CAROLYN B. MALONEY
CHAIRWOMAN

ONE HUNDRED SIXTEENTH CONGRESS

JAMES COMER
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

August 7, 2020

Mr. Jamil N. Jaffer
Founder & Executive Director, National Security Institute
George Mason University
3301 Fairfax Drive
Arlington, VA 22201

Dear Mr. Jaffer:

Enclosed are post-hearing questions that have been directed to you and submitted for the official record for the hearing on Wednesday, July 15, 2020, titled "U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act."

Please return your written responses to these questions by Thursday, August 20, 2020, including each question in full as well as the name of the Member. Your response should be addressed to the Committee office at 2157 Rayburn House Office Building, Washington, D.C. 20515. Please also send an electronic version of your response by email to Amy Stratton, Deputy Chief Clerk at amy.stratton@mail.house.gov.

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Elisa LaNier, Chief Clerk, at (202) 225-5051.

Sincerely,

Carolyn B. Maloney
Chairwoman

Enclosure

cc: The Honorable James R. Comer, Ranking Member

Questions for Mr. Jamil N. Jaffer
Founder & Executive Director, National Security Institute
George Mason University
Questions from Chairwoman Carolyn B. Maloney

July 15, 2020, Hearing: "U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act."

---

1. In your opinion, what are the greatest cybersecurity threats posed by our State and non-State adversaries today, and what changes are needed at the federal level to better prepare America to confront those threats?

2. H.R. 7331 would enable the National Cyber Director to engage internationally on cybersecurity coordination, specifically by participating in international meetings or conferences on cybersecurity.

    a. What agencies, departments, and officials currently represent the U.S. at such events?

    b. Do you think sending a National Cyber Director to these events on behalf of the United States would be more effective at conveying a cohesive, whole-of-government approach to cybersecurity to our allies and partners?

3. Do you think establishing a National Cyber Director would signal the seriousness with which we confront the cyber threat to our allies and partners, as well as our adversaries?

4. Are there any benefits to our national security to **not** having a statutorily empowered central authority coordinating our nation's whole-of-government cybersecurity operations in the Executive Office of the President?

5. In the hearing, you stated:

    "…Today in our country, we expect [large companies and small businesses alike] to defend themselves against nation-states like Russia, China, Iran, [and] North Korea that have virtually unlimited human and monetary resources to throw at this problem. It's an unwinnable battle. We've got to get those companies to come together with one another to create a collective defense structure with multiple industries working with one another, and the Government, frankly, takes all this intelligence it collects and provides it back to industry in an actual form to help them defend themselves. If we're going to put them on the front lines, we owe them better, and we're not doing that right now."

a. Can you provide additional detail on this idea? Should this "collective defense structure" be set up by the federal government, and if so, what form should it take?

b. How should existing federal agencies fit into this structure, and what new authorities or entities are needed to make it successful?

c. Should this be included in the National Cyber Strategy required by H.R. 7331?

QUESTIONS FOR THE RECORD

On behalf of Ranking Member James Comer (R-KY)

Committee on Oversight & Reform

"U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act"

Hearing took place on Wednesday, July 15, 2020, remotely via Webex

---

Questions for Mr. Jamil Jaffer:

1. Is a Homeland Security Advisor in the White House, tasked by Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, with reporting to the President directly on an assessment of cyber readiness, capable of operating as the primary voice to the President on cybersecurity matters?
    a. Could a president restructure this position to do what is envisioned by an NCD?
    b. What authorities would the Cyber Director have over intelligence community and Defense Department led offensive and incident response activities? Would the NCD office be a peer coordinating entity or would it have any actual ability to influence the activities of the nation's intelligence and defense functions?

2. The National Security Council (NSC) has traditionally operated as the hub for coordinating the nation's cybersecurity response. Should Congress instead be supporting the NSC in this mission rather than splintering the authorities of the NSC yet again, following removal of various mission areas like drug coordination and trade coordination from its ambit?

3. President Trump recently signed an executive order declaring foreign threats to the nation's energy infrastructure a national emergency. Under the executive order, the Secretary of Energy will lead a task force to ensure that power systems are protected against foreign intrusion and attack. The Secretary of Defense, Secretary of Homeland Security and the Director of National Intelligence will also be members of the task force.
    a. Is this task force model potentially a better way of dealing with sector-specific cyber threats rather than a specified individual who is expected to handle such a diverse range of cyber threats?
    b. What other federal agencies would need a seat at such a task force and why?

4. The Foreign Intelligence Surveillance Act (FISA) authorizes DOJ to seek orders to surveil individuals acting as agents of foreign powers.
    a. Is FISA a tool for investigating foreign cyber intrusions?
    b. Are there gaps in FISA which, if filled, would assist investigators and prosecutors in combatting foreign cyber-attacks?

5. Why shouldn't we take more time to study this matter and further evaluate the need for creation of a new office, something the Senate companion legislation ponders?