



governmentattic.org

"Rummaging in the government's attic"

Description of document: Office of The Director of National Intelligence (ODNI)
Questions For the Record (QFR) and agency QFR
responses to Congress 2017-2020

Requested date: 21-December-2020

Release date: 20-May-2021

Posted date: 07-June-2021

Source of document: FOIA Request
Director, Information Management Office
ATTN: FOIA/PA
Office of the Director of National Intelligence
Washington, D.C. 20511
Email: dni-foia@dni.gov

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

May 20, 2021

Reference: ODNI Case DF-2020-00247

This responds to your Freedom of Information Act ("FOIA") request dated and received by the Information Management Office on 21 December 2020 (Enclosure 1), in which you requested *"A copy of the Questions For the Record (QFR) and agency QFR responses to Congress responding to QFRs during calendar years 2017, 2018, 2019 and 2020 to date, for ODNI. These records are likely found in the ODNI office that handles legislative affairs/congressional relations."*

Your request has been processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. A search has been conducted and records responsive to your request were located; they are being released to you in full (Enclosure 2).

If you have any questions, please feel free to contact our Requester Service Center at dni-foia@dni.gov or 703-275-1313.

Sincerely,



Sally A. Nicholson
Chief, Information Review &
Release Group
FOIA Public Liaison
Information Management Office

Enclosures

UNCLASSIFIED



**One Hundred Fifteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515**

December 14, 2017

The Honorable Nicholas J. Rasmussen
Director
The National Counterterrorism Center
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Rasmussen:

I write to thank you for appearing before the Full Committee hearing entitled "World Wide Threats: Keeping America Secure in the New Age of Terror," on Wednesday, November 30, 2017.

Your testimony was helpful refining the Committee's understanding of current internal and external threats to the nation. I appreciate the effort you took preparing and presenting your testimony.

While many questions were asked during the hearing, the Committee has additional questions, attached, for your reply. Please forward your responses to the Committee, attention Mr. Michael Twinchek, Chief Clerk, at H2-176 Ford House Office Building, by no later than Friday, December 29, 2017.

Once again, thank you for appearing.

Sincerely,

A handwritten signature in blue ink that reads "Michael T. McCaul".

MICHAEL T. McCAUL
Chairman

Attachment

Questions for the Record by Mr. Scott Perry of Pennsylvania

1. What do you consider to be the most critical threat to US national security today?
2. Given that terrorism is merely a tactic – and thus, we are not fighting terrorism - whom would you say are the most dangerous enemies we face today & why?
3. Would you agree that the US faces a domestic insurgency from the forces of Islamic jihad?
 - a. If so, what do you think are the most urgent steps the US must take to protect ourselves from that threat?
 - b. If not, why not & what would you say is the most critical domestic security threat we face at this time?
4. Islamic jihad terror spans the globe & crosses national borders at will, both in the movement of people & by way of the Internet. What are the steps you believe most critical for the NCTC to implement in order to stay ahead of the global Islamic Movement & its myriad domestic US operatives?
5. Please describe your understanding of Antifa's international networks & how NCTC acts to counter them.

Questions for the Record by Mr. Bennie G. Thompson, Ranking Member

6. Do you believe that HVEs present an emerging threat to the homeland?
 - a. How can we be more effective in preventing these attacks and “lone wolf” attacks”?
7. The FBI and DHS produced an intelligence bulletin on May 11, 2017, that purported to warn about the “persistent threat of lethal violence” from white supremacist groups. The data reported in the bulletin claimed there were 49 homicides in 26 attacks from 2000 to 2016, but these numbers are significantly lower than those reported by academics who study this issue.
 - b. Please provide a full list of the 49 homicides in 26 attacks from 2000 to 2016.
 - c. How do you account for these discrepancies?
 - d. Do these discrepancies affect local law enforcement efforts to police such groups?
8. Between 1977 and 2016, there have been hundreds of crimes committed against reproductive health care facilities and abortion providers, including at least 11 murders, 26 attempted murders, 42 bombings, 186 arsons, 98 attempted bombings or arsons, and 411 clinic invasions. Please provide any data that your agency has used to track crimes targeting reproductive health care facilities and abortion providers.

- e. Does violence aimed at reproductive health care clinics, doctors, patients, and staff fall under the federal statutory definition of “domestic terrorism”?
 - i. If not, when would anti-abortion violence rise to the level of “domestic terrorism”?
- f. Are the Department of Homeland Security, the FBI, and the National Counterterrorism Center currently committing funding and staff to investigate violence against reproductive health care clinics, doctors, patients, and staff in order to identify whether any patterns and practices emerge?
 - i. If yes, please explain what level of personnel and budget is being provided.
 - ii. If not, why not?

Questions for the Record by Ms. Val Butler Demings, Florida

- 9. Most of the administration’s CVE efforts to date have been focused on Muslim communities. However, recent reports, arrests, and convictions indicate that new recruits to ISIS do not have a particular ethnic background and are not always familiar with Islam. Moreover, as we have seen in the recent tragic events in Charlottesville and Las Vegas, not all “extremists” are adherents of Islam. How are the CVE programs being tailored to target a wider audience to reach would-be perpetrators of extremist attacks?
- 10. The agencies engaged in CVE programs have both law enforcement and intelligence gathering responsibilities. However, the purpose of CVE programs is to foster substantive relationships with the community and to reach vulnerable populations prior to radicalization.
 - a. Are there are other federal agencies that are better equipped to carry out that mission?
 - b. How do you disengage your law enforcement and intelligence-gathering mission when participating in CVE activities?
 - c. What safeguards are in place to protect the civil liberties of the communities that your agencies are engaging?

VADM Joseph Maguire (USN, ret.)
211 West Davis Blvd.
Tampa, FL 33606

August 30, 2018

The Honorable Rand Paul, M.D.
United States Senate
Washington, DC 20510

Dear Senator Paul:

Thank you for the opportunity to respond to your letter of August 28. As the nominee to be the next Director of the National Counterterrorism Center, I do not currently hold a security clearance and do not have access to classified or otherwise sensitive information.

In response to the first set of questions, I can state without reservation that, if confirmed, I will carry out the responsibilities of the NCTC Director in a manner consistent with the highest standards of the Intelligence Community and in strict adherence to the Constitution and all applicable laws. This commitment includes ensuring that the constitutional rights afforded to all our citizens are protected. In addition, I view congressional oversight as an essential part of our constitutional system of checks and balances, and I believe Congress is obligated to exercise its oversight role over NCTC's activities and that NCTC is obligated to support these oversight requests. Given that many of the activities of NCTC and the IC are classified, this relationship only becomes more important. If confirmed as the Director of NCTC, I assure you that I will continue to abide by the responsibility to keep Congress fully and currently informed of NCTC activities as required by law.

Separately, I am committed to public transparency and am familiar with the Intelligence Community's Principles of Intelligence Transparency. In providing the public with transparency regarding intelligence activities, however, the Intelligence Community must continue to protect its most sensitive sources and methods. With respect to the potential targeting of United States citizens who are part of an enemy force, it is my understanding that the legal framework is understood and has been publicly released as it related to Anwar al-Awlaki. That framework provides that NCTC, at the direction of the National Security Staff, shall conduct assessments of individuals nominated for capture, custody, or long-term disposition. I understand that prior to targeting a U.S. person, the U.S. Department of Justice conducts a rigorous review to ensure that lethal action would be consistent with the Constitution and U.S. law.

In response to the two questions regarding NCTC's role as a nexus for information collected across the IC and the responsibilities inherent with that role, I confirm my position that NCTC, like the Intelligence Community as a whole, must always act in a manner that complies with the Constitution and other legal requirements, protecting fully the freedoms and civil liberties, and privacy rights of the American people. I understand that NCTC has a strong

compliance program and is subject to a robust oversight regime. If confirmed as Director, I will ensure that the workforce understands my commitment to ensuring that when data arrives at the Center we meet our obligations to protect these holdings, with appropriate safeguards to protect both the data and our citizens' privacy and civil liberties.

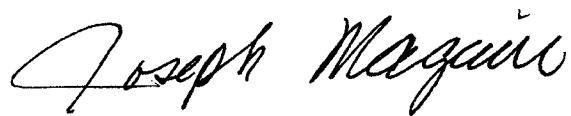
I further recognize and value the close involvement of the Office of the General Counsel, the Inspector General, and the Civil Liberties Protection Officer in the operations of NCTC. If confirmed, I intend to rely heavily on the staff of these critical offices to ensure that NCTC fulfills its mission in a manner that complies with the Constitution and all applicable laws, including disclosure and reporting obligations.

The Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information, (commonly referred to as the 2012 NCTC Attorney General Guidelines) govern the access, retention, use and dissemination by NCTC of terrorism information that is contained within datasets maintained within other executive departments or agencies that are identified as including non-terrorism information.

My understanding is that the 2012 NCTC Attorney General Guidelines help to enable NCTC to serve its mission of integrating and analyzing all intelligence pertaining to terrorism and counterterrorism prevention, detection, and disruption of acts of terrorism directed against the United States and its interests both at home and abroad, while ensuring the protection of our citizens' privacy and civil liberties. NCTC has a strong compliance program focused on ensuring that the Center complies with the requirements set forth in these guidelines, and that the Center is subject to oversight by both ODNI and the Department of Justice to ensure compliance with the guidelines. If confirmed as the Director of NCTC, I will continue to evaluate how the Center collects, retains, and disseminates terrorism information, consistent with NCTC's mission, while simultaneously protecting the privacy and civil liberties of American citizens.

Thank you again for the opportunity to answer these questions.

Sincerely,

A handwritten signature in black ink, reading "Joseph Maguire". The signature is written in a cursive, flowing style with a large initial "J" and "M".

Joseph Maguire

United States Senate

WASHINGTON, DC 20510

August 28, 2018

Vice Admiral Joseph Maguire
Office of the Director of the National Counterterrorism Center
1500 Tysons McLean Drive
McLean, VA 22102

Dear Vice Admiral Maguire:

In consideration of your nomination to serve as Director of the National Counterterrorism Center (NCTC) of the Office of the Director of National Intelligence, please provide answers to the following questions.

NCTC plays a central role in the development and maintenance of the “Disposition Matrix” – a database of persons, including US citizens, that serves as the basis for lethal actions that occur at a threshold below due process. The American public has an obvious interest in understanding the conditions that lead to losing their constitutionally guaranteed protections of life and liberty.

1. Should Congress have greater oversight responsibility over whether—and under what circumstances—a US person should be included on threat lists such as the Disposition Matrix?
2. Do you believe the public has a legitimate interest in understanding the authority and criteria under which they may lose constitutionally guaranteed protections of their life and liberty and are targeted for assassination in the Disposition Matrix?
3. If confirmed, do you commit to providing that authority and criteria to all Members of Congress?
4. If confirmed, do you commit to providing that authority and criteria to the public?
5. Do you believe US persons, and persons generally, should be able to challenge their status as a target for execution without due process?
6. If confirmed, would you approve the targeting of US persons, and persons generally, for execution without due process based entirely on metadata analysis?

The Intelligence Community (IC) may illegally collect information deliberately, as in *ACLU v. Clapper*, or as a result of technical mistakes, as we observed this summer when the NSA announced it had collected millions of call detail records it had no authority to receive. You state in your Senate Intelligence Committee pre-hearing questionnaire that, “*NCTC alone has access to all terrorism-related information—both foreign and domestic—that it uses to conduct all-source analysis and maintain the database that underpins all government watchlisting*”. NCTC’s role as a

nexus for information collected across the IC gives the agency an opportunity and duty to identify illegal collection.

1. If confirmed, do you commit to actively and continually look for illegally collected information, and to report findings to the Office of the Inspector General of the Intelligence Community?
2. Do you believe the Obama administration's 2012 NCTC guidance that it may deliberately store and "continually assess" massive amounts of data collected without a warrant on non-consenting U.S. citizens with no ties to terrorism for five years is appropriate?

Sincerely,

A handwritten signature in black ink that reads "Rand Paul". The signature is written in a cursive, flowing style with a large, prominent "R" and "P".

Senator Rand Paul, M.D.

VADM Joseph Maguire (USN, ret.)
211 West Davis Blvd.
Tampa, FL 33606

September 7, 2018

The Honorable Rand Paul, M.D.
United States Senate
Washington, DC 20510

Dear Senator Paul:

I appreciate the opportunity to respond to your letter of September 6 and request for additional information. I am honored to have been nominated to be the next Director of the National Counterterrorism Center, and I take seriously the important responsibilities this position entails. As I noted in my August 30th response to your first letter, I do not currently hold a security clearance and do not have access to classified or otherwise sensitive information. If confirmed as the Director of NCTC, I am committed to ensuring that the constitutional rights afforded to all our citizens are protected and will abide by the responsibility to keep Congress fully and currently informed of NCTC activities as required by law.

With regard to your specific questions, below are my responses:

1. **It has been reported that drone strikes have been carried out against un-armed, unknown possible terrorists based on metadata. Is this true?**

Since I am not currently in government and do not currently hold a security clearance, I do not have access to information regarding the reliance upon metadata to carry out counterterrorism operations, including drone strikes.

2. **What members of Congress are allowed access to the "Disposition Matrix"?**

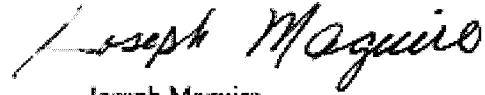
As I highlighted in my earlier response, because I do not currently hold a security clearance and am not currently in government, I have no knowledge of the existence of a "disposition matrix," and therefore am unable to provide an informed response to this question. As I emphasized in my August 30 letter, I am committed to transparency to both the Congress and the public regarding intelligence activities, consistent with the need to protect the Intelligence Community's most sensitive sources and methods. This entails communication with Congress on a regular and continuing basis as required by law. If confirmed as Director of NCTC, I will continue to abide by the responsibility to keep Congress fully informed and provide the information it needs to perform its oversight duties.

3. **Do you understand the Constitution to allow the Executive branch to place Americans on the "Disposition Matrix" for execution? Even if the American is not actively involved in combat?**

My earlier correspondence to you outlined my general understanding of the legal framework for potentially targeting a U.S. citizen who is part of an enemy force. As

to this specific question, it is my belief that it would be unlawful to intentionally target persons not presenting a threat to the United States or its allies, or who are not otherwise lawful targets under existing law. I believe that the Intelligence Community must operate in strict adherence to the Constitution and all applicable laws in order to effectively perform its national security mission and maintain the trust of the American people. If confirmed as the Director of NCTC, I commit to ensuring that NCTC continues to carry out its mission in full compliance with the Constitution and U.S. law.

Sincerely,

A handwritten signature in black ink that reads "Joseph Maguire". The signature is written in a cursive style with a large, stylized "J" and "M".

Joseph Maguire

RAND PAUL
KENTUCKY

United States Senate

WASHINGTON, DC 20510

September 6, 2018

Vice Admiral Joseph Maguire
President and CEO, Special Operations Warrior Foundation
1137 Marbella Plaza Drive
Tampa, FL 33619

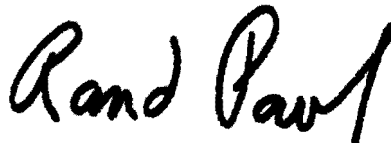
Dear Vice Admiral Maguire:

Thank you for your reply to my earlier letter. I have additional questions:

1. It has been reported that drone strikes have been carried out against un-armed, unknown possible terrorists based on metadata. Is this true?
2. What members of Congress are allowed access to the "Disposition Matrix"?
3. Do you understand the Constitution to allow the Executive branch to place Americans on the "Disposition Matrix" for execution? Even if the American is not actively involved in combat?

Thank you again and I look forward to your reply.

Sincerely,

A handwritten signature in black ink that reads "Rand Paul". The signature is written in a cursive, flowing style with a large, prominent "R" and "P".

Rand Paul, M.D.
United States Senator

Questions for the Record
Senate Select Committee on Intelligence
Nomination Hearing - Open Session
May 5, 2020

Questions for the Record for Representative John L. Ratcliffe

[From Senator Wyden]

1. Three times during your confirmation hearing, you testified that Russia had not been successful in "changing votes or the outcome of [the 2016 election]." While the January 2017 Intelligence Community Assessment (ICA) included a DHS assessment related to vote tallying, the Intelligence Community has made no assessment as to whether Russia's influence campaign did or did not succeed in achieving or contributing to the election of Donald Trump. The ICA stated:

"We did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election. The US. Intelligence Community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze US. political processes or US. public opinion."

- **Have you seen any intelligence analyses supporting your statement that Russia did not succeed in changing the outcome of the 2016 election? If so, please provide it to the Committee. If not, on what do you base your judgment?**

Answer: Page iii of the "Key Judgements" section of the declassified *2017 Intelligence Community Assessment ICA 2017-01D* noted that "DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying." I also understand that the Senate Select Committee on Intelligence's report, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure*, stated that, "In its review, the Committee has seen no indications that votes were changed, vote-tallying systems were manipulated, or that any voter registration data was altered or deleted." The report concluded with SSCI open hearing testimony from Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) witnesses on June 21, 2017, where witnesses expressed agreement "that they had no evidence that votes themselves were changed in any way in the 2016 election."

2. **Have you had any discussions with Attorney General Barr, U.S. Attorney John Durham, or anyone other administration official concerning Mr. Durham's examination of the U.S. Government's Russia investigation? If yes, please describe those discussions.**

Answer: No.

3. During your confirmation hearing, you testified that "no one can spy or surveil outside the law." However, in your responses to written questions, you wrote that "FISA constitutes the exclusive statutory means" by which electronic surveillance may be conducted.

- **Please clarify whether your reference to "the law" was intended to limit surveillance to the FISA statutory framework, or you believe that electronic surveillance outside that statutory framework and based on an assertion of non-statutory authorities can be consistent with "the law."**

Answer: I believe this question relates to my response to Question 10 of the prehearing questionnaire. That question asked, "Do you believe that the intelligence surveillance and collection activities covered by FISA can be conducted outside the FISA framework?" My answer stated and remains, "As set forth in Section 112 of FISA, with limited exceptions, FISA constitutes the exclusive statutory means by which electronic surveillance, as defined in FISA, and the interception of domestic wire, oral, or electric communications for foreign intelligence purposes may be conducted."

4. **Do you support any legislative reforms to FISA? If so, please describe them.**

Answer: As a Congressman and a member of the House Judiciary and Intelligence Committees, I have supported past efforts to reauthorize FISA authorities that are critical to our national security and the Intelligence Community (IC) while also ensuring civil liberties are protected and proper protocols and accountability are established throughout FISA and its statutes. FISA is a vital tool for the IC to collect information on valid intelligence targets. If confirmed, I look forward to working with Congress, the Attorney General, and the IC to continue to promote legislation that ensures FISA's operational effectiveness while strengthening U.S. person privacy protections.

5. Top election cybersecurity experts, as detailed in a 2018 National Academy of Sciences report, are in universal agreement that transmitting marked ballots over the internet is dangerous and should not be done. However, in your responses to written questions, you wrote "resilience built on audits, redundancies and expertise minimizes the impact any threat can have even if using the internet to deliver some portion of ballots."

- **Please provide a fulsome and detailed explanation for how internet voting can be rendered secure from sophisticated hacking and why you disagree with the recommendations in the 2018 National Academy of Sciences report.**

Answer: I do not disagree with the recommendations of the 2018 National Academy of Sciences report. The DHS Cybersecurity and Infrastructure Security Agency (CISA), along with the FBI, serve as the Federal leads on election infrastructure security. My complete response to Question 49 of the pre-hearing questionnaire states, "The goal of our system is to be resilient. In today's age, no system is truly invulnerable to an aggressive and capable threat. However, resilience built on audits, redundancies and expertise minimizes the impact any threat can have even if using the internet to deliver some portion of ballots. The IC will continue to support DHS and FBI in their work to support the states in their leadership role on securing elections." This was in reference to the states who currently permit overseas and military voters to transmit their marked ballots directly to local election officials over the internet, mostly via email. My answer alludes to the fact that no system is ever completely secure, and that only by building auditability, redundancies and expertise into all systems do we minimize any threat, regardless of the manner in which that threat occurs. CISA continues to assist in advising states and localities on how to incorporate best practices that can keep their systems secure. If confirmed, I look forward to ensuring DHS and the FBI continue to receive all the IC support they need to accomplish their critical election security missions.

- **Please identify the cybersecurity experts with whom you have consulted on this topic, and specifically those who have informed you that the risks of internet voting can be sufficiently minimized through "audits, redundancies and expertise."**

Answer: As stated above, no system is ever completely secure, and if confirmed, I look forward to supporting DHS and the FBI in their work to support the states in their leadership role on securing election systems.

6. There are currently no mandatory, federal cybersecurity standards for voting systems, including the servers and technology used by local election officials in 23 states that receive marked ballots over the internet from Americans in the military and those living overseas.

- **How confident are you that these servers and the technology currently used by local election offices to receive marked ballots over the internet are sufficiently secure to protect against hacking by foreign governments?**

Answer: As it relates to election security, the role of the IC is to identify potential foreign-related threats and potential mitigating factors. I trust that our DHS and FBI partners, specifically CISA, in combination with other federal partners, will continue to develop and promulgate best practices, protocols, and tools that help inform state and local election authorities on how to enhance the security and resilience of our nation's election systems. This includes the ability to test systems, audit, and review results accordingly to maintain and strengthen states' election security needs.

7. Federal cybersecurity experts did not conduct forensic examinations in 2016 and 2018 of any of the servers used by local election offices to receive ballots over the internet.

- **How confident are you that foreign governments have not tampered with internet-returned electronic ballots in prior federal elections?**

Answer: I am not aware of any information indicating an adversary has tampered with ballots in prior federal elections. At this time and without further information, I am unable to assess a particular level of confidence in response to your question.

[From Senator Heinrich]

8. Mr. Ratcliffe, you testified in the open nomination hearing that you concur with the unanimous assessment of the 17 agencies of the Intelligence Community that Russia engaged in an effort to interfere in the 2016 elections and that Moscow will keep working to sow discord. But you hedged about the IC's assessment that Russia's aim was to bolster Donald Trump's campaign, and in other forums, you have suggested that it was Hillary Clinton's campaign that colluded with Moscow.

On that point, you stated at the hearing that you had not seen the "underlying intelligence to tell me why there is a difference of opinion" between the assessments of the IC and this Committee and the House Intelligence Committee. You committed to Vice Chairman Warner that you would come back to the Committee if you reach a different conclusion than the IC once you review the underlying intelligence. My request is a slight variation on the Vice Chairman's request:

- **Please provide a commitment that if confirmed, you will review the underlying intelligence within the first six months of your tenure as DNI and that you will brief the Committee on the conclusions you reach about the accuracy or inaccuracy of the IC's assessment and the basis for your conclusions.**

Answer: If confirmed, I will study this issue and provide my feedback to the Committee within six months of my tenure as Director of National Intelligence.

9. During a House Judiciary Committee markup of the USA FREEDOM Act in 2015, the Committee considered an amendment to end the "backdoor searches" of Americans' communications under Section 702 of the FISA Amendments Act without a warrant.

In your comments on the amendment, you stated: "In full disclosure to everyone, I am a former terrorism prosecutor that has used warrantless searches, and frankly have benefitted from them in a number of international and domestic terrorism cases."

- **Please explain how you "used warrantless searches and have benefitted from them," and to which cases you werereferring. (If necessary, you may provide a separate classified answer.)**

Answer: My comments related to the importance of Section 702 authorities generally, and were a reference to the same matters previously disclosed to the Committee in the Annex to Question 9c.

- **Do you believe that it is reasonable for the government to conduct warrantless searches of Americans' communications?**

Answer: The U.S. government should conduct warrantless searches only in accordance with the Constitution and the authorities and laws passed by Congress.

10. When you were first nominated last year for the position of Director of National Intelligence, critics on both sides of the aisle registered concerns about your lack of qualifications and about false claims you made about your record as a prosecutor. Explaining your reasons for withdrawing your nomination five days after it was first submitted, you stated: "I do not wish for a national security and intelligence debate surrounding my confirmation, however untrue, to become a purely political and partisan issue."

- **Do you believe critics were being "political and partisan" in highlighting your lack of qualifications for this position and your misrepresentations regarding your record as a prosecutor?**

Answer: Yes, I do believe some critics were being "political and partisan" in attempting to mischaracterize or inappropriately construe my records and qualifications. My experience and background stands on its own, and it is covered extensively in my responses to the Committee's prehearing questionnaire and to questions I received in the Committee's nomination hearing.

- **Please acknowledge that you misrepresented/exaggerated/lied about your past experience and explain why the Members of this Committee should have confidence that if confirmed, you will not misrepresent facts to this Committee.**

Answer: I have not misrepresented, exaggerated, or lied about my past experience to anyone. Members of this Committee should have confidence because I have provided this Committee with both documentation and testimony under oath establishing that media reports alleging a lack of national security and intelligence

experience were inaccurate and untrue. Out of all the prosecutions brought under my name, authority, and signature as U.S. Attorney from 2007-2008, I am aware of only a single case where details of my role were inaccurately stated in press and/or campaign materials, and which were immediately clarified when brought to my attention.

[From Senator King]

11. In your written statement, you mentioned having a "good rapport" with the President.

- **How did you establish your rapport with the President? Was this rapport forged during political conversations or at fundraisers?**

Answer: My reference to good rapport relates to discussing policy matters, including national security and intelligence issues, with the President when he first began considering me as a possible nominee for DNI. Since that time, and until present, we have continued to develop a good relationship during personal interactions at official events.

12. **What commitments did you make to the President or his team when he originally nominated you last summer? What commitments did you make prior to being re-nominated in March?**

Answer: In both instances, I committed to the President that, if nominated, I would lead with integrity, and at all times, act in accordance with the Constitution and the laws of the United States.

13. **Did you and the President ever discuss the Durham Investigation?**

Answer: I cannot comment on the particulars of my conversations with the President, other than to say that our discussions have been on policy matters. Please also see my response to Question 2 of the Open Hearing Questions for the Record.

14. **Will you state, unambiguously and for the public record, that you concur with the Intelligence Community' assessment that Russia engaged in an unprecedented effort to interfere in the 2016 U.S. presidential election, with the specific aim of bolstering then-candidate Donald Trump's campaign?**

Answer: I concur with the IC assessment that Russia engaged in unprecedented efforts to interfere in the 2016 U.S. presidential election to sow discord and undermine faith in our democracy. As I stated in the open hearing, the House and Senate intelligence committees reached different conclusions on whether a specific aim by Russia was to bolster then-candidate Donald Trump's campaign. I respect both committees, was not involved with the findings of either committee, and have not seen the underlying intelligence to render an informed opinion on that specific issue. As indicated above, if confirmed, I will study this issue and will provide my feedback to the Committee as expeditiously as possible.

15. On April 3, 2020, the President fired IC Inspector General Michael Atkinson.

- **Did you concur with the decision to fire the ICIG?**

Answer: As I stated in the open hearing, I do not have enough information to offer an opinion.

16. During a December 11, 2019, hearing of the House Judiciary Committee, you claimed without any evidence that the Ukraine whistleblower "got caught" and "made false statements." The next day you tweeted that "the whistleblower didn't tell the truth both verbally and in writing."

- **Do you believe it is appropriate for elected officials to defame whistleblowers who have complied with the law?**

Answer: No, I do not believe it is appropriate for anyone to defame, as used in the law, whistleblowers who have fully complied with the law.

17. As a member of HPSCI, do you make it a point to participate in every classified meeting?

Answer: I make it a point to participate in as many HPSCI activities, both classified and unclassified, as I possibly can. As one of only a few of the 435 House members, and until recently the only HPSCI member, to serve concurrently on four committees, I do my best to balance the obligations for all my committee assignments.

[From Senator Sasse]

18. Please provide an assessment of what DNI's AI strategy (Augmenting Intelligence Using Machines or AIM) has accomplished thus far, including highlighting accomplishments by agency.

- **What do you plan to do to enable more efficient progress on implementing AI technologies at the agencies?**

Answer: I have received initial briefs on the IC's AIM Initiative. As I understand it, the ODNI has been leading this initiative, and is in the early stages of seeing it implemented across the IC. Its goal is to align IC efforts and oversee IC investments in adopting Artificial Intelligence (AI). The AIM Initiative has made substantial progress organizing formerly disparate AI activities, reducing overlap and duplication, and setting in place a coordinated, long-term portfolio management approach and investment strategy. I further understand the IC is already implementing elements of the AIM initiative across the Community. If confirmed, I look forward to supporting efforts to help speed the development and application of AI technologies in critical IC mission areas like identity

intelligence, strategic indications and warning, countering foreign malign influence, confirming authenticity of information and enhancing security.

- **What do you plan to do to enable more efficient hiring and training of AI professionals - to include software engineers, data engineers and scientists, mathematicians, and machine learning experts?**

Answer: Like the rest of the Federal Government, the IC competes for the same workforce that is in high demand across the economy. The IC simply cannot compete with private sector compensation packages, and the IC's need for cleared professionals further complicates the matter. In my briefs, I learned that the AIM Initiative does have a workforce component, and its objective is to build and sustain an AI-ready workforce to shape and integrate AI solutions into IC operations, analysis, and support across the board. If confirmed, I will work to ensure the IC is working to build a deep bench of AI and machine learning expertise through targeted and innovative recruiting; training of existing staff; improved and accelerated clearance and onboarding practices as part of security clearance reform and utilizing partnerships with universities, industry, other agencies, and liaison services to augment the current workforce. I will also focus on examining what structural changes are necessary to successfully recruit and retain the best and the brightest talent.

[From Senator Feinstein]

19. During your confirmation hearing, when asked about your views on contractors, you responded that "I agree [that] contractor use . . . should be limited and [that] government employees should be doing government functions. I know there's always a look in terms of ratios and the percentages. I'm not a one-size-fits-all person. If confirmed as DNI, I'll look at where things stand right now."

- Please provide a more detailed answer, including the steps you plan to take to review the IC's use of contractors, and how you will ensure that contractor use does not encroach on inherently government functions.

Answer: Contractors play a critically important role in the success of the IC's mission. In many cases, contractors offer specialized skills and abilities that the civilian workforce, in some cases, may not possess with the required level of proficiency. In other cases, contractors can be leveraged for specialized skills to execute short-term requirements. But contractors cannot and should not be utilized for inherently governmental functions. I understand that both law and policy provide clear guidance to the IC on the appropriate use of contract personnel.

If confirmed, I will work with IC leadership to ensure compliance with both law and policy on the utilization of contractors across the Community. I will also ensure that IC elements are fully utilizing the authorities provided under the Multi-Sector Workforce Initiative to ensure the appropriate mix of contractor, civilian and military personnel to meet mission priorities.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF LEGISLATIVE AFFAIRS
WASHINGTON, DC 20511

JUL 31 2018

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

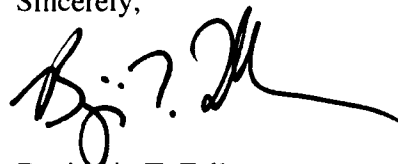
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Burr and Vice Chairman Warner:

Attached are unclassified responses to Questions for the Record following the "Security Clearance Reform", open hearing on March 6, 2018. The attached responses are cleared for public release.

If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,

A handwritten signature in black ink, appearing to read "B.T. Fallon", with a long horizontal flourish extending to the right.

Benjamin T. Fallon

Enclosure:

Unclassified Responses to "Questions for the Record" from the March 6, 2018 Hearing before the Senate Select Committee on Intelligence

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 1: Compliance & Enforcement.

Question 1a: Is the Security Executive Agent (SecEA) responsible for reviewing each government agency's compliance with laws, executive orders, and policies regarding the security clearance process? If yes, does this duty include reviewing the policies for reciprocity and/or the robustness of programs for continuous evaluation and insider threat?

Answer: Yes, the Security Executive Agent (SecEA), is responsible for conducting Executive Branch oversight of investigations and adjudications for personnel security clearances. This includes development and implementation of uniform and consistent policies and procedures; standardization of security questionnaires, financial disclosure requirements, polygraph policies and procedures, and reciprocal recognition of accesses to classified information. The SecEA is also the final authority for designating an authorized investigative or authorized adjudicative agency. This oversight includes the establishment of policies for continuous evaluation and insider threat programs, as well as monitoring compliance.

Question 1b: Which agency's processes does the SecEA review? How often is this review conducted?

Answer: In executing SecEA oversight responsibilities, on April 29, 2014, the DNI established the Security Executive Agent National Assessment Program (SNAP) to review department and agency (D/A) personnel security programs in the areas of security clearance initiation, investigation, adjudication, and application of due process. The annual review process assesses select D/A compliance with the policies and procedures governing the conduct of investigations and adjudications of eligibility for access to classified information or eligibility to hold a sensitive position government-wide. In addition, the ODNI regularly reports to Congress, via Congressionally Directed Actions on our processes and performance.

Question 1c: What assessments or reports does the SecEA issue to the agency or to Congress on such compliance?

Answer: The DNI has responded to Congressionally Directed Actions mandated in the 2010-2017 Intelligence Authorization Acts on numerous topics related to security clearance timeliness, backlog, reciprocity, and security clearance determinations for the Executive Branch. The following is a current list of these CDAs: Improving the Periodic Investigation Process, Security Clearance Determinations, Resolution of Backlog of Overdue Periodic Reinvestigations, Assessment of Timeliness of Future Periodic Reinvestigation, Insider Threat, and Continuous Vetting, Enhancing Government Personnel Security Programs - Implementation Plan.

Question 1d: What are the SecEA's means of enforcing compliance at a particular agency (e.g. through budgets, withholding certain certifications)?

Answer: The SecEA is given authority in Executive Order (E.O.) 13467, as amended, to designate an investigative or adjudicative agency. The SecEA may rescind a D/A's investigative or adjudicative authority if it is unable or unwilling to comply with applicable standards. The SecEA personally issues a letter to each agency head to inform them of their annual security program performance. If an agency does not meet performance goals, the agency head is required to submit a Corrective Action Plan with milestones and a

date of completion. The SecEA staff follows up with these organizations regularly until they achieve compliance and the desired end-state.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 2: Trusted Workforce 2.0.

Question 2a: Who is involved in the DNI-led "Trusted Workforce 2.0" initiative? Are representatives from industry, think tanks, Government Accountability Office, or Congress involved?

Answer: The Trusted Workforce 2.0 initiative is led by the SecEA and Suitability Executive Agent (SuitEA) in concert with the other Performance Accountability Council (PAC) Principal Organizations, the Office of Management and Budget, the Office of the Undersecretary of Defense (Intelligence) and the National Background Investigations Bureau. Trusted Workforce 2.0, which began in March 2018, is supported by Executive Branch senior leadership, change agents, and innovative thinkers from government and industry.

Question 2b: What is the scope of the "Trusted Workforce 2.0" effort?

Answer: Trusted Workforce 2.0 is a fulsome, "clean slate" review of the vetting enterprise. The initiative will serve as the foundation for a trusted workforce while keeping pace with emerging technologies, capabilities, and opportunities to continuously identify, assess, and integrate key sources of information. Trusted Workforce 2.0 will chart a bold path forward for transforming the vetting enterprise in the areas of policy, governance, business processes and modernization of information technology architecture. This aggressive effort may require additional resources from Congress. We look forward to partnering with agency leadership and private industry to transform our vetting enterprise into a system that protects our nation's sensitive equities and meets the needs of the workforce.

Question 2c: Will the DNI initiative produce any recommendations or policy changes?

Answer: Yes. The intent of Trusted Workforce 2.0 is to identify the way forward in improving the quality, timeliness, and performance of the personnel security vetting process while incorporating new capabilities and approaches. This effort will require changes to existing policies and, potentially, the statutes governing those policies.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 3: Reciprocity. Security Executive Agent Directive 4 on reciprocity contains an Appendix C that allows agencies substantial latitude in levying additional requirements before accepting a clearance. The SecEA provides data on reciprocity for the Intelligence Community (IC) pursuant to Sec. 504 of the *Intelligence Authorization Act for Fiscal Year 2014*, but not the rest of government.

Answer: Security Executive Agent Directive (SEAD) 4, *National Security Adjudicative Guidelines*, Appendix C, identifies exceptions to the adjudicative guidelines. These exceptions are defined as “an adjudicative decision to grant initial or continued eligibility for access to classified information ... despite failure to meet the full adjudicative or investigative standards.” Appendix C lists the specific exceptions: Waiver, Condition, Deviation, or Out of Scope. While the existence of an exception in a national security determination can affect the application of reciprocity, the cited SEAD and appendix do not specifically address reciprocity.

NCSC has drafted SEAD 7, *Reciprocity of Background Investigations and National Security Adjudications*. This directive will provide reciprocity guidance and procedures for government-wide use. The requirements of 50 U.S.C. 3341(b, d), and E.O. 13467, as amended, serve as the basis for the DNI to provide reciprocity guidance for agencies. The draft SEAD has cleared internal ODNI review and is currently in the formal OMB policy coordination process.

Question 3a: As the SecEA, can you please detail what additional requirements IC and non-IC agencies require, by agency, at each clearance level?

Answer: The requirements for secret and top secret clearance reciprocity are the same for IC and non-IC agencies and are consistent with OMB and Intelligence Community Policy Guidance. The SecEA issued E/S 01074, “Executive Order 13467 (as amended) and Reciprocal Recognition of Existing Personnel Security Clearances,” dated October 1, 2008. This memorandum endorses the guidance provided in the OMB memorandum. SEAD 7, when issued, will standardize policies and procedures for individuals eligible for access to classified information or eligible to hold a sensitive position across the Executive Branch.

Question 3b: As the SecEA, can you please provide data on the time it takes to for both government and industry personnel at the same level (e.g., SECRET, TOP SECRET, SCI) to transfer a clearance from an IC agency to an agency beyond the IC?

Answer: Currently, the SecEA does not capture clearance cross-over timeliness from the IC to non-IC agencies as reciprocity data is not collected from agencies outside of the IC. SecEA’s reciprocity reporting for the whole of government is pending issuance of SEAD 7. Data from current reporting is limited to the IC, and the cases are Top Secret or Top Secret/SCI. In fiscal year 2017, the average IC processing time for reciprocity was 8.2 days. Once SEAD 7 is issued, it will provide standardized metrics requirements for IC and non-IC agencies.

Question 3c: Why is it possible for clearance delays to exist within an agency when a cleared individual, either government or contractor, switches projects within the same agency?

Answer: Many variables can affect clearance transfers for government employees and contractors. An individual may have a security clearance that is ineligible for reciprocity, the access may not be at the correct

level for the new position, or there may be suitability aspects of the position that require review of the original access determination.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 4: Government v. Contractor Personnel.

Question 4a: Under existing policy, is a contractor who is "out of scope" for her background investigation treated differently than a government employee who is "out of scope," when moving jobs or contracts? If so, please describe how this treatment differs.

Answer: While the personnel security vetting process is very similar for contractors and government employees, the process is the same for out of scope background investigations between contractors and government personnel. However, individual circumstances and position requirements can impact security determinations. An "out of scope" background investigation can impact eligibility for reciprocity. A contractor with an out of scope background investigation could potentially move from one contract to another with the same sponsoring agency, but may not be accepted on a contract sponsored by another agency. Likewise, a government employee with an out of scope background investigation may be eligible to change jobs within their agency, while their clearance may not be accepted as part of a transfer to another agency. Suitability for employment or fitness for a position may also be a consideration.

Question 4b: Can an agency have one policy for use of the polygraph for its cleared government population and a different policy for its contractor community? If so, please provide an example.

Answer: Yes. The application of polygraph in the national security vetting process is governed by SEAD 2, *Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position*. Consistent with that directive, agencies structure their polygraph programs and may use any of the approved types of polygraph. While SEAD 2 does not prohibit disparate application of a given polygraph technique to government employees and contractors, NCSC would defer to individual agencies to discuss the specifics of their programs.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 5: Transparency. The ODNI's most recent report on security clearance determinations was marked FOUO, in contrast to the previous version of this report, which was only UNCLASSIFIED.

Question 5a: Can you please explain what caused the change in the handling caveat?

Answer: Yes. The most recent report provided data in greater detail than in prior reports. Due to the sensitivity of the data presented, as well as the potential benefit possession of that data would provide to adversaries, a determination was made that report would be marked FOUO.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senators Burr and Warner
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 6: Clearance Portability. Is there a reason why the government cannot treat security clearances like a 401(k) that travels with the person, rather than holding the clearances at a particular government agency?

Answer: The government actually does treat security clearances in a manner very similar to a 401(k). Clearances are granted and managed by a sponsoring agency. Sponsorship includes managing the security clearance determination, reporting requirements, continuous evaluation, training, and other oversight responsibilities. While sponsorship rests with a single agency, current reciprocity guidelines direct D/As to reciprocally accept the national security determination and/or the background investigation of an individual if it is of a similar type and is within proscribed age limits. D/As are required to check for the existence of a valid background investigation prior to requesting a new one and to utilize a favorable national security determination to meet a national security access requirement. D/As are also required to document background investigations and adjudications in one of the national databases. Thus, an individual's security clearance is accessible and transportable within the existing personnel security vetting process. The issuance of SEAD 7 will support consistent application of reciprocity.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senator Wyden
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 1: Transparency. The ODNI released to the public the 2015 Annual Report on Security Clearance Determinations.

Question 1a: Does the ODNI intend to release the 2016 and subsequent reports?

Answer: Yes and did so on the ODNI's website in March of this year.

Question 1b: If not, why not?

Answer: N/A

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senator Wyden
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 2: Reducing the Number of Cleared Positions. Please describe progress made in reducing the total number of government positions requiring a security clearance and lowering the clearance level for positions that do require clearances. In which departments, agencies, and offices have there been the most progress, and where has there been the least progress? Are there target goals to reduce the number of positions requiring a clearance? If yes, what current processes are in place for achieving any of these goals?

Answer: The SecEA initiated actions to better manage the size of the cleared national security population. On an ongoing basis, the SecEA reminds D/A heads to review and validate individuals' need for access to classified information. As a result of the SecEA's coordination with agency heads, the eligible national security population has decreased from approximately 5.1 million on October 1, 2013, to roughly 4.0 million on October 1, 2017 – approximately a 20% decrease in the size of the cleared population. The intent is to ensure the national security population is "right-sized," not simply reduced.

The Department of Defense (DoD) has the largest population of personnel with national security eligibility. A majority of the reduction in the national security population resulted from data integrity efforts at DoD that removed personnel who were no longer affiliated with DoD or no longer required national security eligibility.

There are no target goals for security clearances. Rather, the approach seeks to ensure that the Executive Branch has the correct number of personnel with the appropriate security clearances. In support of these efforts the SecEA and the SuitEA jointly revised Title 5 Code of Federal Regulations Part 732 (5 CFR 732), "National Security Positions," and reissued it as 5 CFR 1400, "Designation of National Security Positions in the Competitive Service, and Related Matters." This effort provided greater clarity for D/As in classifying positions requiring national security eligibility. The OPM Position Designation Tool was revised to incorporate the guidance in 5 CFR 1400, and all Executive Branch D/As were required to review existing position designations using the 5 CFR 1400 standards. These efforts seek to ensure that Executive Branch positions are properly designated and that they validate requirements for national security eligibility. The SecEA continues efforts to ensure there is a sufficient number of individuals with the appropriate clearances to meet mission requirements while ensuring unnecessary clearances are not maintained.

Hearing Date: 6 March 2018
Committee: SSCI
Member: Senator Wyden
Witness: ODNI/NCSC, Mr. Brian D.
Info Current as of: July 2, 2018

Question 3: Whistleblowers. On June 18, 2014, Senator Grassley and I wrote the DNI about the potential impact of continuous monitoring and continuous evaluation on whistle blower protections. On July 25, 2014, the DNI responded that "some agencies" were training investigators and that the National Insider Threat Task Force had issued guidance emphasizing legal protections afforded whistleblowers. The DNI further wrote that "the Inspector General of the Intelligence Community, in coordination with the Intelligence Community Inspectors General Forum, is currently examining the potential for internal controls that would ensure whistleblower-related communications remain confidential, while also ensuring the necessary UAM [user activity monitoring] occurs." Please detail any guidance, mechanisms, or procedures related to the controls the Intelligence Community and each of its component entities have implemented to ensure that any security-related personnel monitoring does not compromise the confidentiality of whistleblower-related communications.

Answer: On May 17, 2018, Michael Atkinson was sworn in as the second Senate confirmed Inspector General of the Intelligence Community (IC IG). Since that time, Mr. Atkinson has been reviewing the data available to him regarding the IC IG whistleblowing program and, also, the Intelligence Community Inspectors General Forum (IC IG Forum). With respect to this specific question, he has not located records establishing that the Forum undertook an examination of internal controls to ensure whistleblower-related communications remain confidential, while also ensuring the necessary user activity monitoring (UAM) occurs. During his confirmation process, Mr. Atkinson committed to undertake, in coordination with the IC IG Forum, an immediate review of whistleblower complaints being handled currently by the IC IG and other IC IG Forum members to ensure they are receiving appropriate resources, attention, and priority. The IC IG will also work with the ODNI and the IC IG Forum to identify best practices and procedures governing UAM to enable and encourage lawful whistleblowing while respecting the required balance with insider threat monitoring.

The National Insider Threat Task Force (NITTF) incorporates the importance of privacy, civil rights and civil liberties protections into all training and guidance materials, as well as all of its briefings and presentations. Although whistleblower protections were not uniformly addressed separately in earlier documentation, modifications were made within the past few years to do so explicitly in subsequent materials. NITTF has an active partnership with the Defense Security Service's Center for the Development of Security Excellence to develop Insider Threat training materials for the executive branch and these materials also incorporate this guidance. The criticality of Insider Threat Programs incorporating these protections is grounded in Executive Order 13587 and the National Insider Threat Policy. Examples of these NITTF products include: Hub Operations Course; 2013 Guide to Accompany the National Insider Threat Policy and Minimum Standards; 2016 Protect Your Organization from the Insider Out: Government Best Practices; and the 2017 Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards. The most recent presentation given by the Director of the NITTF was at the 25 April 2018 DARPA Defense Industry Security Symposium in San Diego where he stated, "Your leadership and insider threat program personnel need to consult with legal counsel, privacy and civil liberties and whistleblower protection officers from the outset of the insider threat program. They should be an ongoing part of any insider threat program discussions."

RICHARD BURR, NORTH CAROLINA, CHAIRMAN
MARK R. WARNER, VIRGINIA, VICE CHAIRMAN

JAMES E. RISCH, IDAHO
MARCO RUBIO, FLORIDA
SUSAN M. COLLINS, MAINE
ROY BLUNT, MISSOURI
JAMES LANKFORD, OKLAHOMA
TOM COTTON, ARKANSAS
JOHN CORNYN, TEXAS

DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
MARTIN HEINRICH, NEW MEXICO
ANGUS S. KING, JR., MAINE
JOE MANCHIN, WEST VIRGINIA
KAMALA HARRIS, CALIFORNIA

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CHARLES SCHUMER, NEW YORK, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO
JACK REED, RHODE ISLAND, EX OFFICIO

CHRISTOPHER A. JOYNER, STAFF DIRECTOR
MICHAEL CASEY, MINORITY STAFF DIRECTOR
KELSEY STROUD BAILEY, CHIEF CLERK

May 3, 2018

The Honorable Daniel Coats
Director of National Intelligence
Washington, DC 20511

Dear Director Coats:

Thank you for making Mr. Brian Dunbar available to testify before the Committee at the March 6, 2018 hearing on security clearance reform.

Attached you will find additional questions for the record. Please provide written responses no later than May 25, 2018. If you or your staff have any questions, please contact Vanessa Le or Jon Rosenwasser of the Committee staff at (202) 224-1700.

Sincerely,



Richard Burr
Chairman



Mark R. Warner
Vice Chairman

QUESTIONS FOR THE RECORD
SENATE SELECT COMMITTEE ON INTELLIGENCE
OPEN HEARING ON SECURITY CLEARANCE REFORM
MARCH 6, 2017

Chairman Burr & Vice Chairman Warner

1. Compliance & Enforcement.

- a. Is the Security Executive Agent (SecEA) responsible for reviewing each government agency's compliance with laws, executive orders, and policies regarding the security clearance process? If yes, does this duty include reviewing the policies for reciprocity and/or the robustness of programs for continuous evaluation and insider threat?
- b. Which agency's processes does the SecEA review? How often is this review conducted?
- c. What assessments or reports does the SecEA issue to the agency or to Congress on such compliance?
- d. What are the SecEA's means of enforcing compliance at a particular agency (e.g., through budgets, withholding certain certifications)?

2. Trusted Workforce 2.0.

- a. Who is involved in the DNI-led "Trusted Workforce 2.0" initiative? Are representatives from industry, think tanks, Government Accountability Office, or Congress involved?
- b. What is the scope of the "Trusted Workforce 2.0" effort?
- c. Will the DNI initiative produce any recommendations or policy changes?

3. Reciprocity. Security Executive Agent Directive 4 on reciprocity contains an Appendix C that allows agencies substantial latitude in levying additional requirements before accepting a clearance. The SecEA provides data on reciprocity for the Intelligence Community (IC) pursuant to Sec. 504 of the *Intelligence Authorization Act for Fiscal Year 2014*, but not the rest of government.

- a. As the SecEA, can you please detail what additional requirements IC and non-IC agencies require, by agency, at each clearance level?
- b. As the SecEA, can you please provide data on the time it takes to for both government and industry personnel at the same level (e.g., SECRET, TOP SECRET, SCI) to transfer a clearance from an IC agency to an agency beyond the IC?
- c. Why is it possible for clearance delays to exist within an agency when a cleared individual, either government or contractor, switches projects within the same agency?

4. Government v. Contractor Personnel.

- a. Under existing policy, is a contractor who is "out of scope" for her background investigation treated differently than a government employee who is "out of

scope,” when moving jobs or contracts? If so, please describe how this treatment differs.

- b. Can an agency have one policy for use of the polygraph for its cleared government population and a different policy for its contractor community? If so, please provide an example.
5. **Transparency.** The ODNI’s most recent report on security clearance determinations was marked FOUO, in contrast to the previous version of this report, which was only UNCLASSIFIED.
 - a. Can you please explain what caused the change in the handling caveat?
6. **Clearance Portability.** Is there a reason why the government cannot treat security clearances like a 401(k) that travels with the person, rather than holding the clearances at a particular government agency?

Sen. Ron Wyden

1. **Transparency.** The ODNI released to the public the 2015 Annual Report on Security Clearance Determinations.
 - a. Does the ODNI intend to release the 2016 and subsequent reports?
 - b. If not, why not?
2. **Reducing the Number of Cleared Positions.** Please describe progress made in reducing the total number of government positions requiring a security clearance and lowering the clearance level for positions that do require clearances. In which departments, agencies, and offices have there been the most progress, and where has there been the least progress? Are there target goals to reduce the number of positions requiring a clearance? If yes, what current processes are in place for achieving any of these goals?
3. **Whistleblowers.** On June 18, 2014, Senator Grassley and I wrote the DNI about the potential impact of continuous monitoring and continuous evaluation on whistleblower protections. On July 25, 2014, the DNI responded that “some agencies” were training investigators and that the National Insider Threat Task Force had issued guidance emphasizing legal protections afforded whistleblowers. The DNI further wrote that “the Inspector General of the Intelligence Community, in coordination with the Intelligence Community Inspectors General Forum, is currently examining the potential for internal controls that would ensure whistleblower-related communications remain confidential, while also ensuring the necessary UAM [user activity monitoring] occurs.” Please detail any guidance, mechanisms, or procedures related to the controls the Intelligence Community and each of its component entities have implemented to ensure that any security-related personnel monitoring does not compromise the confidentiality of whistleblower-related communications.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF LEGISLATIVE AFFAIRS
WASHINGTON, DC 20511

JUL 31 2018

The Honorable Richard Burr
Chairman
Senate Select Committee on Intelligence
United States Senate
Washington, DC 20510

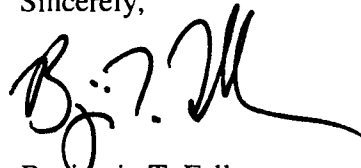
The Honorable Mark R. Warner
Vice Chairman
Senate Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Burr and Vice Chairman Warner:

This correspondence responds to Questions for the Record entered by Senator Tom Cotton (R-AR) and Senator Susan Collins (R-ME) for VADM Joseph Maguire for his July 25, 2018 open confirmation hearing for the position of Director of the National Counterterrorism Center. The requested information is enclosed.

If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,

A handwritten signature in black ink, appearing to read "B. T. Fallon", with a long horizontal flourish extending to the right.

Benjamin T. Fallon
Director of Legislative Affairs

Enclosure:

Responses to Questions for the Record from the July 25, 2018 Confirmation Hearing before the Senate Select Committee on Intelligence

Hearing Date: 25 July 2018
Committee: SSCI
Member: Sen. Tom Cotton (R-AR)
Witness: VADM Joseph Maguire
Info Current as of: 27 July 2018

It has been publicly reported that on Saturday, June 30, 2018, a Belgian security unit detained a married couple of Iranian origin at a traffic stop in a residential neighborhood of Brussels. They were found to be carrying 500 grams of the military-grade explosive TATP along with a detonation device, which the couple allegedly obtained in Luxembourg from a Vienna-based Iranian diplomat.

Further, it was reported that on Sunday, July 1, 2018, German Security forces detained the Iranian diplomat and three companions. The Iranian diplomat was reportedly racing back to Vienna where he had diplomatic immunity.

While these operations were unfolding, French officials reportedly detained several Iranian-origin nationals linked to the Brussels suspects.

Question 1: What does this report tell you about the brazenness of Iranian intelligence services to commit attacks in Europe that would kill hundreds if not thousands of peaceful European citizens?

Answer: Stepping back and looking at this thwarted attack in the referenced news report, it appears that Iran lacks a clear understanding of U.S. and European decision calculus regarding terrorist activity. It also suggests that Tehran views Iranian dissident groups as an enduring threat to its national security, such that it is willing to conduct lethal operations against these groups in Europe despite the possibility of killing or injuring European and U.S. citizens, potentially including high-ranking U.S. officials.

Hearing Date: 25 July 2018
Committee: SSCI
Member: Sen. Tom Cotton (R-AR)
Witness: VADM Joseph Maguire
Info Current as of: 27 July 2018

Question 2: Is there any doubt in your mind that Iran is still the number one state sponsor of terrorism in the world today?

Answer: I have no doubt that Iran is the number one state sponsor of terrorism today, and I would refer back to my statement for the record that, in addition to being the world's most active state sponsor of terrorism, Iran is by far the most prolific financier of terrorist organizations in the world.

Hearing Date: 25 July 2018
Committee: SSCI
Member: Sen. Tom Cotton (R-AR)
Witness: VADM Joseph Maguire
Info Current as of: 27 July 2018

Question 3: On Sunday evening, at the Reagan Library, Secretary Pompeo described how the Iranian security services are getting rich at the expense of the general population and that sanctions targeting the Iranian economy will not go away while attacks like these continue. Do you agree with Secretary Pompeo?

Answer: Should I be confirmed as director of NCTC, I would reach back to the experts in my organization and the broader intelligence community to understand how the current social and economic environment in Iran might impact the terrorist threat posed by Iranian-aligned groups worldwide.

Hearing Date: 25 July 2018
Committee: SSCI
Member: Sen. Tom Cotton (R-AR)
Witness: VADM Joseph Maguire
Info Current as of: 27 July 2018

Question 4: What kind of response is required by the Germans, Austria, French, Belgians, and others so that Iran realizes that this kind of state sanctioned terrorist behavior will not be tolerated?

Answer: I stated during my testimony how important partnerships are and as NCTC Director, if confirmed, I would ensure that we continue to work closely with U.S. partners and allies, such as the Germans, Austrians, French, and Belgians, to ensure that Iranian terrorist operations will not endanger innocent civilians across the globe. As the disrupted plot in Paris demonstrates, when our allies understand the depth and breadth of Iranian malign activities, our relationships grow even stronger and we can successfully disrupt these terrorist operations. I hope a lawful conviction will send a strong message to the Iranian regime that these actions will not be tolerated. The disruption of the plot in Europe appears to have required security officials across several countries to work together to share information, a positive sign for the future. Overall, I will champion a U.S. position that will support and encourage our European partners to join us in confronting Iranian malign activities around the world.

Hearing Date: 25 July 2018
Committee: SSCI
Member: Sen. Susan Collins
Witness: VADM Joseph Maguire
Info Current as of: 27 July 2018

Question 1: NCTC's most important resource is its people. The organization is unique in the community, however, by its reliance on detailees. What is your plan to attract and retain talented staff for multiple years from other agencies?

Answer: I agree that the people and the unique skills, knowledge, and backgrounds that each person brings are critical to NCTC mission success and are its most important asset. NCTC relies heavily on detailees from other departments and agencies to achieve this success. The experiences these officers bring to the Center are vital to every aspect of NCTC's mission and continuing to attract and retain detailees will be one of my highest priorities. I will need to build strong relationships with my interagency partners to ensure that they understand the value of having their employees do rotations in NCTC. In order to ensure that we get that buy-in from other agencies, I believe a first step is to conduct a thorough review of NCTC's mission-critical staffing requirements. This review is vital to make informed decisions on how to prioritize our needs ahead of any engagement with our partner departments and agencies on this issue. In addition, NCTC must continue to foster a workplace that is inclusive, dynamic, and viewed as career-enhancing by our partner agency workforces.

Hearing Date: 25 July 2018
Committee: SSCI
Member: Sen. Susan Collins
Witness: VADM Joseph Maguire
Info Current as of: 27 July 2018

Question 2: In Wednesday's hearing you discussed the perennial "lanes in the road" challenge regarding how the IC covers CT issues. CIA's Counterterrorism Mission Center and NCTC's Directorate of Intelligence remain the two most obvious areas of overlap, especially on strategic terrorism analysis. What is your position on how these two organizations should cover CT and how would you implement this as the next National Intelligence Manager for Counterterrorism?

Answer: In an environment of competing national security priorities and resource constraints, I understand how minimizing any redundancy—analytic or otherwise—is critical. I believe NCTC is well-positioned to identify redundancy in terrorism analysis across the IC and to work with the ODNI and the broader IC to reduce such instances. I understand that NCTC is already taking steps to systematically and objectively look into this issue and identify potential unnecessary redundancies across the U.S. counterterrorism community. For example, I know NCTC is examining the extent of analytic redundancy in CT-focused finished products, and should I be confirmed, I look forward to learning more about the detailed findings. I know from discussions with NCTC leadership the Center takes efforts to monitor planned and published CT articles in other product lines to avoid unwanted redundancy and minimize the impact for the Center's customers. If confirmed, I am committed to continuing this review process started by NCTC and to taking a hard look at the "lanes in the road" issue with NCTC's IC partners to reduce unnecessary redundancy.

RICHARD BURR, NORTH CAROLINA, CHAIRMAN
MARK R. WARNER, VIRGINIA, VICE CHAIRMAN

JAMES E. RISCH, IDAHO
MARCO RUBIO, FLORIDA
SUSAN M. COLLINS, MAINE
ROY BLUNT, MISSOURI
JAMES LANKFORD, OKLAHOMA
TOM COTTON, ARKANSAS
JOHN CORNYN, TEXAS

DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
MARTIN HEINRICH, NEW MEXICO
ANGUS S. KING, JR., MAINE
JOE MANCHIN, WEST VIRGINIA
KAMALA HARRIS, CALIFORNIA

MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CHARLES SCHUMER, NEW YORK, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO
JACK REED, RHODE ISLAND, EX OFFICIO

CHRISTOPHER A. JOYNER, STAFF DIRECTOR
MICHAEL CASEY, MINORITY STAFF DIRECTOR
KELSEY STROUD BAILEY, CHIEF CLERK

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

July 26, 2018

Vice Admiral Joseph Maguire
c/o Office of the Director of National Intelligence
Washington, DC 20511


Dear Vice Admiral Maguire:

We appreciate your testimony before the Committee on July 25, 2018. We are submitting the attached questions for the record, and we request a response as soon as possible. Please refer any questions you may have concerning the Committee's consideration of your nomination to Don Martin at (202) 224-1700.

Sincerely,



Richard Burr
Chairman



Mark R. Warner
Vice Chairman

Enclosure

UNCLASSIFIED

QUESTIONS FOR THE RECORD

From Senator Cotton

It has been publicly reported that on Saturday, June 30, 2018, a Belgian security unit detained a married couple of Iranian origin at a traffic stop in a residential neighborhood of Brussels. They were found to be carrying 500 grams of the military-grade explosive TATP along with a detonation device, which the couple allegedly obtained in Luxembourg from a Vienna-based Iranian diplomat.

Further, it was reported that on Sunday, July 1, 2018, German security forces detained the Iranian diplomat and three companions. The Iranian diplomat was reportedly racing back to Vienna where he had diplomatic immunity.

While these operations were unfolding, French officials reportedly detained several Iranian-origin nationals linked to the Brussels suspects.

1. What does this report tell you about the brazenness of Iranian intelligence services to commit attacks in Europe that would kill dozens if not hundreds of peaceful European citizens?
2. Is there any doubt in your mind that Iran is still the number one state sponsor of terrorism in the world today?
3. On Sunday evening, at the Reagan Library, Secretary Pompeo described how the Iranian security services are getting rich at the expense of the general population and that sanctions targeting the Iranian economy will not go-away while attacks like these continue. Do you agree with Secretary Pompeo?
4. What kind of response is required by the Germans, Austrians, French, Belgians, and others so that Iranian realizes that this kind of state sanctioned terrorist behavior will not be tolerated?

UNCLASSIFIED

UNCLASSIFIED

From Senator Collins

1. NCTC's most important resource is its people. The organization's reliance on detailees is, however, unique in the Intelligence Community. How do you plan to attract and retain talented staff (for multiple-year details) from other agencies?
2. During Wednesday's hearing you discussed the perennial "lanes in the road" challenge regarding how the IC covers CT issues. CIA's Counterterrorism Mission Center and NCTC's Directorate of Intelligence remain the most obvious areas of overlap, especially on strategic terrorism analysis. What is your position on how these two organizations should cover CT, and avoid duplication, and how would you implement this as the next National Intelligence Manager for Counterterrorism?

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF LEGISLATIVE AFFAIRS
WASHINGTON, DC 20511

DEC 15 2017

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Johnson:

(U) This correspondence responds to Questions for the Record entered by Senator Daines (R-MT), Senator McCain (R-AZ), Ranking Member McCaskill (D-MO), and Senator Peters (D-MI) for Director Rasmussen of the National Counterterrorism Center during the Committee's September 27, 2017 open hearing on "Threats to the Homeland." The requested information is enclosed.

(U) If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,

A handwritten signature in black ink, appearing to read "Deirdre M. Walsh", with a stylized flourish at the end.

Deirdre M. Walsh

Enclosure:

(U) "Response to Questions for the Record from 27 September 2017 Hearing before the Committee on Homeland Security and Governmental Affairs"

Hearing Date: 27 September 2017

Committee: Senate Homeland Security & Governmental Affairs

Member: Senator Daines (R-MT)

Witness: D/NCTC Rasmussen

Info Current as of: 8 December 2017

Question: 1

Question 1: Mr. Rasmussen, thank you for testifying. As everyone mentioned, threats to the homeland have only grown and diversified. From domestic and foreign actors to man-made and natural threats, this year, we have seen wildfires ravage my home state of Montana and hurricanes flatten our neighbors in the southeast, gangs and drug trafficking devastate families across the country, and ISIS inspired shootings – all which have led to the loss of American lives.

Mr. Rasmussen, you touched on social media platforms being used to spread vile propaganda. We as a society encourage the free flow of information and ideas. But there are limits. This platform has enabled reward for illegal and gruesome actions. We must stop it. How do we protect First Amendment rights while also encouraging private business to improve identification and filtration of terrorist propaganda?

Answer:

The National Counterterrorism Center (NCTC) believes companies want to do more; however, they may not have the counterterrorism experience required to differentiate between a non-violent Arab opposition group, and the propaganda of a designated foreign terrorist organization. NCTC is exploring ways to educate companies on broader violent extremist online trends and support companies' efforts to identify official terrorist propaganda.

NCTC has recently seen industry do more to address terrorists' use of their platforms and has reached out to several companies to gain a better understanding of how NCTC could be helpful in this regard.

Specifically - Twitter, Telegram and several other social media and hosting service providers are working to improve their capability to automatically identify and delete ISIS-related content. This effort is complicated by ISIS's ability to reconstitute closed accounts and quickly adjust media practices, and migrate to new platforms when necessary.

Finally, as it is impossible to completely remove terrorist content from the Internet, NCTC continues to work with civil society, coalition partners, and industry to ensure that alternative narratives are available to individuals who are exploring terrorist propaganda and considering a pathway to violence – while protecting the first amendment rights of those in the United States.

Hearing Date: 27 September 2017

Committee: Senate Homeland Security & Governmental Affairs

Member: Senator McCain (R-AZ)

Witness: D/NCTC Rasmussen

Info Current as of: 8 December 2017

Question: 2

Question 2: CYBERSECURITY - No Policy and No Strategy: Our greatest frustration has been the lack of any direction from this administration, or from the prior administration, on how we should be deterring our adversaries in cyberspace. Among other urgent problems, we need to define what forms of cyber-attack constitute an act of war and how authorities for cyber responses should be delegated to various agencies. We must also consider geographic and sovereignty issues; the list goes on.

- Do you agree that until our adversaries believe the consequences of an attack in cyberspace will outweigh the benefits, behaviors will not change?
- What are the chief impediments to crafting a coherent strategy?

UK's National Cyber Security Center: Our cyber efforts are divided among DoD, DHS, and the FBI. In contrast, Britain has adopted a unified model in the recently established National Cyber Security Centre. Our British allies recognize the twin absolute necessities of bringing all capacity under one roof and acting in close partnership with the private sector.

- Are you familiar with the UK's NCSC, and do you believe it is something we should pursue here in the U.S.?
- Do you agree that we should reevaluate the roles and responsibilities of DHS or pursue a model that combines our government-wide expertise in a center like the UK established?
- Is the current approach working; is the status quo effective?

Answer:

Cybersecurity does not fall under the mission of the National Counterterrorism Center. NCTC respectfully defers to our partners, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) who joined NCTC at the 27 September Hearing; as a direct response on questions related to preparedness, response, strategic planning and comparisons to our foreign partners on cyber related security efforts are best answered by DHS & FBI.

Hearing Date: 27 September 2017

Committee: Senate Homeland Security & Governmental Affairs

Member: Senator/Ranking Member McCaskill (D-MO)

Witness: D/NCTC Rasmussen

Info Current as of: 8 December 2017

Questions: 3 - 7

Question 3: Terrorism - Europe has experienced a number of attacks recently, including a rise in the use of ramming attacks. We have not experienced the same frequency of attacks in the United States. To what factors do you attribute the lower frequency?

Answer:

Homegrown violent extremist (HVE) arrests and disruptions in the U.S. in 2017 have been on par with 2016, and the number of successful attacks has fallen from six in 2016 to three in the first 10 months of this year, including the most recent attack in New York City on October 31.

Despite the lower number of attacks here than Europe, NCTC continue to assess that the threat from HVEs in the U.S. remains the most immediate and unpredictable. NCTC assesses HVEs are likely to continue to use simple tactics, such as edged weapons or vehicle assaults, and may see others attempt to copy previously successful attacks.

Multiple factors probably contribute to a higher frequency of terrorist attacks in Europe than in the U.S. Europe is in close geographic proximity to Iraq and Syria and has a significantly larger pool of potential violent extremists and former foreign fighters that ISIS can leverage for directed or enabled attacks. Unlike the more dispersed and integrated immigrant communities in the U.S., European immigration settlement policies over the last several decades have helped create large marginalized minority communities who might be more receptive to ISIS's propaganda encouraging attacks because of a shared sense of isolation and perceived religious discrimination.

Question 4: Ramming attacks are on the rise globally and in the U.S. What can communities do to prevent or mitigate these kinds of attacks?

Answer:

NCTC, DHS, and FBI routinely issue unclassified threat familiarization products to law enforcement and first responders to help identify potential vulnerabilities and aid response planning.

With specific regard to ramming attacks, some potential prevention or mitigation techniques include physical security considerations, such as installation of bollards/barriers to limit access, controlling traffic access, law enforcement and security officer visibility, and improving ingress and egress routes.

The Intelligence Community and law enforcement officials regularly participate in outreach and education initiatives, such as performing joint private-sector and local law-enforcement terrorism exercises, encouraging local businesses to share security plans with law enforcement, and conducting response planning encompassing the private and public sectors.

Question 5: What steps do you recommend to address the vulnerabilities posed by social media?

Answer:

NCTC works to ensure a continuing dialogue with tech companies and, where possible, fill knowledge gaps that help them to identify terrorist materials that violate their content policies. This includes involving smaller companies and startups in these conversations and building mechanisms for our own counterterrorism experts to share some of their knowledge with industry. NCTC views industry's establishment of the Global Internet Forum to Counter Terrorism last summer as a positive step.

Our understanding is that this forum is intended to bring smaller companies into conversations on addressing terrorism that once only involved the largest social media platforms.

The Hash Sharing Coalition that some members of the Global Internet Forum to Counter Terrorism are working on is particularly promising and NCTC applauds its efforts to use technology to more efficiently enforce members' terrorist content policies.

Finally, as it is impossible to completely remove terrorist content from the Internet, NCTC continues to work with civil society, coalition partners, and industry to ensure that alternative narratives are available to individuals who are exploring terrorist propaganda and considering a pathway to violence – while protecting the first amendment rights of U.S. citizens.

Question 6: In your opinion, if there is a terrorist attack on U.S. soil in the future, how likely is it that transportation systems or a “soft target” location will be targeted?

Answer:

As demonstrated by the recent attack in New York City on October 31, NCTC believes that future terrorist attacks in the U.S. will continue to target soft targets or targets of opportunity, including some transportation systems. HVEs are likely to remain focused on soft targets because of the increased perception of success, lower levels of security, ease of access, and familiarity with the target.

ISIS and al-Qa'ida probably remain intent on attacking transportation systems because of the potential for mass casualties, amount of media coverage generated, resulting fear and anxiety amongst the targeted population, and the economic costs associated with such attacks. Specifically, successful aviation attacks during the past few years encouraged terrorists to focus

on aviation by cultivating the perception that it may not be a hard target and by promoting copycat attacks, based on the apparent ease with which public areas were attacked in Zaventem Airport in Brussels, Belgium.

Recent ISIS attacks against transportation targets include the Ataturk Airport attack in Istanbul, Turkey that killed 44 individuals, and the Zaventem Airport and the Maalbeek metro station attack in Brussels that killed 32 people.

Violent extremist publications, including ISIS's *Dabiq* and *Rumiyah* magazines and AQAP's *Inspire*, encourage attacks against aviation targets and trains and provide ways to circumvent airport security or potential derailment tools. Al-Qa'ida leadership continues to herald the success of 9/11 and reiterates calls for attacks in the West, referring potential operatives to *Inspire* magazine as a source of reference.

Transportation related attacks are likely to cause significant economic damage. Zaventem Airport lost an estimated 5 million euros the day it was shut down, and it is difficult to calculate the revenue that nations divert to increased security measures.

Surface transportation systems cannot employ airport-type screening because of the volume of passengers who use rail and bus lines on a daily basis, and expanding security perimeters could create large passenger bottlenecks at entrances that could themselves become attractive targets.

These types of attacks do not require a high degree of skill or training, would not require attackers to breach security checkpoints, and could be carried out with little or no warning. While transportation and soft targets remain the most probable focus for terrorists, they probably retain the intent to attack symbolic targets, to include U.S. Government and military targets, and would probably prioritize those where the likelihood for success is higher.

NCTC cannot discount the possibility that a U.S.-based violent extremist may use insider access to conduct an attack on a hardened target, as happened in November 2009 when Nidal Hassan conducted an attack on Fort Hood.

Question 7: Information Sharing - The Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) released a joint report in March 2017 reviewing domestic sharing of counterterrorism information. The report found that improving information sharing required federal, state, and local entities involved in counterterrorism to better understand the other's roles, responsibilities, and contributions. What is the status of the implementation of the IGs' recommendations at the National Counterterrorism Center?

Answer:

Of the 23 Recommendations within the March 27, 2017 – Joint Inspector General Report – numbers 1, 2 & 22 are specific to NCTC.

Through 1 & 2, the IC IG and DHS and DOJ OIGs recommend that the ODNI, DHS, and DOJ review the 2003 interagency MOU on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments. Number 2 also recommends codifying an overarching engagement and coordination body for the terrorism-related ISE.

Specific to Recommendation 1, NCTC concurs with the determinations made through a joint assessment by ODNI, DHS, DOJ and FBI; that laws, Presidential directives, and regulations, along with Department and Agency policies, and various MOUs subsequent to the 2003 MOU, have further defined and refined the standards and processes, and reflect the current structure, roles, and responsibilities of the ISE partners and the current threat environment and priorities. Further, NCTC concurs with the assessment that updating the 2003 MOU is unnecessary because it has been superseded by subsequent intelligence information sharing standards and processes that have the effect of affirming and formalizing the roles and responsibilities of partners in the current information-sharing environment. NCTC concurred with the assessment, supported the recommendation, and considers the recommendation closed.

Specific to Recommendation 2, NCTC concurs with the determinations made through a joint assessment by ODNI, DHS, DOJ and FBI that as prescribed in section 1016(g) (2) of IRTPA, that the Act established the ISC as the overarching engagement and coordination body for the terrorism-related ISE. Further, NCTC also concurs with the joint assessment that there is no need to codify a separate body with the same responsibilities. NCTC concurred with this assessment, supported the recommendation, and considers the recommendation closed.

Through Recommendation 22, the IC IG recommends that the Director, National Counterterrorism Center, consider assigning additional NCTC representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

Specific to Recommendation 22, NCTC plans to establish a Domestic Representative position in Detroit, Michigan, in the fourth quarter of fiscal year (FY) 2018. The NCTC Domestic Representative Program is the cornerstone of NCTC's mandate to collaborate with regional Intelligence Community agencies and counterterrorism (CT) officials. NCTC has Domestic Representatives in eleven U.S. cities, co-located with FBI field offices. Each representative serves as a liaison for NCTC's Director, providing tailored analytic briefings to CT partners, contributing to ongoing CT investigations, and facilitating the flow of strategic and regional CT information to and from NCTC, while coordinating with the FBI and the Department of Homeland Security. The addition of a Domestic Representative position in Detroit will help alleviate the geographic challenges placed on NCTC's representative in Chicago, who is responsible for supporting CT partners in nine states, and will enable NCTC to manage more effectively key CT partnerships and competing regional priorities. The fourth quarter FY2018 timeframe will enable adequate time for the selection process and will align with the turnover of the current Chicago Representative to ensure a smooth transition.

Hearing Date: 27 September 2017

Committee: Senate Homeland Security & Governmental Affairs

Member: Senator Peters (D-MI)

Witness: D/NCTC Rasmussen

Info Current as of: 8 December 2017

Questions: 8 – 12

Question 8: A bioterrorist attack could have a devastating impact in a major city, both in terms of human life and our sense of safety and security. However, reports such as the Blue Ribbon study panel's report on biodefense have indicated that our national defense against bioterrorism is lacking in both detection capability and response. In the 2016 Worldwide Threat Assessment, the CRISPR gene editing tool was identified as a key enabling technology that could be used by terrorists to more easily create a biological weapon. Among the terrorist threats facing the homeland, how worried are you about bioterrorism as compared to other threats such as conventional terrorism or dirty bombs?

Answer:

NCTC expects most terrorists to continue pursuing conventional attacks over biological, chemical, radiological, or nuclear materials in attacks against the U.S. homeland, because conventional capabilities are more familiar and easier to acquire for most terrorists. NCTC remains concerned about the threat of bioterrorism; however, some bioterrorism scenarios could have a disproportionate impact compared to typical conventional attacks or even a dirty bomb.

Question 9: How much does the rapid spread of biotechnology due to advancements such as CRISPR impact your assessment of the threat of bioterrorism?

Answer:

NCTC believes that in the near term, non-state actors are more likely to seek to conduct bioterrorism attacks with traditional BW agents rather than genetically modified organisms. However, NCTC continues to monitor for indications non-state actors are seeking to use advanced biotechnologies such as CRISPR to acquire or advance a bioterrorism capability.

Using CRISPR to genetically modify organisms does not bypass the need for life science knowledge and experience, and successfully using CRISPR can pose challenges even for experienced life scientists.

Question 10: Could CRISPR be used by someone who doesn't have bad intentions, but perhaps isn't taking the proper safety precautions, to inadvertently cause a health emergency?

Answer:

NCTC believes that the chances that a hobby-level project involving genome editing technologies such as CRISPR could unintentionally result in a public health crisis in the near term are very low because currently these projects typically involve benign materials unlikely to create a harmful organism. Health emergencies from biosafety lapses could occur even without the use of genome editing technologies, for instance the inadvertent release of a highly transmissible, naturally occurring pathogen.

Question 11: Is NCTC prepared to deal with the emerging bioterror threats that exist today?

Answer:

NCTC maintains vigilance against emerging bioterror threats by monitoring all-source reporting for any potential intersection between malevolent non-state actors, individuals with skills or expertise that could be used to support a bioterrorism effort, and advances in biotechnology. NCTC also works with collectors to promote intelligence collection on non-state groups interested in biological threats. NCTC serves a central role in managing terrorist crises, and regularly exercises how it would leverage existing crisis management capabilities and responsibilities in a WMD event.

Question 12: What can NCTC do to better prepare for these threats?

Answer:

Monitoring these types of emerging bioterror threats takes a variety of expertise. To better prepare for any possible technology-enabled bio-threat, NCTC not only leverages internal expertise, but also routinely consults other technical subject matter experts within the U.S. Intelligence Community and outside the U.S. Government to stay informed of advances in relevant biological sciences and their potential threat implications. NCTC will continue to work to improve information sharing, collection, and analysis against non-state actors interested in leveraging biotechnology for nefarious purposes.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

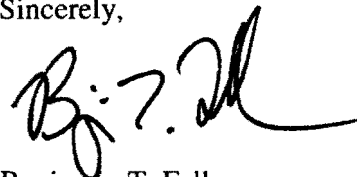
FEB 28 2019

Dear Chairman Johnson:

In response to your letter dated October 26, 2018, I am providing the enclosed document which addresses the post-hearing questions submitted by Senator Kamala Harris and Senator Doug Jones during the hearing titled "Threats to the Homeland."

Should you have any questions, please contact Legislative Affairs at (703) 275-2474.

Sincerely,

A handwritten signature in black ink, appearing to read "Bj. T. Fallon", with a stylized flourish extending to the right.

Benjamin T. Fallon
Assistant DNI for Legislative Affairs

Enclosure:

1. Post-Hearing Questions for the Record submitted to Mr. Russell Travers from Senator Kamala Harris and Senator Doug Jones, "Threats to the Homeland," October 10, 2018

cc: The Honorable Gary Peters, Ranking Member

**Post-Hearing Questions for the Record
Submitted to Mr. Russell Travers
From Senator Kamala Harris**

**“Threats to the Homeland”
October 10, 2018**

On NCTC’s Strategy to Address Evolving Threats

The NCTC was founded in the aftermath of 9/11 to collect and analyze intelligence about potential terrorists. As the threats our nation faces evolve—so must the work of NCTC. As such, overtime, the agency’s focus has shifted from al-Qaida to homegrown threats and ISIS. These new actors have adopted different tools and different targets. Instead of recruitment requiring proximity, these entities can use extremist propaganda to reach any vulnerable and disaffected person with an internet connection. Instead of pursuing hard targets such as buildings or monuments these entities are attacking “soft targets” such as pedestrians on the sidewalk.

1. In your opinion, what intelligence tools are needed to address these new and evolving threats?

The Center’s ability to address threats largely hinges on its ability to effectively cull through an ever-growing volume and variety of data. Given this trend, the Center will become more reliant on enabling data integration technologies, which provide analysts access to machine matched results. As such, NCTC needs to invest in the next generation of tools that leverage automated intelligence and machine learning technologies, which not only empower CT analysts, but multiply analytic capabilities.

2. Under your leadership, what has the NCTC done to minimize the reach and potency of extremist propaganda? Please be specific.

Countering terrorists’ ability to inspire individuals to conduct attacks in our homeland remains a priority for our workforce and is a mission that requires our government to apply nearly all tools at its disposal.

Under my leadership, our analysts continue to support our intelligence, law enforcement, and military counterparts with analytic production that explains how terrorists are seeking to use communications technologies—including social media—to expand their global reach and identifies opportunities for the US Government and our partners to disrupt those activities.

We also recognize the important role that the technology sector plays in minimizing terrorists’ exploitation of their platforms. Under my leadership, and that of Director Rasmussen before me, NCTC expanded its efforts to educate the tech sector on terrorism issues, such as the trends in terrorists’ use of tech platforms, through the provision of informational briefings and analytic products. NCTC also has participated in meetings held by the industry-led Global Internet Forum

to Counter Terrorism, which focuses on fostering collaboration between small and large tech companies on terrorism-related issues.

I also recognize the important role our government can play in refuting the narratives of terrorist organizations and providing alternative narratives to consumers of terrorist propaganda. As such, NCTC is providing intelligence support to our operational counterparts involved in countering terrorist messaging at the Department of Defense and the Department of State's Global Engagement Center.

Finally, NCTC views terrorism prevention efforts as a critical component in reducing the appeal of terrorist messaging and helping to stop individuals who might be vulnerable to such messaging from mobilizing to violence. In recognition of the important role local community organizations can play in helping to intervene before individuals radicalize to violence, NCTC has provided Community Awareness Briefings to groups around the country aimed at helping them identify and understand the signs of radicalization.

3. Under your leadership, what has the NCTC done to prevent attacks on "soft targets"? Please be specific.

The Intelligence Reform and Terrorism Prevention Act of 2004 established the Information Sharing Environment to be the combination of policies and technologies linking the resources (people, systems, databases, and information) of federal, state, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration among users to combat terrorism more effectively. The Joint Counterterrorism Assessment Team (JCAT) directly realizes the intent of the act. JCAT is a collaboration by the National Counterterrorism Center (NCTC), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) in the truest sense of the word. It was established in 2013 and the program embeds public safety (law enforcement, fire, emergency medical services, health and human services, emergency planners) personnel in the Intelligence Community to improve information sharing among federal and non-federal governments, the private sector and the general public, and to enhance public safety in the homeland against international terrorism. Each of the three federal organizations sponsors fellowships for highly-qualified public safety personnel to work in the CT mission space, where they develop reporting and reference materials at the lowest possible classification for broad distribution that may be useful to the widest range of audiences. They perform extensive outreach to public safety partners and they support the development and delivery of joint CT exercises and training to the same.

JCAT publications frequently address the challenges of protecting soft targets. The publications are unclassified and are distributed widely. They depict an environment in which all stakeholders in an emergency response from law enforcement, to fire, to emergency medical services and to security personnel must understand their collective roles and responsibilities in order to effectively work together. The products provide indicators, suggestions, considerations and additional resources tailored to each topic. JCAT publications are developed with the assistance of subject matter experts from relevant fields and jurisdictions, from outside the intelligence and public safety communities, including the private sector. Previous publications have covered soft

targets, such as malls (2014 and 2017), stadiums (2014), hotel high-rises (2015), mass transit (2016), open-access special events (2016), religious facilities (2017) and bridges (2018). The products have been cited by national security, public safety and private sector officials, both domestically and internationally, for their usefulness and impact. In November 2017, JCAT published a product on terrorist attacks from elevated positions and as a result, the District of Columbia Fire and Rescue Department when dispatched to an alleged active shooter at a tall building in SE Washington, DC, broke with standard procedure. The department stated the decision was influenced by the recommendations of the product. Unclassified JCAT products are available at www.dni.gov.

The NCTC Counterterrorism Readiness Exercise Program is a leading provider of counterterrorism exercises to State and local customers. This program is focused on enhancing an entity's ability to apply prevention and protection measures in response to terrorist threats and attacks. NCTC develops exercise scenarios for both discussion and operation-based events that entail real-world, soft targets to include: airports, seaports, trains, stadiums, hotels, concerts, parades, shopping venues, and more. NCTC has supported the following exercise events in 2018: BWI Airport, MD; Carson City, NV; Jackson International Airport, MS; Salt Lake City, UT; and, Seattle, WA.

The Joint Counterterrorism Awareness Workshop Series (JCTAWS), sponsored by NCTC, DHS, and FBI, is a nationwide initiative designed to improve the ability of local jurisdictions to prepare for, protect against, and respond to complex terrorist attacks. JCTAWS, held in cities across the US, brings together federal, state, and local participants representing law enforcement, fire, emergency medical services, communication centers, private sector communities, and nongovernment organizations to address this type of threat. NCTC designs and develops the exercise scenarios for this program which are focused on the most likely attack the State or local governments will face in the near future, which are typically soft targets as outlined above. In 2018, this program supported: Aurora/Naperville, IL; Eugene, OR; Honolulu, HI; and Salt Lake City, UT.

NCTC is a joint partner with DHS in support of their Science and Technology Exercise Partnership Showcase (STEPS). This program is used to exercise first responders on soft targets which has included: schools, movie theaters, churches, subways, stadiums and train stations. STEPS showcases and delivers innovative solutions through the demonstration of current and emerging technologies in a realistic operational environment. During these events, NCTC delivers three iterations of a full scale exercise against select soft targets. This exercise allows first responders to sample the technologies as they simultaneously address their response to a terrorist event. An operational analysis is provided at the conclusion of the exercise regarding the responder's ability to prevent, protect from, respond to and recover from the attack. NCTC is currently working with DHS S&T on the development of an exercise in support of Seattle's Puget Sound Ferry System and Boston's TD Gardens Stadium.

Since October 2007, NCTC has placed 11 officers as Domestic Representatives in the following U.S. cities: Atlanta; Boston; Chicago; Denver; Houston; Los Angeles; Miami; New York City; San Francisco; Seattle; and Washington, D.C.

Each Domestic Representative serves as the front-line liaison for NCTC's Director and leadership team through multi-faceted engagements with federal, state, local, and private industry partners. NCTC's Domestic Representatives work closely with FBI Field Offices, JTTFs, other government agencies, local police departments, and first responders with CT missions in their regions, providing intelligence support to facilitate collaboration and enable the targeting, collection, processing, and reporting of CT-related interests.

The Domestic Representatives facilitate the flow of both strategic and regional CT information to and from NCTC while coordinating with the FBI and DHS, ultimately deferring to those agencies' domestic authorities to share CT information with federal, state, local, and private industry partners. Their duties also include: ensuring senior IC officials have access to NCTC analysis and strategic planning resources such as NCTC CURRENT; taking part in Joint Terrorism Task Force (JTTF) meetings; ensuring NCTC analysts and principals have up-to-date CT information from the field; and facilitating engagements and travel for NCTC principals, analysts, and planners to their respective regions.

The Office of National Intelligence Management for Counterterrorism (NIM-CT) leads production of the Homegrown Violent Extremist Mobilization Indicators (HVE MI) booklet, a guide intended primarily for public safety officials to support their efforts to combat the threat against soft targets. We have distributed over 60,000 hard copies of this product and annual updates since its initial publication in December 2015, and estimate soft-copy distribution to be in the hundreds of thousands. Multiple federal, state, and local law enforcement partners also have printed HVE MI booklets to meet stakeholder demand. NIM-CT complements the HVE MI booklet distribution with several parallel efforts including the dissemination of Mobilization Indicators HVE case studies, provision of briefings, and national and regional HVE practitioner conferences. In these activities, NIM-CT, with our DHS and FBI partners, work with multiple public safety, state homeland security, corrections, and homeland defense organizations, integrating the broader CT community and enabling improvements in their capability to address the HVE problem set. Finally, multiple foreign liaison law enforcement and intelligence organizations have adapted the booklet to help with their own security efforts.

4. Under your leadership, how have these new and evolving threats shaped the NCTC's strategic operational planning? Please be specific.

NCTC continues to adapt its strategic operational planning efforts to account for an increasingly complex and diffuse range of threats and to position the US Government to operate effectively in challenging CT environments worldwide. In particular, NCTC's Directorate of Strategic Operational Planning, in alignment with the recently published 2018 National Strategy for Counterterrorism, is focused on developing national-level plans and strategies that integrate offensive, defensive, and preventative counterterrorism capabilities to protect the Homeland and US interests abroad by disrupting and eliminating terrorist networks, severing their sources of support, and preventing terrorist recruitment. This approach emphasizes the use of the full spectrum of CT instruments, recognizing that non-military capabilities are an increasingly important part of our CT toolkit. Our strategic plans, therefore, are not limited to military, intelligence, and law enforcement actions, but also address prevention efforts, strategic communications, diplomatic engagement, and the use of financial tools. In addition, NCTC's

strategic planning efforts acknowledge the increasingly important role of partners in our counterterrorism efforts, both in the US and abroad, and seek to expand our partnerships—including with private sector entities and civil society groups—to counter the evolving terrorist landscape. Finally, our planning efforts are addressing the need to keep pace with a rapidly changing technology environment by prioritizing the development of capabilities to enhance our ability to detect and disrupt new terrorist tactics, including in the online domain.

5. In your opinion, does NCTC have the tools needed to address these new and evolving threats? Please be specific.

Like the remainder of the IC, NCTC struggles to integrate both structured and unstructured data to perform better, more sophisticated, and faster threat analysis; moreover, compartmentalization and other data access restrictions pose challenges for analysts. Due to differences in data formats, cross-tool and cross-domain data exchanges remain a considerable challenge. Additionally, varying authorities and policies limit CT community collaboration. As an example, varying authorities for collection, retention, and dissemination of data, including US person data, require that IC agencies collect, retain, curate, analyze, and oversee duplicative data in order to meet their individual mission needs, rather than treating IC-collected data as an IC enterprise resource that is collected once for use by all. A second example is the lack of community tool development, which has forced agencies to develop their own solutions to meet individual mission needs. Consequently, data remain segmented by agency and mission, leading to duplication and no single, complete effort to improve the state of CT data integration. This has led to no single organization within the CT Enterprise having access to all of the lawfully collected information relevant to their analytic requirements. Creation of a more standardized authorities, policy, and oversight framework is needed to enable the treatment of data as an IC-enterprise resource thereby reducing duplication of effort throughout the data lifecycle—collection, retention, curation, analysis, and oversight.

**Post-Hearing Question for the Record
Submitted to Acting Director Russell Travers
From Senator Doug Jones**

**“Threats to the Homeland”
October 10, 2018**

Director Travers, in a speech on August 13, you listed several challenges for the NCTC in using data to address terrorism. One of those was a recognition that we are inundated with data, but that more data is not always better. As you explained, we need a sophisticated look at what kinds of data are valuable.

- 1. Do you have a plan to do that analysis and if so, can you please describe how you would go about that and what partners you would engage in determining what kinds of data are valuable?**

NCTC's assessment of data's value is driven by identifying threat actors, and then determining their intentions and activities. However, those actors continually try to thwart the Center's efforts by concealing their activities in an ever-evolving technological environment. Additionally, there is no one CT dataset, and as a result, NCTC must glean pertinent intelligence from a sea of irrelevant data. To accomplish this, NCTC's cadre of analysts, data scientists, and identity experts continually works across the Government at all levels, with our foreign partners, industry, and others to foster and maintain insight into what data is relevant to produce an amalgamation of different data that helps create the necessary intelligence picture. From a technical perspective, NCTC, in partnership with the Intelligence Community, continues to invest in artificial intelligence and machine learning solutions to help the Center pore through millions of different types of data to make non-obvious, but critical CT connections that would be impossible by manual review. From this standpoint, there is value in NCTC leading agencies involved in watchlisting and screening to evaluate, improve, and integrate business and IT processes to collect and share key biometrics and other data critical for identity discovery, watchlisting, and screening. It is worth noting that NCTC's data challenges are not unique to the CT mission but are equally applicable to the entirety of the IC.

08 March 2017

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

The Honorable Mark R. Warner
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Burr and Vice Chairman Warner:

Thank you for your letter of 03 March 2017 in which you provided additional questions related to my nomination to be the Director of National Intelligence. Attached, please find unclassified responses to your questions.

Sincerely,

//S//

Dan Coats

Enclosure

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

QUESTIONS FOR THE RECORD FROM SENATOR FEINSTEIN

Enhanced Interrogation Techniques

During his campaign, President-elect Trump publicly called for U.S. forces to use torture in the War on Terror. He said he would reinstitute waterboarding, which he called a minor form of torture, and bring back “a hell of a lot worse than waterboarding.” This brought tremendous condemnation from our allies and our own intelligence and security professionals who have declared that torture is largely ineffective at getting reliable intelligence. Additionally, yesterday you highlighted the fact that as a Senator, you voted against the 2015 National Defense Authorization Act that restricted all of the US government to only those interrogation procedures authorized by the Army Field Manual. You informed the Committee that the reason you voted against the NDAA was that you believed the Army Field Manual is not fast enough in a ticking time bomb scenario.

- 1. If you were ordered by the President to restart the Intelligence Community’s use of enhanced interrogation techniques that fall outside of the Army Field Manual, would you comply?**

I will absolutely follow the current law as it has been passed by the Congress and signed into law. Under the law, interrogation techniques are limited to those in the Army Field Manual.

- 2. Do you believe that enhanced interrogation techniques, which fall outside of the Army Field Manual, are more effective than approved techniques? If so, based on what?**

Current law limits approved interrogation techniques to those found in the Army Field Manual. I do not see it as the role of the DNI to recommend a reinterpretation of the law, or advocate for legislative changes to it, based on any personal beliefs.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

- 3. Do you plan to advocate for changes to the law based on your personal beliefs that enhanced interrogation techniques, which fall outside of the Army Field Manual, are more effective than lawful techniques approved by experts in the study of interrogations?**

If confirmed as the next Director of National Intelligence, I will be responsible for providing timely, objective, and integrated intelligence to the President and his senior advisors to best inform policy decisions.

In that role, I will absolutely follow the current law. I will also ensure that the Intelligence Community as a whole follows both the Constitution and laws of the United States, as I am required to do by the National Security Act. I do not see it as the role of the DNI to recommend a reinterpretation of the law, or advocate for legislative changes to it, based on any personal beliefs.

- 4. Would you support reinterpretation of current law (rather than a change in statutes) as justified in departing from the public Army Field Manual techniques?**

I do not see it as the role of the DNI to recommend a reinterpretation of the law, or advocate for legislative changes to it, based on any personal beliefs.

- 5. If you received a legal opinion saying that the Intelligence Community could legally use, or ask another country to use, enhanced interrogation techniques that fall outside the Army Field Manual on detainees, and the president ordered you to do so, would you comply?**

If confirmed as the next Director of National Intelligence, I will be responsible for providing timely, objective, and integrated intelligence to the President and his senior advisors to best inform policy decisions. In that role, I will absolutely follow the current law in this area as it has been passed by the Congress and signed into law. I will also ensure that the Intelligence Community as a whole follows both the Constitution and laws of the United States as I am required to do by the National Security Act.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

The current Secretary of Defense, Secretary of State, Secretary of Homeland Security, Attorney General, CIA Director, and Chairman of the Joint Chiefs of Staff have all said that waterboarding and other Enhanced Interrogation Techniques are unlawful and unnecessary. Attached is a letter written to the President from 176 generals and admirals urging him to reject waterboarding and other forms of detainee abuse. The letter, which includes 33 four-star retired generals and admirals, states:

"The use of waterboarding or any so-called 'enhanced interrogation techniques' is unlawful under domestic and international law."

"Torture is unnecessary. Based on our experience—and that of our nation's top interrogators, backed by the latest science—we know that lawful, rapport-based interrogation techniques are the most effective way to elicit actionable intelligence."

"Torture is also counterproductive because it undermines our national security. It increases the risks to our troops, hinders cooperation with allies, alienates populations whose support the United States needs in the struggle against terrorism, and provides a propaganda tool for extremists who wish to do us harm."

- 6. Do you agree that waterboarding and other enhanced interrogation techniques are not only unlawful but also inappropriate for the fight against terrorism?**

I believe the law is clear, interrogation techniques are limited to those in the Army Field Manual.

- 7. Will you commit to refraining from taking any steps to authorize or implement any plan that would bring back waterboarding or any other enhanced interrogation techniques?**

Waterboarding and certain other enhanced interrogation techniques are prohibited by law, and I will take no action that is contrary to the law.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

QUESTIONS FOR THE RECORD FROM SENATOR WYDEN

Surveillance

Section 702 of the Foreign Intelligence Surveillance Act prohibits “reverse targeting” of U.S. persons.

8. What policies do you believe are necessary to guard against reverse targeting?

As the question notes, reverse targeting is already prohibited by Section 702. I understand that training is provided on this prohibition, and that prevention of reverse targeting is an important area of focus for the government personnel who implement this program and who review compliance.

If confirmed, I plan to review how Section 702 is being implemented to determine whether any changes should be made to further strengthen compliance and oversight, including with respect to the reverse targeting prohibition.

Section IV (“Processing Raw SIGINT”), paragraph (C)(2) of the Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency Under Section 2.3 of Executive Order 12333 states that, when raw signals intelligence is shared with IC elements, queries for communications reasonably likely to be to, from, or about a U.S. person or a person located in the United States may be conducted for purposes of targeting that person if the Attorney General determines that the person is an agent of a foreign power or an officer or employee of a foreign power and the purpose of the selection is to acquire significant foreign intelligence or counterintelligence information.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

- 9. Are there situations where IC elements can conduct queries for communications reasonably likely to be to, from, or about a U.S. person or person located in the United States for purposes *other* than targeting that person *without* an Attorney General finding that the person is an agent of a foreign power or an officer or employee of a foreign power?**

In the interests of transparency, the ODNI redacted and released a public version of the procedures, and also released a corresponding Fact Sheet. As they indicate, an IC element that receives access to raw SIGINT under these procedures may use a selection term based on the fact that the communications mention a particular person, but the element may only use a selection term associated with a U.S. person or person in the United States if: (1) the element's legal and compliance officials confirm that the selection term is associated with a U.S. person who is a current FISA target; or (2) if the selection is approved by the Attorney General, or in certain limited cases, is approved by the Director of the NSA or the head of the recipient element (or a high-level designee). It is my understanding that the committee has received the classified and unredacted version of the procedures, which describes those limited cases.

- 10. What do you see as the distinctions between queries for communications likely to be to, from, or about a U.S. person or a person located in the United States with regard to Executive Order 12333 raw signals intelligence and collection under Section 702 of FISA?**

I understand that there is a difference in the legal standard for conducting those queries. For raw SIGINT under EO 12333, the standard is set forth in Section IV of the Raw SIGINT Availability Procedures, as described in the response to Question 9. For queries under Section 702, the standard is set forth in the minimization procedures, the 2015 versions of which have been redacted and publicly released. In both cases, it is important for such queries to be conducted carefully, for authorized purposes, and in full compliance with applicable legal requirements.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

- 11. If a foreign entity offers to the Intelligence Community communications that are known to include the communications of Americans who are not suspected of anything, how should those communications be handled?**

Information about Americans – including information provided by a foreign entity – must be handled with great care, in full compliance with applicable legal requirements, including those contained in Attorney General-approved procedures under Executive Order 12333. In no event should the Intelligence Community request that a foreign entity undertake activities that the Intelligence Community is itself forbidden from undertaken.

- 12. Are there cases in which the sheer number of innocent Americans' communications involved, or in which the Americans' communications are particularly politically sensitive (for example, they include those of American politicians, political activists, or journalists), that there should be limitations on what the Intelligence Community can collect, use or retain?**

My understanding is that any IC element collecting information must do so only in accordance with EO 12333 and with specific procedures required by EO 12333 that are issued by the head of the element, in consultation with the DNI, and approved by the Attorney General. Similarly, the receiving IC element would handle the collected information in accordance with the same Attorney General-approved procedures. My understanding is that certain of those Attorney General-approved procedures include specific parameters that apply to sensitive information concerning U.S. persons, among other things.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

In your response to pre-hearing questions, you wrote that “If a foreign partner lawfully collects and shares information relating to a U.S. person, that information would be subject to the Attorney General approved guidelines discussed in response to question 6.”

13. Please explain what “lawfully collects and shares” means in this context. What would constitute an unlawful collection or sharing of information by a foreign partner?

Under FISA, if the IC is interested in targeting a specific U.S. person, it must obtain a court order that meets all the applicable requirements of FISA. It would be unlawful for the IC to circumvent the law and request that a foreign partner intercept those communications on the IC’s behalf, and to then provide those communications back to the IC.

Lethal Operations

14. Please describe your view of the legal and policy implications of targeting or otherwise knowingly killing a U.S. person in a U.S. Government lethal operation. What additional public transparency do you believe would be warranted in that situation?

The 2001 AUMF provides a domestic legal framework for targeting enemy forces in the context of hostilities and legal principles have long held U.S. persons that are part of an enemy force are not immunized from becoming targets of lethal operations. However, prior to targeting a U.S. person, I understand that DOJ conducts a rigorous review to ensure that lethal action may be conducted against that individual consistent with the Constitution and laws of the United States. The role of the DNI is to ensure the IC provides accurate and relevant information to assist DOJ and our operational decision-makers in the process. If confirmed, I will work with the relevant department and agency heads to assess whether additional transparency is warranted in these situations.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

The Obama Administration made a distinction between lethal strikes that are carried out in places it considers part of “areas of active hostilities,” and those that take place outside those areas.

- 15. Do you support this distinction as well as the application of the standards, requirements, and guidelines contained in the Presidential Policy Guidance (PPG)? If not, please describe any modifications you would suggest.**

At the beginning of every new Administration, it is not unusual for officials to review existing presidential policy guidance in the interest of determining whether in their present form they still address national priorities or deserve to be revisited. The most important policy objective of this office is to ensure the IC continues to provide accurate and relevant information to our operational decision-makers. If confirmed, I look forward to working with my inter-agency colleagues to ensure the intelligence informing any direct action activity consistent with American values and comport to the Law of Armed Conflict.

- 16. Do you support Executive Order 13732, which includes public reporting on “combatant” and “non-combatant” casualties for strikes that take place outside of areas of active hostilities; a commitment to review or investigate incidents involving civilian casualties and to consider information from non-governmental organizations in that review; and a commitment to provide as appropriate ex gratia payments to civilians who are injured or to the families of civilians who are killed in U.S. strikes? If not, please describe any modifications you would suggest.**

Earlier this year, the National Security Council directed ODNI, in accordance with EO 13732, to release a summary of information provided to the DNI by other agencies about both the number of strikes taken in 2016 by the U.S. Government against terrorist targets outside areas of active hostilities and the assessed number of combatant and non-combatant deaths resulting from those strikes.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

As noted in response to earlier questions, at the beginning of every new Administration, it is not unusual for officials to review existing presidential policy guidance in the interest of determining whether in their present form they still address national priorities or deserve to be revisited.

I do not yet have a view on whether changes to this Executive Order are needed. In any event, ODNI will continue to comply with EO 13732 consistent with IC practices.

Additionally, the IC does not play a role in determining the status of ex-gratia payments.

On December 2, 2015, now-President Trump stated the following: "The other thing with the terrorists is you have to take out their families, when you get these terrorists, you have to take out their families. They care about their lives, don't kid yourself. When they say they don't care about their lives, you have to take out their families."

17. Do you agree that this would be a violation of international law?

The United States goes to great lengths to adhere to its international law obligations in the execution of armed conflicts. The Law of Armed Conflict prohibits intentional attacks against civilians, unless they are directly participating in hostilities. Outside armed conflict, it may be appropriate to leverage law enforcement authorities to question, detain, or prosecute those that support terrorists, to include their family members.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

Interrogation and Detention

In pre-hearing questions, you were asked about your current position with regard to the 2015 legislation that: (1) prohibited interrogation techniques not authorized by the Army Field Manual; (2) prohibited revisions to the Army Field Manual that involved the use or threat of force; (3) required that the Army Field Manual be public; and (4) required ICRC notification of and prompt access to detainees. You responded that "Current law dictates that the Army Field Manual be the standard for conducting interrogations, and if confirmed, I will ensure that the IC complies with the law."

18. Are you fully supportive all four aspects of the 2015 legislation listed above?

If confirmed, I would comply and would ensure the IC complies with all aspects of current law.

During the hearing, you stated that you opposed the 2015 legislation because:

"I thought perhaps we ought to at least have a discussion about, what do you do in a situation when you have the necessary intelligence to know that something terrible is going to happen to the American people in a very short amount of time and you have a legitimate individual who can tell you where that radiological bomb or biological material is, and you don't have time to go through the process that the Army field manual requires."

You stated that you will ensure that the Intelligence Community follows the law and that you do not intend to advocate for any changes. You further stated, however, that:

"But I do think that it's at least worth discussion relative to the situation that might occur, where we might have to -- hopefully with some special authority -- might have to go outside that."

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

19. Are you aware of any situation similar to the one you described above in which coercive interrogation techniques thwarted an imminent terrorist attack against the American people?

In responding to the SSCI study on the interrogation program, former CIA Director Brennan stated in December 2014, "Our review indicates that interrogations of detainees on whom EITs were used did produce intelligence that helped thwart attack plans, capture terrorists, and save lives. The intelligence gained from the program was critical to our understanding of al-Qa'ida and continues to inform our counterterrorism efforts to this day." I have no reason to dispute the conclusions of Director Brennan.

Attorney General Sessions has committed to ensuring that he and other appropriate officials are fully briefed on the Committee's torture report, to the extent it is pertinent to the Department of Justice. CIA Director Pompeo committed to reviewing parts of the report relevant to his position and the Committee.

20. Will you make the same commitment on the part of the ODNI?

As a former member of this body, I have already been briefed on the Committee's Study of the Central Intelligence Agency's Detention and Interrogation Program.

Inspectors General

In your responses to pre-hearing questions, you wrote, in the context of the CIA's Detention and Interrogation Program, "Lacking a reasonable suspicion of fraud, waste, abuse or violation of law, rule or regulation, I am not aware of any affirmative responsibility the [CIA] had to proactively involve their IG in each on-going operation."

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

- 21. If confirmed, would you encourage IC entities to inform their Inspectors General when initiating programs that pose significant new legal questions or that, by their nature, could raise new concerns about fraud, waste, abuse or violations of law, rule, or regulation?**

I believe it is the responsibility of an agency's leadership, including its legal counsel, to develop programs in a legally compliant manner that avoid potential fraud, waste, abuse, and violations of law, rule, and regulations.

If confirmed, I will encourage IC leadership to maintain proactive relationships with their Inspectors General to ensure that allegations of fraud, waste, abuse, or violations of law, rule, or regulation are quickly investigated and addressed.

Privacy and Civil Liberties Oversight Board

In your responses to pre-hearing questions, you wrote that, if confirmed, you would ensure that the Intelligence Community supports the Privacy and Civil Liberties Oversight Board in fulfilling its statutorily mandated role. In order to do that, the PCLOB needs members.

- 22. Will you advocate for the quick nomination of PCLOB members?**

I support the timely nomination of the PCLOB Members so they can provide advice on new counterterrorism policies and conduct their statutory oversight responsibilities.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

Oversight of the CIA

In your responses to pre-hearing questions, you confirmed that the DNI's statutory role includes overseeing the CIA's coordination of foreign intelligence relationships.

- 23. When the CIA decides to establish or continue a relationship with a foreign partner against which there are allegations of human rights abuses, what role should the DNI play in the oversight of that relationship?**

Current law provides that the DNI shall oversee the coordination of foreign liaison relationships, to include those conducted by the CIA. The CIA plays a vital role for the U.S. Government by managing and developing relationships with foreign liaison services, which have served as force multipliers in a broad range of endeavors, especially counterterrorism. In executing its responsibilities, the CIA has developed policies and procedures, coordinated with ODNI, on handling relationships with foreign liaison services who are alleged to have participated in human rights violations. These procedures include requirements for documenting, assessing, and reporting allegations of human rights violations. When those allegations are deemed credible, there is an established process for reviewing a relationship, making informed decisions to suspend or terminate information flows as appropriate, and keeping the congressional intelligence committees fully informed.

- 24. If a U.S. ambassador directs the CIA to cease a particular operation, is the CIA obligated to do so, absent intervention from the president?**

With few exceptions, Chiefs of Mission (COM) are responsible for the conduct of all Executive Branch personnel within their area of responsibility. If there is a disagreement between a COM and any department or agency under his or her authority, there are long-standing procedures to handle such disputes.

Declassification

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

Executive Order 13526 (December 29, 2009) provides that: "In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of national security." Executive Order 13292 (March 25, 2003) and Executive Order 12958 (April 17, 1995) prohibited classification based on the same factors.

25. Do you agree with the prohibitions in these Executive Orders?

Yes, I fully agree with the restrictions placed on classification of information for inappropriate reasons as laid out in the Executive Orders you cite. If confirmed, I will ensure the Intelligence Community continues to use classification only to protect information of appropriate national security concern during my tenure.

I have conveyed to you through classified channels four matters that I believe should be declassified and released to the public.

26. Do you commit to working with me in an effort to have those matters declassified?

If confirmed, I will consult with the relevant IC element heads to assess the extent to which these matters can be redacted and publicly released in a manner consistent with the need to protect classified information and other sensitive intelligence sources and methods.

Russia

27. Please disclose any meetings or conversations you have had with Russian government officials in 2016 or 2017.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

To the best of my recollection, and after reviewing my schedule, I have not had any meetings or conversations with Russian government officials in 2016 or 2017; since 2014 I have been prohibited from entering Russia by the Russian government because of my outspoken opposition to their annexation of Crimea.

QUESTIONS FOR THE RECORD FROM SENATOR COLLINS

Cyber

Senator Coats, in your statement for the record, you start with the vulnerabilities that exist in cyberspace. The danger posed to our critical infrastructure from cyber-attacks of our foreign adversaries is demonstrated most clearly by the attacks that have already taken place in the past few years:

- a significant portion of Ukraine's power grid was taken down by Russian-backed actors in 2015;
- Iranian-backed actors sought to deny online access to U.S. financial systems from 2011-2013; and
- more than 35,000 computers associated with Saudi Arabia's oil and gas sector were rendered worthless after malware destroyed data on those computers.

That is why I am grateful for your support and co-sponsorship of Section 312 of the Fiscal Year 2017 Intelligence Authorization Act. This provision would ensure that the unique expertise in the intelligence community is made available to help the most significant critical infrastructure entities in our country protect themselves from cyber threats. Our provision was adopted unanimously by the Committee, but the overall bill awaits consideration on the Senate floor, which means the Administration's anticipated Executive Order on cybersecurity could be implemented first.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

- 28. Do you continue to support the provision in our bill, and if the new Executive Order is issued before our bill passes, will you advocate for bringing to bear the unique capabilities of the Intelligence Community to assist the Section 9 entities in improving their defensive posture against nation-state level attacks as the new Executive Order is implemented?**

As I noted before the Committee, I believe that cyber threats are a principal threat to the United States including potential threats to critical infrastructure. I am aware that through DHS, various elements of the IC currently provide critical infrastructure owners and operators with intelligence products and analysis. If confirmed, I will work closely with DHS, the FBI, and the entire IC to work to provide information to Section 9 entities while protecting sensitive sources and methods.

Russia

In your statement for the record, you express your great concern regarding Russia's assertiveness in global affairs. 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.

- 29. Do you believe we have shared interests with Russia in the Middle East, and in Syria in particular?**

Russia's increasing assertiveness in the foreign policy realm is a concern, but there are some areas of potential bilateral cooperation. Russia has long looked to establish an international counterterrorism coalition against ISIS, and has called for stability in the Middle East as the first step toward fighting terrorism in the region, though the US and Russia may not share a common definition of terrorism. Furthermore, Russia has also worked with the Syrian Regime and pro-Regime forces to conduct devastating attacks against the Syrian Opposition and

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

civilian populations and has repeatedly failed to convince the Regime to maintain ceasefires. In Iraq, Russia has sought to expand cooperation with Baghdad against ISIS, increase arms sales, and broaden diplomatic and economic ties. In Egypt and Libya, Russia is looking to expand diplomatic and economic ties and cooperate on counterterrorism initiatives. In Iran, Russia participated in the negotiations on the JCPOA nuclear deal and has publicly committed to ensuring Iranian compliance to the deal. Moscow also appears to be interested in serving as a facilitator to a revived Middle East Peace Process. However, in all of these cases, although Moscow appears interested in improved cooperation with Washington, it will seek outcomes that align with its own interests.

QUESTION FOR THE RECORD FROM SENATORS KING AND HEINRICH

Vulnerabilities Equities Process

As you know, the Vulnerabilities Equities Process (VEP) is the primary process for deciding whether a government entity must disclose to private companies information about security vulnerabilities in their products, or whether the government may withhold the information for law enforcement or intelligence purposes.

In April 2014, the Office of the Director of National Intelligence reported that the White House had “reinvigorated an interagency process for deciding when to share vulnerabilities” through the VEP. Later that month, President Barack Obama’s Cybersecurity Coordinator Michael Daniel wrote that the administration has “established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure.” And in October, Senators Heinrich and King wrote a letter asking the administration to establish enduring policies governing the VEP process; including the issuance of standard criteria for reporting vulnerabilities, setting forth guidelines for making determinations, delineating clear time limits for each stage of the process, ensuring adequate participation of all relevant government agencies, and mandating regular reporting to Congress.

**QUESTIONS FOR THE RECORD
FORMER SENATOR DANIEL R. COATS**

30. As Director of National Intelligence, will you be willing to continue the VEP, formalize its processes, and increase transparency into the VEP?

The Vulnerability Equities Process (VEP), as it currently operates, is led and overseen by the National Security Council through the VEP Executive Review Board. The National Security Agency serves as the Executive Secretary for the overall process ensuring the vulnerability notifications received from the departments and agencies are communicated, coordinated, and disseminated in a timely manner. The Executive Secretary also provides the administrative functions for the VEP ensuring consistency in the process and maintenance of appropriate documentation. The VEP has specific formats required for all participants, time requirements, and processes that require departments and agencies to identify equity and concerns. The departments and agencies also provide subject matter expertise to discuss the impacts and concerns of the zero-day vulnerabilities, and provide recommendations for the NSC Executive Review Board decisions. The ODNI contributes to the process as a member of the Executive Review Board, and at the subject matter expert working level.

If confirmed, I will review the VEP to best understand its effectiveness and consider requests, with my interagency partners, to process adjustments.

**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

Question: 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

Question: 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.

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 already 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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
United States House of Representatives
Washington, DC 20510

MAR 28 2018

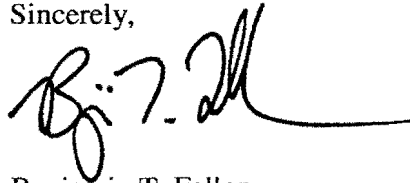
The Honorable Bennie Thompson
Ranking Member
Committee on Homeland Security
United States House of Representatives
Washington, DC 20510

Dear Chairman McCaul and Ranking Member Thompson:

The enclosed documents responds to Questions for the Record following the "World Wide Threats: Keeping America Secure in the New Age of Terror," open hearing on 30 November 2017.

If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,

A handwritten signature in black ink, appearing to read "B. T. Fallon", with a long horizontal flourish extending to the right.

Benjamin T. Fallon
Acting Director of Legislative Affairs

Enclosure:
Responses to "Questions for the Record" from the 30 November 2017 Hearing before the
Committee on Homeland Security

Hearing Date:	30 November 2017
Committee:	House Committee on Homeland Security Governmental Affairs
Member:	Rep. Scott Perry
Witness:	D/NCTC Rasmussen
Info Current as of:	20 March 2018

Question 1: What do you consider to be the most critical threat to US national security today?

Answer:

Within the counterterrorism mission space, the National Counterterrorism Center believes that the most immediate terrorist threat to the Homeland is the threat of violence carried out by Homegrown Violent Extremists (HVEs)—a threat we expect will persist through the next year.