senate, I fully commit to ensuring that all employees at

NCSC are treated with respect and without regard to their personal political preferences. Throughout my career I have always maintained apolitical leadership in the workplace. I have been and remain focused on the mission, authorities, organization, and technical expertise/performance of the workforce.

QUESTION 45: If confirmed, what assurances will you provide to the NCSC workforce that personnel decisions will be based exclusively on professional qualifications, performance, and needs and not on personal political preferences?

If confirmed by the U.S. Senate, I fully commit to ensuring that all employees at NCSC are treated with respect and without regard to their personal political preferences. Throughout my career I have always maintained apolitical leadership in the workplace. I have been and remain focused on the mission, authorities, organization, and technical expertise/performance of the workforce.

QUESTION 46: Will you impose a political litmus test for NCSC employees? Is a political litmus test ever appropriate in determining who can or should work in NCSC?

No. Employees in the U.S. Intelligence Community and NCSC should be selected based on their specific skills, work performance and needs of the organization. The work of the U.S. Intelligence Community must be apolitical. The personal political positions of employees are irrelevant to the mission of NCSC.

Questions from Senator Warner

Legal Compliance

QUESTION 47: If confirmed, will you commit to expend the funds authorized and appropriated by Congress for the NCSC and to formally notify Congress and obtain approval for any recessions or deferrals, in accordance with the law?

Yes.

QUESTION 48: If confirmed, will you commit to ensure that all personnel actions taken by the NCSC are carried out in strict accordance with the law?

Yes.

QUESTION 49: If confirmed, will you commit to comply with all duly issued court orders or other rulings, even if you disagree with the court's decision?

Yes.

Department of Government Efficiency

QUESTION 50: If confirmed, will you commit not to accept direction from the Department of Government Efficiency (DOGE) on any personnel or other matters relating to NCSC?

If confirmed as the Director of the NCSC, I will ensure that I, and NCSC personnel, follow all legal directives and guidance of the Director of National Intelligence.

QUESTION 51: If confirmed, will you commit to prevent DOGE from accessing NCSC systems?

I will follow all legal guidance and directives of the DNI. The NCSC space and systems are at the classified level and I will always maintain appropriate security protocols for any/all access to any NCSC systems.

Protecting Classified Information

QUESTION 52: Should any employee of the Intelligence Community be granted access to classified information if they have not been determined to be eligible for access under Executive Order 12968 based upon a favorable adjudication of an appropriate investigation of the employee's background?

Generally, no. EO 12968 requires employees of the U.S. Intelligence Community to undergo the appropriate background investigation and be favorably adjudicated prior to accessing classified information. However, EO 12968 does provide an accommodation for exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudicative process, allowing temporary access to classified information in such cases.

QUESTION 53: Do you agree that all personnel granted access to classified information have a lifetime obligation to protect that information, including after they leave government service?

Yes.

Ethics

QUESTION 54: Federal ethics laws, to include 10 U.S.C. §208, prohibit government employees from participating in matters where they, or certain family members or organizations with which they have certain relationships, have a financial interest. Do you agree, without qualification, if confirmed, to disclose any potential conflicts of interest, including investments, business ties, family relationships, or other connections that could be perceived as influencing your decision making?

Yes. If at any time there is ever any question or potential conflict of interest, I will immediately report it and consult with the appropriate ethics attorneys.

QUESTION 55: Do you agree, without qualification, if confirmed, that if a conflict of interest arises, you will recuse yourself from participating in any relevant decisions regarding that specific matter?

Yes. I completely agree with this standard. I am obligated, legally and morally, to follow all ethical standards.

QUESTION 56: Do you commit, without qualification, if confirmed, to decision-making on the merits and exclusively in the public interest, without regard to private gain or personal benefit?

Yes.

National Counterintelligence Strategy

QUESTION 57: On August 1, 2024, NCSC publicly released a new National Counterintelligence Strategy. Do you agree with the goals and plans laid out in the Strategy? What would you change? If confirmed, what immediate actions will you

take to implement the strategy?

Yes. I agree with the goals and plans laid out in the National Counterintelligence Strategy. I agree that China represents the most prolific threat to the national security and economic security of the United States, followed by other adversarial actors of Russia, Iran and North Korea. However, I do not see the threat as linear and only emanating from those nations. Foreign intelligence entities, including China, Russia and Iran are innovative in their approaches to exploit all aspects of U.S. society. We can expect that they will use all aspects of their enterprise, including non-traditional collection, unmanned systems, third country nationals and co-opted U.S. persons to achieve their collection, exploitation and influence objectives. The whole-of-government/whole-of-nation “counterintelligence fight” is in a constant state of evolution. We must be agile in our response. Addressing these challenges takes a whole-of-government and whole-of nation approach. Given that the NCSC is statutorily prohibited from conducting counterintelligence investigations and operations (as outlined in section 904 of the Counterintelligence Enhancement Act of 2002), enhanced collaboration across federal entities is critical to success. In addition to the commonly recognized partners associated with counterintelligence (DOJ, FBI, DoD, DHS), this collaboration must be expanded to NT-50 federal organizations, state, local, tribal entities, private industry, academia and the American public. If I am fortunate enough to be confirmed by the Senate, I will immediately look to expand and strengthen partnerships/engagement with all entities, in full partnership with the FBI, DoD, and DHS. My intent would be to achieve results and impose cost on adversarial actors exploiting the nation and report those results to Director of National Intelligence Gabbard and the U.S. Congress.