UNCLASSIFIED RESPONSES TO QUESTIONS FOR THE RECORD
SENATE SELECT COMMITTEE ON INTELLIGENCE
HEARING FEBRUARY 13, 2018

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Rubio**
Witnesses: **Director Coats**
Info Current as of: **April 2, 2018**

Question: The National Security Strategy of the United States emphasizes, "The United States also remains committed to supporting and advancing religious freedom."

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

Answer:

Most foreign government violations of religious freedom—from the persecution of small communities of Baha'is and Jehovah's Witnesses in many countries to North Korean prohibitions against all faiths—can be categorized as human rights concerns that might create conditions for future harm to U.S. national security interests. More direct threats to U.S. interests primarily arise when religious repression fuels either the growth of anti-Western violent extremism or instability in a country, such as majority-Buddhist Burma's crackdown on its population of 2 million Muslim Rohingyas, which the United Nations and others have described as ethnic cleansing. Violations by governments against Muslims, for example, can bolster Islam-under-attack narratives that jihadist groups use to attract recruits and advance their agendas against the West and its partners. Government violations of religious freedom also can fuel societal intolerance against the targeted faiths, which in turn can lead to societal tensions, protests, political turmoil, or other forms of instability in a wide variety of places around the globe, including China and Western Europe.

- Among the governments that violate religious freedoms—Burma, China, Eritrea, Iran, North Korea, Saudi Arabia, Sudan, Tajikistan, Turkmenistan, and Uzbekistan—are designated by the Department of State as Countries of Particular Concern (CPC) for engaging in or tolerating "systematic, ongoing, and egregious" violations. In 2017, the U.S. Commission on International Religious Freedom (USCIRF) recommended designating Russia and Syria as CPCs and placed Egypt, Indonesia, and Malaysia on the second-highest tier of concern.

- Of the non-CPC countries, Egypt, Indonesia, Malaysia, Russia, and Syria ranked highest on the Pew Research Center's most recent index of government violators compiled in December 2015. Sunni terrorist groups are internationally notorious for being among the more egregious violators of religious freedom globally.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Rubio**
Witnesses: **Director Coats**
Info Current as of: **April 2, 2018**

Question: The National Security Strategy of the United States emphasizes, "The United States also remains committed to supporting and advancing religious freedom."

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

Answer:

The depth and breadth of religious freedom violations around the world varies from country to country but is historically elevated, according to diplomatic, UN, and other open-source reporting. The level of violations in the early and mid-1990s that spurred passage of the 1998 International Religious Freedom Act has since worsened, according to the USCIRF and other open-source reporting. Government restrictions on religious practice increased in all major regions of the world between 2007 and 2015, according to the Pew Research Center, while social hostilities and violations by nonstate actors also steadily increased in most regions. Department of State and USCIRF reporting highlights the growth in recent years of government violations of religious freedom tied to laws intended to counter terrorism or extremism.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Wyden**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

Question: Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior US government officials, defense contractors, and scientists through their personal email accounts. (AP, "'Fancy Bear' hackers took aim at US defense contractors," February 7, 2018.)

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

Answer:

The personal accounts and devices of government officials can contain information that is useful for our adversaries to target, either directly or indirectly, these officials and the organizations with which they are affiliated.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Wyden**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

Question: Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior U.S. government officials, defense contractors, and scientists through their personal email accounts. (AP, "'Fancy Bear' hackers took aim at U.S. defense contractors," February 7, 2018.)

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:

We have the resources we need to continue our respective education and awareness programs, which are the most important weapons in the cyber-battlefield when it comes to personal devices and accounts. We also need to continue to harden our government systems, both classified and unclassified, to prevent the potential compromise of a Government-issued personal device or account from becoming a major cyber-intrusion or cyber-success against our government networks or programs; I have made this a priority for the IC. If these programs require additional resources, I will inform this committee.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Cotton**
Witnesses: **Director Coats**
Info Current as of: **March 29, 2018**

Question: In 2017, the Director of the Central Intelligence Agency referred to WikiLeaks as a "non-state hostile intelligence service" that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

Do you agree with Director Pompeo and this Committee that WikiLeaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?

Answer:

Yes, WikiLeaks should be viewed as a non-state hostile foreign intelligence entity whose actions, both individually and in collaboration with others, have caused harm to U.S. national security and interests.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Heinrich**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

Question: How long can personnel from the Executive Office of the President (EOP) hold an interim clearance before the clearance process is terminated and access suspended?

Answer:

Under Executive Order 12968 (EO 12968), where official functions must be performed prior to the completion of the investigation and adjudication process, temporary eligibility for access to classified information may be granted. EO 12968 imposes no time limit on temporary access.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Heinrich**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

Question: **What accountability is there to the DNI, as the government's security executive agent, for the granting of interim security clearances generally, and the interim SCI clearances, specifically?**

Answer:

While the DNI has policy and oversight responsibilities for Government personnel security programs and access to SCI, under authorities set forth in statute and Executive Order, Agency Heads are responsible for establishing and maintaining an effective program to ensure that temporary access to classified information by personnel is clearly consistent with the interest of national security. Agency Heads are responsible for following the DNI's policy guidance when granting such clearances.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Heinrich**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

<u>Question:</u> Has the DNI reviewed all the cases of interim access to SCI, both in the EOP and across the government?

Answer:

The DNI does not routinely review cases of interim access to SCI in the government. The DNI does not recommend temporary accesses be granted or denied in specific cases unless an Agency Head specifically requests guidance.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Heinrich**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

<u>Question:</u> Are personnel with interim access to SCI under a Continuous Evaluation protocol, and if so, who manages that?

Answer:

Personnel with interim access may be under Continuous Evaluation. Identification of the population covered by Continuous Evaluation is the responsibility of the Agency Head.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Heinrich**
Witnesses: **Director Coats**
Info Current as of: **April 23, 2018**

Question: **Are there executive branch and EOP personnel who have held interim access to SCI for longer than one year, and if so, how many such personnel and in what agencies do they work?**

Answer:

In terms of EOP interim SCI access, the best source of information would be EOP, and I would defer to them to address questions regarding EOP personnel with interim access to SCI.

Hearing Date: **February 13, 2018**
Committee: **SSCI**
Member: **Sen. Harris**
Witnesses: **Director Coats**
Info Current as of: **April 16, 2018**

Question: You have the authority to issue Intelligence Community Directives that establish policy across the IC. Your predecessor used that authority to establish specific duties to warn victims?

Will you commit to using that same authority to establish a specific duty to warn states about election related cybersecurity threats? If not, why not?

Answer:

We appreciate the importance of this issue, and the IC remains committed to warning our intelligence consumers about the wide range of serious threats facing the United States that are prioritized and disseminated commensurate with oversight by select committees for intelligence. We do not intend to issue a policy specifically establishing a duty to warn states about election-related cybersecurity threats. The referenced policy, ICD 191, *Duty to Warn*, was issued in 2015 directing IC elements to warn U.S. and non-U.S. persons of impending threats of intentional killing, serious bodily injury, or kidnapping. The Duty to Warn Directive was established to account for intelligence that, when encountered, would be acted upon in a time-sensitive manner directly by IC elements. We do have policies in place that were established to ensure the IC is providing intelligence information, at an appropriate clearance level, to support the Department of Homeland Security (DHS) and other Executive Branch agencies, as appropriate, in their ability to provide useful information to state, local, and tribal governments in a timely manner. The first of these policies, ICD 209, *Tearline Production and Dissemination*, was issued at the request of DHS to expand the utility of intelligence to a broad range of customers. The second Directive, ICD 208, *Write for Maximum Utility*, was issued to ensure intelligence products were written and disseminated in a manner that provides the greatest use for our customers. The IC will continue to support our customers by providing useful and timely intelligence information as appropriate.