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

Ms. Suzanne Spaulding
Commissioner, U.S. Cyberspace Solarium Commission
Senior Adviser, Homeland Security
International Security Program
Center for Strategic & International Studies
1616 Rhode Island Avenue, N.W.
Washington, D.C. 20036

Dear Ms. Spaulding:

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 Ms. Suzanne Spaulding
Commissioner, U.S. Cyberspace Solarium Commission
Senior Adviser on Homeland Security, Center for Strategic & International Studies

Questions from Chairwoman Carolyn B. Maloney

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

---

1. Does the United States' risk for sustaining a major cyber incident increase when the country experiences other national crises like the coronavirus pandemic? How would having a National Cyber Director help to control the risk and decrease the likelihood that one national crisis leads to another?

2. What harm did the elimination of the Cybersecurity Coordinator role by then-National Security Advisor John Bolton do to our nation's cybersecurity readiness?

3. Would the size and placement of the Office of the National Cyber Director within the Executive Office of the President add a layer of bureaucracy, or would it enable the Director to reduce redundancies to make our cyber response more effective?

4. How would consolidating leadership for U.S. cybersecurity policy in a National Cyber Director provide greater direction for agencies as they implement the National Cybersecurity Strategy?

5. How would the National Cyber Director's proximity to the President, and connection to each Federal cybersecurity player, make a difference in our overall ability to manage cyber risks?

6. Your testimony mentions that variability between different Administrations' approaches to cybersecurity leadership has "prevented the persistence and consistency needed to establish enduring policy and strategy."

    a. Do you think creating the National Cyber Director position outlined in H.R. 7331 would help set the long-term vision needed for lasting progress on national policy goals?

    b. Thinking several decades into the future, how could America's relationship with China and the rest of the world be altered by the establishment of a National Cyber Director?

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 Ms. Suzanne Spaulding:

1. Do our foreign allies have officials comparable to a National Cyber Director? If so, did the Commission study any of these foreign models?

2. In the "layered approach" to cybersecurity, one of the goals articulated by the Commission is to "deny benefits" to cyber enemies by securing "critical networks."
    a. Did the Commission take a view on the potential use of Huawei and ZTE products in U.S. networks or networks operated by our allies like the U.K.? Should these companies' products be banned due to the risk posed by China?
    b. What infrastructure networks in our country are most at risk and what entities own and operate these entities? Water, electric, healthcare, banking and financial services, transportation, etc.?
    c. In terms of our energy networks, some often cite cyber risk for choosing not to build new nuclear plants. Has a country like France, which operates a significant nuclear infrastructure, faced significant cyber-attacks on its nuclear plants? Did the Commission study cyber risk to potential alternative energy sources?

3. It is often said that the security of networks is only as safe as the conduct of individuals on those networks. Phishing scams continue to be a primary vector of attack. Did the Solarium Commission study this weakness? Any recommendations?

4. The Commission said that we must "impose costs" on our adversaries who choose to attack us through cyber means. U.S. Cyber Command is organized to go on the offense. Other entities in the Intelligence Community (IC) also have that power.
    a. Could you describe the instances where you would recommend Cyber Command responding in retaliation with offensive measures?
    b. Imposing costs seems to be a concept that could cause reciprocation. What are the risks?
    c. Is the intelligence community properly organized to impose costs on adversaries for cyber-attacks?
    d. Does the intelligence community need any further authorities in order to implement a strategy of imposing costs for malevolent activity by our adversaries?
    e. 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?

5. Through the Commission's recommended policy of "shaping behavior" - enforcing norms of responsible cyber behavior – how do diplomacy, sanctions, and even indictments deter malicious actors?
    a. Have you seen evidence of the success of these actions in deterring malicious behavior?