

**UNCLASSIFIED RESPONSES TO QUESTIONS FOR THE RECORD
SENATE SELECT COMMITTEE ON INTELLIGENCE
HEARING JANUARY 29, 2019
DIRECTOR OF NATIONAL INTELLIGENCE DANIEL COATS**

Hearing Date: January 29, 2019
Committee: SSCI
Member: Sen. Wyden
Witnesses: DNI Coats
Info Current as of: March 21, 2019

Question: In its decision in *Carpenter v. United States*, the U.S. Supreme Court found that the collection of cell-site location information (CSLI) from wireless providers constituted a search under the Fourth Amendment.

- Have the ODNI or any elements of the Intelligence Community issued any guidance regarding how the *Carpenter* decision should be interpreted and/or applied to intelligence programs and operations?
- If so, please provide any relevant memoranda or guidance.

Answer:

Although the *Carpenter* opinion “does not consider other collection techniques involving foreign affairs or national security”¹ the Intelligence Community, as always, carefully considers all Supreme Court precedent, including *Carpenter*, when evaluating how and whether the Fourth Amendment applies to a proposed intelligence activity. The Intelligence Community will continue to assess the potential implications of the *Carpenter* decision and will, in the event a circumstance arises that might implicate the holding of the decision, provide appropriate guidance to the Intelligence Community agencies at that time. That said, the ODNI has not issued any controlling written Intelligence Community-wide guidance regarding how the *Carpenter* decision should be interpreted or applied.

¹ *Carpenter v. United States*, 585 U.S., at ___, 134 S. Ct. 2206, at 2220 (June 22, 2018).

Hearing Date: January 29, 2019
Committee: SSCI
Member: Sen. Wyden
Witnesses: DNI Coats
Info Current as of: March 21, 2019

Question: Does the Intelligence Community agree with Mr. Evanina's recommendation that encryption be used to protect U.S. government officials' work and personal unclassified telephone communications?

- **If yes, what steps, if any, has the Intelligence Community taken to communicate this recommendation to agencies and to government officials?**

Answer:

The National Cyber Strategy, signed by the President on September 17, 2018, states that responsibility to secure federal networks, including federal information systems and national security systems, falls squarely on the Federal Government. National Security Directive 42 expands the responsibilities for protecting national security information systems to also include national security telecommunications systems. The Intelligence Community has distributed these documents to all federal agencies and has made continued access available through appropriate websites. Thus, encryption should be used to protect U.S. Government officials' work and associated federal information. Although personal unclassified telephone communications do not fall under the category of official government work and are not required to be afforded such protection, Director Evanina has consistently advocated for strong cyber hygiene practices through the Know the Risk – Raise Your Shield campaign. Through this campaign, Director Evanina has issued tips and guidance to the public on how to protect personal information from being exploited by cyber criminals and foreign intelligence services.

Hearing Date: January 29, 2019
Committee: SSCI
Member: Sen. Heinrich
Witnesses: DNI Coats
Info Current as of: March 21, 2019

Question: As the government's Security Executive Agent, have you reviewed the Executive Office of the President's process for granting access to classified information for compliance with Executive Order 12968?

- **If so, is the Executive Office of the President compliant?**

Answer:

Congress has sent several letters seeking information on the security clearance process. To ensure a complete response to all of these questions, responses to this question will be included under separate cover.

Hearing Date: January 29, 2019
Committee: SSCI
Member: Sen. Heinrich
Witnesses: DNI Coats
Info Current as of: March 21, 2019

Question: How often do you conduct such compliance reviews, and when was the last review?

Answer:

Congress has sent several letters seeking information on the security clearance process. To ensure a complete response to all of these questions, responses to this question will be included under separate cover.