# SSCI QUESTIONS FOR THE RECORD

**PPDNI Nominee Gordon's Confirmation Hearing**
**19 July 2017**

## QUESTIONS FOR THE RECORD FROM SENATOR COLLINS

**1. Director Gordon, since I joined the Committee in 2013, I have been briefed on case after case of leaks of highly classified and confidential information from within the Intelligence Community. These cases include Edward Snowden in 2013, the exposure of hundreds of thousands of security clearance forms held by OPM, and, according to his public Department of Justice indictment, NSA contractor Harold Martin stole highly classified information over a period of twenty years.**

**After each of these cases, the Intelligence Community failed to swiftly and fully implement the necessary changes to prevent a repeat of the loss of highly classified information. Why do you believe the IC did not enact sufficient protections after each one of these cases during the past ten years?**

**Answer:** There has been a concerted effort to address these leaks within our authorities and existing laws. I am aware of multiple initiatives that have been completed and many more underway, to include establishment of the National Insider Threat Task Force and insider threat programs within IC agencies, as well as security clearance reform.

Specifically, the IC has taken steps to respond to prior unauthorized disclosures, including:

- Improving Oversight and Management of Personnel Security;
- Defining Privileged User Risk Categories;
- Increasing the Use of Encryption and Digital Rights Management;
- Implementing enhanced User Activity Monitoring on our technology systems; and
- Accelerating Insider Threat Programs.

I believe that we need to aggressively charge forward with the initiatives underway, make sure that we are properly resourced to see them through, continuously pause to evaluate their effectiveness, and identify any remaining gaps that we need to close.

Even with redoubled effort, there will likely always be leaks with regard to classified information. The simple truths that humans need access to information in order to be able to work, that need-to-share always balances need-to-know, and that technology will never provide a perfect solution make this something we will have to continue to address. Our goal is to work, continuously, to both minimize the opportunity and to limit the

damage that any single act might create through aggressive implementation of solutions like those listed above.

**2. What more do you believe needs to be done within the IC to address the almost routine unauthorized disclosure of highly classified and sensitive information?**

**Answer:** I share in your frustration and assessment of the gravity of the situation. We know that unauthorized disclosures of classified information harm our national security. I think there are several things that the IC can continue to do address this situation. First, we must aggressively address unauthorized disclosures by holding individuals accountable for their actions. Second, we should ensure we are taking steps to protect classified information and limit access to it to only those who need it to effectively accomplish the mission. Finally, it is critically important to have safe avenues for whistleblowers to raise concerns, including to this Committee, without fear of retaliation.

**3. Director Gordon, in your statement for the record, you said that at its best, intelligence helps decision-makers identify opportunities to act before events require them to do so. The Committee has repeatedly advocated for greater and faster adoption of analytic tools that have proven to improve forecasting and predictive analysis by the Intelligence Community.**

**While no one can predict the future, work sponsored by the Intelligence Advanced Research Projects Agency has resulted in an impressive body of evidence that identifies specific ways the Intelligence Community can improve the forecasting estimates and anticipatory intelligence it provides to policy makers, such as through prediction markets and increased training of analysts in analytic best-practices.**

**You previously were the director of advanced analytic tools at the CIA. Do you agree that the IC should do more to foster greater and more widespread adoption of these forecasting best practices so that our intelligence analysis is as accurate and useful to policy makers as possible?**

**Answer:** Yes, ODNI's Intelligence Advanced Research Projects Activity (IARPA) has invested in several such technologies, and tested them in real-world forecasting tournaments. IARPA (and others) have found that prediction markets, analytic training, and machine learning models can be used to make more accurate and timely forecasts of significant global events. I agree, and will advance work to encourage the IC to more broadly adopt such evidence-based forecasting methods on topics where they are shown to be effective.

**4. Over the past several years, we have seen a dramatic reemergence of Russia in the Middle East. There is no doubt that Russia's entry into Syria's civil war helped turn**

**the tide of the conflict decisively in favor of the Assad-Iran-Hezbollah axis. Do you believe we have shared interests with Russia in the Middle East, and in Syria in particular?**

**Answer:** The United States and Russia have common concerns in the Middle East, but there are significant barriers to cooperation. The Syria crisis represents both a venue for Russia-U.S. competition in the region and an opportunity for a bilateral relationship through counterterrorism (CT) cooperation and joint efforts to resolve a complex regional crisis. Russian goals in Syria are centered on finding an international political solution that: 1) preserves a Russia-friendly regime in some form; 2) protects a long-term Russian military, security, and economic presence in Syria, even if Syria is broken up into enclaves; 3) gives Moscow international "credit" for "solving" the Syria problem; and 4) eliminates the threat from ISIL and other Islamic extremists. Moscow's emphasis on countering ISIS, coupled with Russia's broad desire to find areas of shared interest with the United States, offer a potential opening for joint CT cooperation in Syria.

**5. The danger posed to our critical infrastructure from cyber attacks of our foreign adversaries is demonstrated most clearly by the attacks that have <u>already</u> taken place in the past few years. The White House recently published an Executive Order on cybersecurity and critical infrastructure that requires the Department of Homeland Security, in coordination with the Director of National Intelligence and other federal agency heads, to identify unique "authorities and capabilities" that can be brought to bear to improve the cybersecurity posture of Section 9 entities in the private sector.**

**As you may know, the Section 9 entities refer to those critical infrastructure entities that, if a single cyber incident were to occur, could cause catastrophic harm to public safety, the economy, or national defense. Yet, despite the fact that many Section 9 entities already confront nation-state adversaries probing their networks, the U.S. government as a whole has offered little tangible help to assist them before an attack.**

**If confirmed, will you commit to looking into this and updating the Committee on what authorities and capabilities elements of the IC can offer in support of this White House directive to play a more helpful role in assisting owners and operators defend these vital elements of critical infrastructure?**

**Answer:** Yes, I will commit to looking into this and updating the Committee on the authorities and capabilities the IC can offer in support of the White House cybersecurity directives, with the goal of assisting critical infrastructure owners and operators. In this regard, ODNI facilitates engagement between the IC, DHS, and other sector specific agencies, and critical infrastructure entities to share information on threats that could impair their ability to operate effectively and securely.

**QUESTIONS FOR THE RECORD FROM SENATOR WYDEN**

**6. The Department of Homeland Security (DHS) recently published a report on cybersecurity threats related to mobile phones and cellular networks. In that report, DHS stated that it "believes that all U.S. carriers are vulnerable to [Signaling System No. 7 (SS7)] exploits, resulting in risks to national security, the economy, and the Federal Government's ability to reliably execute national essential functions." According to DHS, these "vulnerabilities can be exploited by criminals, terrorists, and nation-state actors/foreign intelligence organizations." As the DHS report noted, the SS7 vulnerabilities can be used to "determine the physical location of cellular mobile devices, disrupt phone service from individual phones to entire networks, intercept or block SMS text messages, and redirect or eavesdrop on voice conversations."**

**(a) Do you agree with DHS's assessment with regard to the impact of SS7 vulnerabilities on U.S. national security, the economy, and the federal government, and with regard to the threat posed by SS7 surveillance?**

**Answer:** Yes, I agree with the DHS report regarding the risks posed by Signaling System 7 (SS7).

**(b) Do you agree with DHS's assessment that SS7 vulnerabilities can be exploited by criminals, terrorists and nation-state actors/foreign intelligence organizations?**

**Answer**: Yes, I agree that SS7 is vulnerable to these threat actors**.**

**(c) Do you support Intelligence Community efforts to address this threat and do you commit to keeping Congress informed of both the threat and efforts to address it?**

**Answer:** Yes, I believe the Intelligence Community must manage the threat and I commit to keeping Congress informed of both the threat and countermeasure efforts.

**7. In his testimony at the Committee's March 13, 2013, Worldwide Threat Assessment hearing, 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)***

**(a) How significant is the threat posed by foreign governments using these capabilities against targets in the United States such as individuals, businesses, and U.S. government agencies?**

**Answer:** The threat posed to individuals, businesses, and U.S. government targets by foreign governments using cyber intrusion software capabilities is quite significant. These cyber tools are commercially available worldwide and anyone can obtain them. The tools make it much easier for adversaries to conduct exploitation or potentially cyber attacks against U.S. equities.

**(b) How should the U.S. government respond to this threat?**

**Answer:** The IC and U.S. government writ large should respond to this threat in a coordinated and effective manner, keeping Congress consistently informed about these evolving threats and any countermeasures that are implemented. It is critical for the U.S. government to track emerging cyber threats, identify the targeted vulnerabilities, identify patches and mitigations specific to these vulnerabilities, and monitor the status of the implementation of these patches and vulnerabilities to ensure cyber situation awareness across the government. Our response also needs to include U.S. private industry and universities who are often the target of foreign cyber intrusion intended to steal intellectual property or to gain economic advantage.

**8. Please describe your view of "secret law." Should the Intelligence Community conduct programs or operations based on secret interpretations of law that are inconsistent with what the American public believes the law to mean?**

**Answer:** As I noted in my responses to the pre-hearing questions, I firmly believe that earning the public's trust requires not only that the IC follow applicable rules and that support effective oversight, but also that the IC provide appropriate transparency to the public. This is no less true when it comes to legal interpretations of intelligence authorities. It is of course challenging to enhance intelligence transparency and simultaneously protect sources and methods, but it is a challenge we must continue to proactively address. There are a number of statutory provisions, including provisions in the National Security Act and the Foreign Intelligence Surveillance Act, that work to strike this balance by ensuring that Congress and the public are informed of significant interpretations of law consistent with due regard for the protection of classified information. I also understand that the ODNI, in partnership with all IC elements, has worked actively to make legal interpretations publicly available as part of its overall transparency efforts. If confirmed, I look forward to working with the IC to promote transparency to the extent possible while continuing to protect national security