NSA Response to QFRs from SSCI Worldwide Threats Hearing – Open Session 13 February 2018 – Unclassified Only

[From Senator Rubio]
The National Security Strategy of the United States 2017 emphasizes, "The United States also remains committed to supporting and advancing religious freedom."

1. *What kind of violations of and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?*

   Answer: (U) The National Security Strategy (NSS) recognizes that religious freedom is one of our country's values and it is equally cherished by others throughout the world. Although the NSS does not state that a lack of religious freedom is a threat to national security, the denial of this right to individuals can be a destabilizing force within a society. Such destabilization can ultimately lead to conflict, and create U.S. national security concerns.

2. *What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security and countering extremism?*

   Answer: (U) I would refer the Committee to the State Department's annual International Religious Freedom Report, detailing government policies violating religious belief and practices of groups, religious denominations and individuals, and U.S. policies to promote religious freedom around the world. The report is available at: https://www.state.gov/j/drl/rls/irf/.

3. *What is your assessment of the impact of these violations on our efforts to counter terrorists and violent extremists?*

   Answer: (U) See answer to question #2 above.

The word "corruption" is mentioned 14 times in the National Security Strategy. Corruption enables authoritarian leaders to keep their cronies loyal and serves as a tool of statecraft by providing a backdoor to influence the politics of neighbors and rivals. This style of government by corruption, otherwise known as "kleptocracy," is most clearly demonstrated by Russia, but appears to be spreading in parts of Europe, Eurasia, and Latin America.

4. *To what extent does globalized kleptocracy pose a threat to the national security of the United States and what can be done to combat it?*

   Answer: (U) As the NSS notes, "[t]errorists and criminals thrive where governments are weak, corruption is rampant, and faith in government institutions is low." Terrorism and trans-national crime are ongoing threats to the national security of the United States; the forces that feed these threats are also national security concerns. For its part, NSA works to produce foreign

intelligence in response to national security officials' requests for foreign intelligence regarding these topics.

5. *What is your evaluation of the extent to which Russia can be seen as a viable counterterrorism partner to the United States?*

Answer: (U) Effectively countering global terrorism often requires the help of other nations, and the United States government has a history of working with foreign partners to combat terrorism. Russia, like many other nations, could be a valuable partner in combating terrorism. That evaluation would be highly fact-dependent and, ultimately, a decision that NSA would inform, but would not make.

[From Senator Wyden]
In November 2017, I wrote to White House Cybersecurity Coordinator Rob Joyce, asking him to take steps to protect federal workers and their computers from malware delivered via advertising networks. As I noted in that letter, several federal agencies have already deployed network-based advertising blocking technology.

6. *In the NSA's view, how serious is the threat posed to federal computers by malware delivered via commercial advertising networks?*

Answer: (U) Commercial advertising networks provide a lucrative avenue for attackers to deliver exploits because it enables them to leverage sites their intended targets visit on a regular basis and are more likely to trust. However, this is just one of many methods that can be used to deliver malware and no single method should be a point of focus to the exclusion of others.

7. *Does the NSA recommend government agencies block advertising networks from delivering executable code to computer and mobile devices of federal workers?*

Answer: (U) NSA strongly advocates for a defense-in-depth approach to security. As such, all reasonable steps to protect federal networks and information should be taken, which may include blocking threatening Internet content. However, no single approach is foolproof. NSA encourages all federal departments and agencies to leverage best practices, patch management, and to use up-to date endpoint, network-security products, and updated browsers, to reduce the risk of exploitation by malicious advertisers.

8. *Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?*

Answer: (U) The personal devices and accounts of a wide range of government officials remain natural targets for exploitation. We must raise awareness so all government employees use proper cyber hygiene. Ultimately, the security of personal devices and accounts remains an individual's responsibility.

9. *If yes, what steps, if any, have your agencies taken to improve the security of your employees' personal accounts and devices?*

Answer: (U) As stated in response to question 8, ultimately, the security of personal devices and accounts remains an individual's responsibility. However, NSA can and does contribute to wider governmental efforts to counter malicious cyber activity. For example, NSA regularly collaborates with the Department of Homeland Security (DHS) and other Executive Branch agencies regarding cyber security threat, vulnerabilities, and mitigations. For public awareness, NSA publishes unclassified guidance on how users can secure their communications devices, computing equipment, and networks.

10. *What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?*

Answer: (U) As stated in response to question 8, ultimately, the security of personal devices and accounts remains an individual's responsibility.

[From Senator Harris]
Under the Administration's new Vulnerabilities Equities Process (VEP) charter, the NSA serves as the Executive Secretariat and is responsible for producing an annual report to Congress – the first report will come out this year.

11. *Please confirm that DoD receives one vote.*

Answer: (U) Per the UNCLASSIFIED VEP Charter dated 15 November 2017, the Department of Defense (DoD) is one of the 18 participating members of the VEP Equities Review Board (ERB). Several of the departments and agencies on the ERB are represented by multiple component entities, including DoD, DHS, and DoJ. DoD, at the departmental level, is typically represented by the Office of the Secretary of Defense, but DoD components with unique technical and operational knowledge also participate and may vote separately in the ERB, including NSA, USCYBERCOM, and the DoD Cyber Crime Center (DC3). It is important to note, however, that if there is disagreement about an ERB decision based on a non-unanimous vote, that issue can be elevated for higher-level decision through the process described in National Security Presidential Memorandum (NSPM)-4.

12. *Please confirm whether that one vote is allocated to the NSA.*

Answer: (U) See answer to question #11 above.