# MICHELLE VAN CLEAVE
## Answers submitted in response to questions for the record

# U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE
## September 21, 2022
## Open Hearing on Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center

**Changes in the Counterintelligence Mission**

1. **Should the statutory definition of counterintelligence be updated to include foreign malign influence and malicious cyber activities?**

In my view, the current statutory definition of counterintelligence (CI) [1] is broad enough to encompass malign influence and malicious cyber activities to the extent that CI has a role to play in countering them. Unlike *espionage* directed against the United States, these threats are not the exclusive concern of counterintelligence, but by law fall under multiple authorities. For example,

- Under current law, the Foreign Malign Influence Response Center (50 USC 3058) is to be composed of personnel from all elements of the intelligence community (IC), including those with diplomatic and law enforcement functions.
- Lead authorities over counter-cyber operations are vested in the Secretary of Defense (10 USC 394), who shall "conduct military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power." Those authorities explicitly include "operations in cyberspace short of hostilities."

While it might be helpful to clarify that the term "other intelligence activities" in the definition of counterintelligence includes malign influence and cyber activities, the new statutory language (or accompanying report) should reflect that countering these foreign threats is not exclusively a CI mission.

2. **How should strategic counterintelligence be defined in statute?**

The principal responsibility of counterintelligence, whether strategic or tactical, is to engage and confront the adversary, which means carefully orchestrated, proactive operations to influence, compromise, or disrupt hostile intelligence threats.

---

[1] 50 USC 3003(3): *The term "counterintelligence" means information gathered, and activities conducted, to protect against espionage,* **other intelligence activities***, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.* [Emphasis added]

As I understand the term,[2] what makes a CI effort "strategic" is the means-to-ends analysis (strategic operational planning) that identifies and assesses the "red" (Foreign Intelligence Service) "order of battle" (adversary plans, intentions and capabilities) and arrays "blue" (U.S. CI) assets to achieve defined objectives. In testimony, I offered the following draft definition:

> 50 U.S. Code § 3003(4) – Definitions. As used in this chapter … *(4) The term "strategic counterintelligence" means the direction and integration of counterintelligence activities to disrupt or compromise the ability of foreign intelligence services to harm U.S. national security interests at home or globally.*

If the United States is to have a national strategic CI capability, we will need some fundamental new elements, including a purposefully designed strategic CI program. But first, our national security leadership, and the professionals who lead U.S. counterintelligence, need an agreed understanding that such a national effort is in fact the goal. Defining the term in law – as the Committee's organizational assessment of the National Counterintelligence and Security Center (NCSC) recommends[3] -- would be a very constructive first step.

## The U.S. CI Enterprise

**3. Which legal responsibilities should non-IC entities—including U.S. government agencies, academic institutions, and private sector companies—have to protect their intellectual property, research, technologies, and data with national security implications?**

Government as well as private entities should and do have full legal and practical responsibility to develop and implement security measures to protect their sensitive data, facilities, operations, etc., whether the threat actors are domestic or foreign. They are in the best position to know what is of value and therefore what needs protection, to determine their level of risk (because they know the value of their strategic information, and they know their business), and to apply the security and countermeasures required.

While sound protective measures are unquestionably vital, they are only part of a broader effort to protect our nation's R&D base and other critical information against illicit foreign exploitation. We also need good counterintelligence, meaning that the U.S. government needs to be much more pro-active in identifying, assessing and disrupting foreign intelligence operations against us. Without the tools the U.S. counterintelligence enterprise alone can and must provide, we will continue to lose ground.

**4. Which incentives and resources could Congress provide to help non-Intelligence Community entities better protect their intellectual property, research, technologies, and data from foreign adversaries?**

---

[2] See for example Michelle Van Cleave, "The Question of Strategic Counterintelligence: What is it, and what should we do about it?" *Studies in Intelligence* 51, 2 (Washington DC: Center for the Study of Intelligence, Spring 2007) 1-13

[3] Senate Select Committee on Intelligence, *Organizational Assessment: The National Counterintelligence and Security Center,* Audits and Projects Report 22-01, United States Senate (2022), p132

The single most important resource Congress could provide is to establish in law a strategic CI program, managed by the head of U.S. counterintelligence and empowered to identify, assess and disrupt foreign intelligence operations directed against our commercial wealth, R&D base, critical infrastructures, democratic institutions, and sensitive national security information and activities. In testimony, I offered this draft mission statement:

> U.S. Strategic Counterintelligence shall degrade the ability of foreign powers to project force or prosecute national objectives; establish or maintain hostile control; or securely conduct operations or collect intelligence and other information against U.S. interests globally, by means of their intelligence activities.

**5. What are the biggest challenges academic and private sector entities face in confronting foreign adversarial intelligence collection and economic espionage?**

In order to protect themselves, America's universities and private enterprises need to be aware of the activities of foreign entities directed against them. For example, what are the practices and techniques of foreign intelligence services and their agents in acquiring proprietary and other information? Are they exploiting front companies, if so, which ones and how? What are their recruitment techniques? Their solicitation operations? Who and what are they targeting?

This is the kind of threat information that the FBI endeavors to provide to academia, business and industry, so their security professionals can do the realistic risk assessments required to protect the things they value. In my view, however, we have not invested nearly enough effort (funding, manpower, program execution) in identifying and assessing foreign intelligence operations, much less the CI operations needed to defeat them. Unless U.S. counterintelligence is able to gain better actionable insights into adversary intelligence activities, we will continue to lose ground.

**6. Given the generally lawful nature of foreign acquisition of U.S. technology, does Congress need to consider additional updates to the Committee on Foreign Investment in the United States (CFIUS) to address remaining loopholes?**

The welcome passage of FIRRMA in 2018, coupled with President Biden's new Executive Order 14093 (September, 2022), have given greater reach and specificity to CFIUS reviews and filing requirements, along with a schedule of penalties for failing to honor mitigation agreements. Whether those measures will be adequate remains to be seen, and at a minimum warrants Congressional monitoring with an eye toward additional updates as required.

The core challenge for CFIUS remains defining what constitutes a national security concern, on a case-by-case basis, and weighing that against our fundamental belief in free trade and open commerce, for the purpose of advising the President what to do. One major test case may well be the consortium (led by Elon Musk) that purchased Twitter earlier this year, which reportedly includes a number of foreign investors.

One of my responsibilities as the National Counterintelligence Executive (NCIX) was to provide analytic support to CFIUS concerning the bona fides of foreign investors seeking to acquire an interest in sensitive industries in the United States. At the time, I was concerned that in too many

cases the intelligence community lacked the insights necessary to make key judgments about these critical business dealings with sufficient confidence to enable informed decisions.

In order to exercise his authority under CFIUS, the President must have "credible evidence" that the foreign interest exercising control may take action detrimental to national security. That in turn requires that U.S. intelligence and counterintelligence be tasked and resourced to collect on those foreign interests. As the Congress considers updates to CFIUS, the Oversight Committees may also want to review whether those collection and analytic resources are adequate, not only to support CFIUS deliberations but for other actionable purposes as well.

**7. How can the U.S. government best strike a balance between protecting national security and preserving a culture of international collaboration, free enterprise, and open research?**

Having had the privilege over the years of working with some of our Nation's extraordinary scientists and engineers, I know the ethic and culture of openness that surrounds research and development are essential to nurturing ideas, innovation and progress. I am very respectful of these values, and I share them in full measure.

Unfortunately, the rich network of human interaction that is innocent and open and above board provides excellent cover for the sliver of activity that is none of that. Foreign collectors trained in the art of elicitation know how to obscure their true interests in a cushion of seemingly innocuous exchanges. They routinely exploit joint research undertakings or visits to U.S. businesses, defense contractors, military bases, research facilities, or academia, in order to obtain non-public information that may be valuable in itself, or provide leads to more sensitive sources or insights. The use of cyber tools as a collection modality is of particular concern, especially where informed or facilitated by human sources.

I don't know where the balance should be drawn, but I believe that it should be possible to find a balance that respects and supports our basic values. Within the United States we believe in the free flow of information, but we don't believe in insider trading. We believe in patents and copyrights that protect intellectual property. We believe in respecting the confidentiality of privileged communications. In short, we do recognize important constraints on the free flow of information; the increasingly urgent imperative is to extend like reason and fairness to the protection of our nation's critical information.

**8. What can be done to enhance U.S. government agencies' ability to conduct investigations into grant fraud and technology transfer, in collaboration with universities?**

I do not have any current insights into these criminal investigations, but would respectfully refer the Committee to the relevant law enforcement agencies (FBI, DOC/BIS, DHS/ICE, DoD/DCIS and the military service components) for their views.

**9. Should non-Intelligence Community agencies establish their own counterintelligence and/or security programs? If yes, what should those programs look like? If no, should the FBI or other Intelligence Community entities perform that role?**

Counterintelligence is inherently an intelligence mission ("*information gathered and activities conducted*" to counter foreign "*intelligence activities*"), which by definition is not the responsibility of non-IC agencies. By contrast, security is a distributed "command" or line function, for which each government agency (whether or not part of the IC) is separately accountable.

While there is always room for improvement, rigorous requirements for protective security programs are already in place and binding on non-IC agencies. For example, all government agencies with access to classified information are required to meet standards for detecting and mitigating insider threats (E.O. 13587). Security measures to protect national defense (i.e., classified) information are established by the DNI and binding on all who have access to such information, including such things as background investigations and adjudication standards for granting clearances as well as requirements for the retention and protection of classified documents both physical and digital (ICD 700 series). And all government agencies are responsible for establishing and executing security plans and programs to screen employees (based on position sensitivity and risk) for suitability, and to protect their sensitive information and operations (see for example E.O. 14028 "Improving the Nation's Cybersecurity").

By contrast, the defining job of counterintelligence is to engage and confront the adversary. To that end, the responsibility to identify, assess, and disrupt foreign intelligence services (including their agents and proxies) targeting U.S. national defense information, economic wealth, or democratic institutions, falls to those highly specialized CI agencies manned, trained and equipped expressly for that purpose and so designated by law and executive order (principally the FBI, CIA, and the military services).

I support the recommendation in the Committee's assessment of the NCSC[4] that the distinction between counterintelligence and security be codified in law. These are mutually reinforcing missions, yet each has separate and distinct roles, authorities and objectives, requiring very different resources, capabilities and metrics. The NCSC also needs to help clarify these distinct roles and missions so that each can be assigned, tracked and performed to best effect.

**10. To what extent should the State Department vet foreign students, professors, or employees from a counterintelligence perspective?**

Adversary intelligence services often use academics as well as businessmen and others to facilitate their operations within the United States. First line responsibility for vetting foreign visitors to the United States is assigned to U.S. Immigration and Customs Enforcement (ICE), Department of Homeland Security, as part of the visa application process. Where the need for additional scrutiny is indicated, applications may be referred to other government agencies (e.g., FBI, CIA) for review. Within the State Department, the Bureau of Diplomatic Security, deployed at consular posts abroad, is responsible for investigating suspected passport and visa fraud. I would respectfully refer the Committee to the respective government agencies for their views on whether these reporting channels and information sharing arrangements are being used to best effect.

---

[4] *Ibid*

**11. Should academic institutions do their own research security vetting of visiting students, professors, and employees?**

**a. What tools, resources, and support from the IC would be needed?**

Yes. Any institution of higher learning has a vested interest in ensuring visiting students and faculty are not abusing their academic affiliation for unlawful purposes. Alerts published by the federal government attempt to raise awareness of the ways in which foreign intelligence entities (FIE) exploit these ties.[5]

**12. How can the U.S. government in general and the Intelligence Community in particular better communicate the foreign intelligence threat to the American public, private sector companies, and academic institutions?**

Each year, reports out of U.S. counterintelligence show figures that are worse than the year before. Losses are growing. Numbers of foreign collectors are growing. Vulnerabilities are growing. And the erosion of U.S. security and economic strength is also growing.

Yet neither the recently issued *National Security Strategy of the United States*, nor the 2022 *National Defense Strategy*, addresses the threats posed by hostile intelligence services. If the American public is to have a better appreciation of what is at risk, and what is being lost, and what needs to be done to protect what we value, then our national leadership needs to give these matters the policy priority and prominence they deserve.

I would invite the Committee's attention to the fact that, as of this writing, President Biden has yet to name a head of U.S. counterintelligence. If the administration is serious about engaging the private sector in confronting foreign intelligence threats, filling this key leadership position would be an obvious place to start.

**13. How can the U.S. government in general and the Intelligence Community in particular partner with non-Intelligence Community entities to prevent foreign intelligence penetration and exploitation?**

**a. To what extent should the Intelligence Community be proactively protecting non-Intelligence Community entities through offensive counterintelligence operations to disrupt foreign adversary targeting of those entities or cyber support to prevent foreign adversary penetration and exploitation of online systems?**

Preventing foreign intelligence penetration and exploitation of our nation's sensitive information and operations is job one of U.S. counterintelligence. Unfortunately, America's CI enterprise is not structured to go on the offense.

For much of its history, U.S. counterintelligence has been principally defensive and inward looking. Our default position has been to wait until the foreign intelligence threat is inside our borders before taking action, where the bulk of that responsibility has fallen on the FBI. Here,

[5] See for example Defense Counterintelligence and Security Agency, *Foreign Intelligence Entities' Recruitment Plans Target Cleared Academia* DCSA-AD-21-001, Department of Defense, April 2021

foreign adversaries have found America's free and open society a target rich environment, expanding their operations as the funding and effort we devote to countering them have declined.

To make matters worse, the modalities and vulnerabilities enabled by the information revolution -- and its evil twin the disinformation revolution -- have amplified the price we pay for inadequate counterintelligence, as our very democratic institutions have been put at risk. What has been missing – before and after cyberspace reshaped our world -- is an integrated, nationally-directed strategic CI program.

Executing an offensive CI strategy against adversary intelligence services would require a new way of doing business, beginning with working the target abroad. The considerable resources of the members of the U.S. intelligence community that have global reach would need to be directed to help identify and then disrupt or exploit foreign intelligence activities, wherever they are directed against U.S. interests worldwide.

Likewise, the best cyberspace defense is likely to be a good offense. From a counterintelligence perspective, the key is getting inside the attacker's intelligence operations to find out what they are doing and how they are doing it, in order to stop them, confuse them, and otherwise tip the scales in our favor.

The missing element is a national CI program to enable the integrated planning, orchestration and execution of strategic CI operations to identify and disrupt hostile intelligence threats, whether directed against U.S. national security secrets, business and industry, critical infrastructures, or our democratic institutions.

**NCSC'S Mission**

**14. What should NCSC's mission be going forward?**

In my view, the original purpose for which the national CI office was created remains as compelling today as it was 20 years ago when President Bush first appointed me to the job.

Congress created the NCIX (predecessor to the NCSC) because foreign intelligence services were exploiting the seams in U.S. counterintelligence at a painful cost in lives and treasure. The mission of the NCIX (which is still governing law) was to serve as the head of U.S. counterintelligence – a first for the enterprise. The NCIX was responsible for providing strategic direction, and integrating CI activities across the federal government (principally the FBI, CIA, and DoD/military services) through threat assessment, budget and program guidance, training and education, and operational prioritization.

However, while charging the NCIX with that mission, Congress did not create a national strategic CI program that the NCIX would be empowered to manage. In other words, it created a national Executive but not the means of execution.

As a result, we have a national CI strategy, but we do not have a strategic CI capability. The DNI's decision in 2010 to consolidate CI and security responsibilities under a single national center has resulted in the NCSC spending the bulk of its time and effort on security, rather than the very different challenges of counterintelligence. The unity of effort and priority requirements of

strategic counterintelligence have yet to find expression in ordering the plans, programs, budgets or operations of the component CI agencies.

Any strategy is useless unless it connects means to ends. For that to happen, people need to be held accountable for employing the resources they control to achieve those ends. These are the qualities of a program. And they are qualities the national counterintelligence mission does not yet possess.

Going forward, the NCSC should be revalidated and empowered to perform the mission originally assigned. Most importantly, the NCSC needs to lead the transformation of the CI enterprise to be able to work as a cohesive whole. To that end, I recommend that Congress establish in law a strategic CI program, managed by the head of U.S. counterintelligence, to marshal the resources of U.S. counterintelligence to find out what hostile intelligence services are doing, and how they are doing it, in order to stop them.

**15. Should NCSC focus on coordinating and integrating traditional counterintelligence activities and operations across the Intelligence Community or establishing a strategic counterintelligence program for the U.S. government as a whole?**

To a large extent, these are one in the same. Any national strategic CI program will require the coordination and integration of traditional CI activities and operations across the government to achieve a common goal. What has been lacking is an agreed understanding on that common goal.

U.S. counterintelligence is finely tuned to work individual cases, but it is not postured globally to disrupt a foreign intelligence service. CI resources have been concentrated within the United States, allowing the adversary to bring the threat into our backyard. While there is bilateral deconfliction, CI agencies work independently to meet agency-specific objectives.

Without prejudice to standing agency responsibilities, the national CI enterprise needs a new business model to provide the strategic coherence to go on the offense against select targets. Under the leadership of the NCSC, a strategic CI program, comprising dedicated elements across the CI community, would consist of three parts:

- Develop foreign intelligence service "order of battle" through focused collection of adversary plans, intentions and capabilities, identification of intelligence gaps, and assessment of adversary vulnerabilities
- Conduct strategic operational planning to redirect or reallocate U.S. collection and operations against this now understood target set based on our capabilities and opportunities for interdiction or exploitation
- Integrate and orchestrate CI resources to achieve these strategic objectives, with operations assigned to the appropriate CI entities.

**16. How should NCSC coordinate and de-conflict efforts with the FBI's National Counterintelligence Task Force?**

From my interactions with the FBI and the NCITF, I understand that the principal purpose of the latter is to facilitate information sharing and interagency coordination supporting the FBI's counterintelligence (and related) activities, and to enhance threat awareness and security practices. A strategic CI program, under the leadership of the NCSC, would likely find the NCITF a useful resource.

**NCSC's Duties, Authorities, and Resources**

**17. Which duties and activities are (or should be) an essential part of NCSC's mission?**

The single most important duty of the Director NCSC is to head U.S. counterintelligence, not merely in name, but in fact, as contemplated by the CI Enhancement Act of 2002.

The current CI enterprise is built to support individual department and agency mission sets – all of which are vital. But it is not built to identify, assess, neutralize and exploit foreign intelligence operations directed against the United States. If we are ever to get ahead of the threat, the NCSC will need to lead the transformation of US counterintelligence to work as a coherent whole.

To that end, the head of U.S. counterintelligence should be designated the program manager of a statutory strategic CI program, and assigned funding and authorities to that end. Resources would include dedicated, country-specific strategic operational planning teams, drawn from across the CI community, and the authority to task select elements within the operational agencies for joint execution.

Threat prioritization, strategic guidance, budget assessments, training, education and public outreach, as itemized within the NCSC enabling statute, are all inherent duties of the office charged with leading and integrating the profession.

Whether or not the NCSC should retain responsibility for protective security is a more complicated question. To be sure, there is an inherent partnership between counterintelligence and the distributed functions of security, and a vital two-way flow of information. U.S. counterintelligence identifies foreign threats, and provides threat information to those responsible for protective security across the USG, as well as high priority private sector entities, so they may assess their risk and implement security plans and programs. Security managers in turn need to provide CI with incident reports and related information that may be indicators of foreign elicitation attempts, cyber penetrations, and the like.

But focusing the bulk of the NCSC's time and attention on security concerns, as has been the recent practice, is not the answer. One can pile on so much security that no one can move and still there will be a purposeful adversary looking for ways to get at what it wants. It falls to our CI agencies to defeat foreign intelligence services operating against the U.S. And that is why the core CI mission of the NCSC was and remains so important.

**18. How should the Intelligence Community best conduct educational outreach to other U.S. government agencies and academic and private sector entities?**

**a. What role should NCSC play in educational outreach?**

The NCSC has a leading role to play in educating the public about U.S. counterintelligence – what it is, what it does, and why, as well as coordinating foreign intelligence threat warnings.

**b. How should NCSC coordinate with FBI and other U.S. government agencies to conduct outreach?**

The FBI has long tasked its 56 field offices to identify and engage business, industry and academia at risk to foreign intelligence exploitation, in order to raise threat awareness and facilitate incident and other reporting back to the IC. The FBI should be keeping the NCSC fully and currently informed of these activities, and any insights they may provide.

**c. Should NCSC develop a strategic plan to prioritize outreach efforts?**

I do not know whether a strategic plan would be useful at this time, but I could envision the need to prioritize outreach if the IC/CI were to acquire relevant insights into foreign intelligence operations and collection targets requiring special attention.

19. The Committee understands that NCSC has not been consistently carrying out vulnerability assessments.

**a. Why are such assessments important?**

Effective security plans and programs are based on realistic risk assessments, which require an understanding of both threat and vulnerabilities.

**b. What resources and authorities would NCSC need to conduct vulnerability assessments in compliance with statutory requirements?**

As I read the statute, the NCSC has discretionary authority to conduct or coordinate such vulnerability assessments as it deems necessary or useful, subject to applicable law. Resource requirements would vary, depending on the type and quantity of vulnerability assessments planned. As an example from my time in office, we were instrumental in facilitating red-team testing of certain sensitive government facilities, drawing on funds allocated to those facilities for that purpose.

**c. Rather than directly assessing the vulnerabilities of private sector and academic entities, should NCSC develop standards, criteria, and guidance for organizations in these sectors to do their own assessments?**

In my view, the national-level office should provide policy and strategy guidance, but leave vulnerability assessments to those in the best position to perform them. Those who are in the field and know their business from the inside are far better equipped to identify vulnerabilities in their practices, personnel, physical plants, critical information and IT infrastructures. Moreover, potential vulnerabilities vary widely, depending on the business or industry or academic institution. Where standardized criteria or guidance may be useful for a given industry, I would defer to those government agencies charged with working directly with those sectors (e.g., DCSC and the defense contractor base; FDA and the pharmaceutical industry; etc.)

**d. Should Congress require such entities to conduct vulnerability assessments and take reasonable steps to mitigate identified vulnerabilities?**

In my opinion, private entities who enter into sensitive contractual or grant relationships with the federal government should be required to demonstrate due attention and care to mitigating vulnerabilities to foreign intelligence exploitation.

**20.** The Committee understands the NCSC has not been consistently coordinating counterintelligence research and development efforts.

**a. Why is this important?**

**b. What resources and authorities would NCSC need to coordinate counterintelligence research and development efforts in compliance with statutory requirements?**

To my knowledge, there is no dedicated R&D effort to support the work of U.S. counterintelligence – but there should be. Doubtless there are many ways in which the tradecraft of counterintelligence, and its various analytic and operational tools, could be enhanced through the creative exploitation and application of new technologies. The Defense Science Board (DSB) looked at this issue in 2019, and recommended that the Undersecretary for Intelligence and the Undersecretary for Research and Engineering jointly explore ways to exploit existing S&T investments to improve DoD's counterintelligence capabilities and tools, including:

- Establishing an effort within the office of the Secretary of Defense, perhaps including support from a University Affiliated Research Center or a Federally Funded R&D Center, dedicated to examining new technologies which could enhance the CI mission within the DoD; and
- Creating a program, plan, and budget to accommodate the continuous infusion of these technologies into CI operations.

I would urge the Committee to follow up directly with the office of the Secretary of Defense on the status of this DSB recommendation.

**21. In which key areas is NCSC under-resourced for its mission?**

The current complement of duties and billets at the NCSC appear to be heavily skewed in support of its security-related responsibilities, with far less effort devoted to counterintelligence. As a result, I fear the original purpose for which the NCSC was created has been neglected. A revalidation of that core CI mission, as discussed above, should drive a realignment of resources to support national CI objectives.

Having served as the first head of U.S. counterintelligence, charged with setting up the office of the (now) NCSC, I am not in favor of big new bureaucratic structures that take people away from the field. However, as part of the strategic CI program, I strongly recommend that an elite national CI operations center, manned and empowered by the constituent members of the CI community, be established at the NCSC to integrate and orchestrate operational and analytic activities across the CI community to strategic effect.

In my view, the greater obstacle to progress is not so much lack of resources as it is the mixed signals over the core mission of the national CI office. There is an urgent need to clear up that confusion, if U.S. counterintelligence is ever to have the cohesion needed to get ahead of the threat. Establishing in law a strategic CI program, and reaffirming the responsibility of the head of U.S. counterintelligence to lead that effort, are vital first steps.

**22. What resources and authorities does NCSC need to better influence the counterintelligence budgets of its entities?**

Under the current business model, with program and budgeting authorities divided among the departments and agencies, we are getting about the best we can expect out of our CI programs. For the future, avoiding strategic CI failure will require more than simply doing more of the same. Without the power of a common purse, however, the mission of integrating and redirecting U.S. counterintelligence to achieve strategic cohesion may well be impossible.

To that end, the Director of National Intelligence should delegate his directive authority over CI budget, analysis, collection and other operations, to the NCSC, which would go a long way toward investing the national CI office with the authorities and resources it must have to succeed.

I know that departments and agencies jealously guard their power over their own purse and operations, and for good reason. So let me be clear. In my view, the NCSC does not need plenary directive authority over all CI budgets and programs. Those matters that are properly the purview of the individual CI missions assigned to the operational components must remain under their control (and accountability). The NCSC should review and advise the DNI on the whole of the CI enterprise, which can be accomplished as part of the overall NIP budget preparation.

However, the NSCS does need directive authority over the elements of the strategic counterintelligence program, distributed among the several operational components. While tactical execution must remain with the responsible agencies, D/NCSC should serve as program manager for strategic counterintelligence, with dedicated resources at the national level and as assigned among the executing departments and agencies, to identify, assess, neutralize and exploit high priority foreign intelligence threats to the United States. This should include an effective means of holding agencies accountable for meeting national objectives that go beyond their individual missions.

**23. Should Congress establish a separate appropriation for NCSC to support non-IC U.S. government agencies and counterintelligence programs that support strategic objectives?**

No. Adversary intelligence services do not target the Commerce Department, or DoE laboratories, or the U.S. Congress; they target the United States. Our counterintelligence enterprise must be equally strategic in its orientation and response.

Unfortunately, U.S. counterintelligence is not currently configured to work as a strategic whole; rather, each of the lead agencies has a separate CI mission that grew up as part of their larger responsibilities, with no overarching structure to unite them. The tactical focus of U.S. counterintelligence professionals – our clandestine HUMINT collectors, military commanders responsible for force protection, or law enforcement officers pursuing espionage leads -- is vital to

individual mission success, but they do not answer the larger questions: What are the threats to America's national and economic security presented by foreign intelligence adversaries and what should we do about them?

The Director NCSC should be designated program manager of a strategic IC program, to provide the structure, processes and centralized orchestration needed to go on the offense against foreign intelligence threats wherever they are directed against the United States or our vital interests. As a baseline, CI agencies should designate strategic CI units from among their existing capabilities, or identify such additional capabilities as they may need to support and carry out this new national CI mission. The Committee may want to task the Director NCSC to gather and assess these funding requirements as part of the ODNI budget submission to the Congress.

**NCSC's Structure**

**24. What are the key benefits and drawbacks of remaining a Center within ODNI? [and]**

**25. What is the ideal organization and location for NCSC to best counter the current foreign intelligence threat landscape?**

- **a. Should NCSC remain exclusively within the Intelligence Community, or should it acquire non-title 50 authorities as well, given its current focus on outreach and engagement with non-IC entities?**
- **b. Should NCSC become an independent National Counterintelligence and Security Agency?**

I believe there is a strong argument for splitting national level policy and oversight of security and counterintelligence into two parts, under two separate entities.

1. A security center, outside the intelligence community, could be established to advance, coordinate, and hold agencies accountable for security plans and programs across the federal government, and to interface with the private sector. It would also serve as public spokesman for threat awareness and best practices, which span not only foreign intelligence threats but the full range of cyber threats (including criminal activities), supply chain integrity, and insider concerns (leaks, disgruntled employees), in coordination with sister agencies (*e.g.* CISA, DCSA).
2. The (smaller) national CI office would remain within the ODNI as a separate entity. Counterintelligence is by its very name, definition, authorities and practices an intelligence mission. It is executed by the designated operating agencies. They need a leader to provide strategic cohesion, as the 2002 Counterintelligence Enhancement Act originally provided, and to perform the duties outlined in that law (threat prioritization, national strategy, budget oversight, training and education).

To that end, the national head of U.S. counterintelligence needs to be empowered to serve as program director of a new strategic CI program, including authority over select (new?) resources across the CI community dedicated to that program. The national office would keep book on foreign intelligence threats, array blue side capabilities against them, develop strategic operational plans to neutralize or exploit those threats, and coordinate their execution. As I

emphasized in my testimony, this is a straightforward offensive capability that the United States does not have but sorely needs.

No one wants to see the bureaucracy grow any bigger than it already is; but in this case, I think that two entities would actually prove more efficient:

- A security center, outside the IC, would have the clarity of purpose needed to align responsibilities and staffing with security disciplines across the government and the private sector, and get to work.
- The same is true of a national CI office, which by contrast would be manned by analysts and strategic planning team members from across the IC/CI community to work strategic CI targets. The office would not serve as another "czar" – which we do not need -- but an actual new national-level capability, which would accrue to the benefit of our CI agencies across the board.

Each center would know the parameters of their mission; staffing requirements would not be any greater but they would be easier to meet (with security outside the IC); and each would have a clear and vital job to perform. In my opinion, conflating security and counterintelligence national offices, as they are now, is not saving money or resources; it is just inviting confusion and wasting precious time and effort – all to the benefit of our adversaries.