QUESTIONS FOR THE RECORD

From Senator Feinstein

Security/Insider Threats

I am greatly concerned about the security at NSA. Some of the worst threats we have had over the past decade to national security of the United States have come from within. In particular, two NSA contractors stand out to me – Edward Snowden and Hal Martin – as particularly egregious.

1. **What concrete steps will you take to address the insider threat issue at NSA?**

If confirmed, I will take several concrete steps, building on the extensive work NSA has already completed and briefed in detail to the Committee. I will look at potential necessary technological changes. I intend to review security clearance procedures, and I will seek input on whether additional authorities are required. I find leaks of classified information reprehensible, I consider their damage to national security grave and unacceptable, and I will vigorously hold all personnel accountable to stop leaks and compromises. Additionally, I will submit crimes reports to the Department of Justice when I believe an unauthorized disclosure of classified information, or other potential Federal crime, has occurred.

2. **What steps will you take to better secure your networks?**

I will provide a detailed answer via classified channels.

Industry Help in Insider Threats

Last week during a hearing on Security Clearance Reform, the Committee heard from Industry leaders that they continue to need better sharing of information from the Federal government.

Industry leaders identified a situation where the government will tell a contractor, "This person is no longer suitable. Take them off the contract." But the government won't tell them why. They won't tell them what behavior has occurred or why they're no longer suitable for the contract, leaving the industry to figure out what happened, if they have the time or resources to do so.

3. **What specific steps will you take to ensure these contractors with problems don't just come back on under a different contract with a different company?**

I believe that with greater sharing of information between the Federal government and the contractor base, we will be able to better ensure that contractors with problems do not just come back under a different contract with a different company. As noted below, NSA may need new authority to facilitate this sharing.

4. **Some potential solutions might require legislation. What efforts do you believe would be helpful?**

I am told that the Federal government is not allowed to share information concerning the suitability of civilian employees with contractors, and that contractors are barred from sharing similar information with the government. This inability to share is a barrier to best security practices. This is where, if confirmed, I may need the help of the Committee in the form of new authority.

Use of Contractors

I continue to be concerned about the general use of contractors in the Intelligence Community. Previously, I worked with Director Panetta and others to reduce the percentage of contractors being utilized, and I've been pleased to see the continued decrease of contractors as a percent of the overall workforce.

Government contractors are supposed to be used only if they are performing tasks that are NOT an inherent governmental function. Intelligence collection clearly is an inherently governmental function. This should not be done by outside individuals.

It is my view that Intelligence Community (IC) functions are largely inherently governmental in nature and that the IC's reliance on contractors should be further minimized.

5. **Do you agree that intelligence work is clearly an "inherently governmental function"?**

I wholeheartedly agree that contractors may not perform any inherently governmental function, and the direction and control of intelligence operations is an inherently governmental function. However, intelligence work includes many activities, some of which are in support of NSA's intelligence mission but do not amount to inherently governmental functions. I believe we should regularly look at the balance between government and contractors as part of NSA's overall workforce.

6. **What is the right balance in your opinion between contractors and government employees?**

NSA must always have qualified and experienced government personnel in key roles, and government personnel should always lead mission functions. NSA must also ensure that it has sufficient government personnel to maintain control over functions that are core to the Agency's mission and operations. If confirmed, I will seek the specifics of the current government employee-contractor mix, and attempt to achieve an ideal balance.

7. **Will you commit to assuring contractors are not permitted to perform inherently governmental functions?**

Absolutely.

From Senator Collins

Lieutenant General Nakasone, in your responses to the Committee's prehearing questions regarding threats to America's election infrastructure, you stated that it would take a "whole-of-government solution," with NSA supporting the effort.

1. Please describe that effort in detail; how do you foresee the NSA engaging with Congress, the Department of Homeland Security, and state government officials to address these threats, particularly with regard to the upcoming the November 2018 federal elections? Will you ask Congress for new authorities if you determine they are needed to adequately protect America's election infrastructure?

Cyber defense requires a whole-of-government effort, with DHS as the Federal government lead for the critical infrastructure and key resources, including U.S. election systems. NSA plays a significant role in helping protect election infrastructure by making available to DHS, and other agencies, the cybersecurity information NSA acquires in the course of its signals intelligence (SIGINT) and cybersecurity missions. Consistent with its mission, DHS can use this information, as well as information obtained from other sources, to assist state governments in their efforts to address threats to election infrastructure.

If confirmed, I will look to ensure that NSA is making full use of appropriate authorities and is thoroughly and effectively integrated with its partners to make available to DHS cyber threat information critical to protecting our elections. I will keep this Committee informed of those threats and of NSA's efforts to assist these entities. As with all of NSA's activities, if I learn that NSA has insufficient statutory authority to conduct its missions I will share my findings with the Committee.

Protection of America's critical infrastructure necessitates rapid and fulsome sharing of cyber threat indicators between the public and private sector actors.

2. If confirmed, what steps would you take to ensure that the NSA is doing everything possible to facilitate the efficient and effective sharing of cyber threat indicators, both within and external to the Intelligence Community, where U.S. critical infrastructure is at risk?

The passage of the Cyber Information Sharing Act of 2015 was an important first step that promotes sharing of cyber threat indicators both within the government and bi-directionally with the private sector. With the vast majority of the critical infrastructure owned or operated by the private sector, increasing this exchange of threat information at "cyber speed" will make these sharing efforts even more impactful. If I am confirmed, I will evaluate the methods and processes with which NSA is sharing cyber threat indicators with DOD, the IC, and DHS's National Cybersecurity and Communications Integration Center whose mission is to create shared situational awareness of malicious cyber activity, vulnerabilities, incidents, and mitigations among the public and private sector.

In your responses to advance hearing questions from the Senate Armed Services Committee, you indicated that recruiting and retaining top talent will be among your priorities as Director of the National Security Agency. Leaders from across the Intelligence Community have described the commercial sector as an increasingly acute source of competition for the technical expertise and aptitude upon which NSA's success is predicated.

3. What policies do you intend to propose to make NSA more attractive as an employer, particularly for technical experts who are in high demand in the private sector?

I believe the solution to this issue is twofold. First and most importantly, I will emphasize the attraction of NSA's unique and important mission to both the current and prospective workforce. For current employees, that means ensuring they can be proud of and feel invested in the work they are doing. For future employees, it means emphasizing the unique opportunities and technologies NSA allows its people to engage and implement in defense of the Nation. Second, I intend to work with this Committee to ensure that previous efforts to increase pay for certain high-attrition STEM roles are reinforced. While in my experience the mission is the most important reason people work for NSA, it is important to narrow the difference in pay between the public and private sector.

NSA is often in direct competition with other government agencies and the private sector for highly qualified cybersecurity professionals. While the private sector can offer higher compensation initiatives, NSA offers entirely unique missions along with a sense of serving the Nation and a greater purpose. There are other critical elements to retaining our STEM workforce. They must have a rewarding career progression and meaningful challenges to stay engaged. I believe in the need to offer specialized, sometimes costly, training opportunities to tie our workforce to retention commitments.

From Senator Wyden

U.S. person queries of EO 12333 collection

> **1.** Under what circumstances, if any, is NSA prohibited from conducting a warrantless U.S. person query of communications collected under EO 12333? If the query is conducted without a warrant, what process is required?

I understand that the Attorney General-approved procedures that govern NSA's collection, processing, and dissemination of SIGINT pursuant to EO 12333 impose significant restrictions on queries that are intended to retrieve the contents of communications to, from, or about US persons. Absent consent of the US person or certain emergency situations, my understanding is that such queries normally must be approved by the Attorney General on a case-by-case basis after a finding of probable cause. Metadata queries follow a different process and procedural requirements. In either event, however, all such queries must be undertaken for a foreign intelligence purpose. Redacted versions of NSA's Attorney General-approved procedures are publicly available.

PPD-28

> **2.** The NSA’s January 12, 2015, PPD-28 Section 4 procedures are publicly available. Will you ensure that the NSA continues to post these procedures as well as any modifications, superseding policies and procedures, or significant interpretations?

Yes. According to Section 4(b) of PPD-28, updated or newly issued policies and procedures shall be publicly released to the maximum extent possible, consistent with classification requirements.

Section 702 of FISA

> **3.** Will you undertake a renewed review of the feasibility of estimating the number of communications of Americans or persons inside the United States collected under Section 702 of FISA? Will you commit to working with Congress and outside groups on this issue?

I recognize the importance of this issue. I'm also aware that a significant effort was undertaken recently by NSA to do this. Ultimately, the DNI determined it was not feasible. I understand that NSA and ODNI have shared with this Committee why it is not feasible. If confirmed, I will want to better understand what efforts were explored and why answering this question was determined not feasible to ensure I can better work with Congress on this issue.

Whistleblowers

> **4.** Please describe your commitment to ensuring that NSA personnel and contractor whistleblowers are encouraged, that there will be no reprisals, and that there will be full and timely cooperation with all investigations.

I believe whistleblowing to appropriate entities is an important mechanism for accountability and ultimately strengthens the Agency and the Intelligence Community. If confirmed, I will not tolerate reprisals against those who make protected whistleblower disclosures through appropriate channels and will ensure that the NSA cooperates with all investigations, whether by this committee or the Inspector General.

False statements

> **5.** If you or one of your subordinates were to say something that was factually inaccurate in public, would you correct the public record?

Yes. If I or one of my subordinates makes a materially inaccurate statement in public, I pledge it will be corrected or clarified in public.

Protecting the personal devices and accounts of senior government officials

6. On October 27, 2017, I wrote to Admiral Rogers and then-Acting Secretary of Homeland Security Duke, asking them to take swift action to protect the personal devices and online accounts of senior government officials from targeted cyber-attacks by foreign governments. I have yet to hear back from NSA or DHS about this topic.

a. Do you agree that the personal devices and online accounts of senior U.S. government officials are potentially high-value cyber targets for foreign adversaries?

b. Do you believe that the successful compromise of a senior U.S. government official's personal device or online account can threaten U.S. national security?

c. If confirmed, what, if anything, will you do to protect the personal devices and accounts of senior government officials from cyber-attacks by foreign adversaries?

NSA has a long and successful history securing National Security Systems (NSS). They regularly collaborate with and support technical experts at the Department of Homeland Security (DHS) on cybersecurity issues. If personal devices and accounts, including those of senior government officials, contain work-related information, such devices and accounts would likely be of interest to our foreign adversaries. Successful compromise of such devices and accounts could potentially yield information of intelligence value to our adversaries. If confirmed, I will direct NSA's cybersecurity leadership to continue their cooperation with DHS and determine the authorities and processes under which NSA and DHS could assist senior government officials with personal cybersecurity best practices.

Relations with the FISA Court

7. The declassified version of the April 26, 2017, Memorandum and Opinion and Order of the FISA Court (p. 19) states: "At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those IG and OCO reviews at the October 4, 2016 hearing to an institutional 'lack of candor' on NSA's part and emphasized that 'this is a very serious Fourth Amendment issue.'"

a. What do you believe should be done to ensure that NSA provides to the Court complete, accurate and timely information?

b. What accountability should apply to NSA personnel who fail to provide this information?

It is paramount that the Foreign Intelligence Surveillance Court have a complete and accurate understanding of the matters over which it has jurisdiction, and that information is made available to the Court in a timely manner. Accordingly, if confirmed, I will ensure there are rigorous processes and procedures in place to meet these commitments. Moreover, I can assure you that I will hold NSA personnel fully accountable for their failure to adhere to these processes and procedures.

Information from foreign partners

8. What limitations do you believe should apply to the receipt, use or dissemination of communications of U.S. persons collected by a foreign partner? How should those limitations address instances in which the foreign partner specifically targeted U.S. persons or instances in which the foreign partner has collected bulk communications known to include those of U.S. persons?

When NSA obtains U.S. person information from a foreign partner, the Agency must handle it in accordance with U.S. law and applicable procedures, including Attorney General-approved procedures governing the conduct of DoD intelligence activities. In addition, no element of the IC may participate in or request any person, including a foreign partner, to undertake activities the element is itself forbidden to undertake.

Impact of foreign governments using commercial, off the shelf malware

> **9.** In his testimony at the March, 2013 Worldwide Threat Assessment of the U.S. Intelligence Community hearing before the Senate Select Committee on Intelligence, then-Director of National Intelligence Clapper described the threat posed by the global market for cyber intrusion software:
>
> In addition, a handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. *Foreign governments already use some of these tools to target US systems.* (Emphasis added.)
>
> How significant is the threat posed by foreign governments using lawful-interception software against targets in the U.S., including individuals, businesses, and U.S. government agencies? If confirmed, what will you do to ensure that hostile foreign governments and non-state actors are not able to acquire U.S. made lawful-interception software, or use that technology against U.S. targets?

I certainly recognize the significance of this threat and the dangers it poses. Accordingly, if confirmed, I will work to ensure that NSA provides foreign cyber threat insights such as these to the FBI and other law enforcement agencies, supporting their efforts to prevent the use of software to commit cyber crimes against Americans.

Offensive cyber operations

> **10.** What responsibility does the U.S. government have if a U.S. offensive cyber operation inadvertently affects the computers of U.S. persons or corporations?

It is critically important that our government is doing everything possible to ensure that our effects are limited to the intended targets. In any given case, my response would depend on the particular facts and circumstances of the operation.

From Senator King

1. The Privacy and Civil Liberties Oversight Board (PCLOB) was established by the 9/11 Commission Act of 2007. Its mission is to ensure that the federal government's counterterrorism efforts are balanced with the need to protect privacy and civil liberties. What are your views on the value of the PCLOB?

Oversight of NSA and the entire Intelligence Community (IC) is paramount to ensure, among other things, that intelligence activities are conducted in a manner that protects privacy and civil liberties. The current structure of oversight includes multiple entities across all three branches of government. I believe PCLOB, with its specific mission to oversee the government's adherence to the protection of civil liberties in efforts to prevent terrorism, is a valuable oversight capability. In addition, their July 2014 report on Section 702 of the Foreign Intelligence Surveillance Act illustrates how they can play an important role in promoting transparency, which serves to enhance the public understanding of intelligence activities, while continuing to protect the IC's valuable sources and methods.

2. After CYBERCOM is elevated to unified command status, when do you believe it will be appropriate to end the dual hat relationship between CYBERCOM and NSA? Is this something that should be done immediately? Or, in contrast, should it be done gradually over several years and pursuant to meeting key milestones?

I believe it will be appropriate to end the dual hat when it is clear that it is in the Nation's best interest to do so. That requires that DoD has completed its assessment, has concluded that separation is feasible and desirable, has made the certifications to Congress required by the 2017 NDAA, and has put in place the processes and procedures necessary to ensure that each organization can succeed in its assigned missions while continuing to benefit from close collaboration and support. A decision to terminate the dual-hat status should only be the result of a deliberate process with clear milestones. I project that some measures associated with separation might be immediately implementable while others may need to be accomplished gradually over time. If confirmed, my intent is to look closely at this and provide an assessment to both the Secretary of Defense and the Chairman of the Joint Chiefs of Staff within the first 90 days of my tenure.

3. To what extent does CYBERCOM currently rely on NSA personnel to execute its mission? Once the split occurs, will CYBERCOM need to replicate everything that NSA has been doing? How will this work and how much will this cost?

The National Security Agency (NSA) provides personnel support to USCYBERCOM with 454 authorizations through the Cyber Mission Partnership, and 69 authorizations through the Engagement and Process Coordination program. USCYBERCOM's requirement for NSA personnel support remains enduring with or without the dual-hat arrangement, and these programs have dedicated funding lines across the Future Years Defense Program. USCYBERCOM does not intend to replicate all the capabilities NSA provides, and continued access to NSA's high end capabilities is in the national interest to save the costs of building duplicative infrastructure. USCYBERCOM reimburses NSA for the services provided based on mutually agreed upon rates in Interservice Support Agreements. For Fiscal Year 2017, USCYBERCOM provided $99.3M in reimbursement to NSA for services rendered. Continued support for the Department of Defense's investment in cyberspace capabilities is crucial to maintaining a competitive advantage over determined adversaries in this domain.