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. Amit Yoran
Chairman and Chief Executive Officer
Tenable
7021 Columbia Gateway Drive, Suite 500
Columbia, MD 21046

Dear Mr. Yoran:

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. Amit Yoran
Chairman and Chief Executive Officer, Tenable

Questions from Chairwoman Carolyn B. Maloney

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

---

1. On March 16, a cyberattack reportedly targeted the computer systems of the Department of Health and Human Services in an unsuccessful attempt to disrupt the Department's response to the pandemic. By the end of March, every country in the world had seen at least one attack in connection to the coronavirus pandemic. Do you think America's role in the international coordination and response to these threats would have benefitted from a National Cyber Director?

2. You speak in your written testimony about how essential Chief Information Security Officers (or similar positions) are to company leadership. Would establishment of a National Cyber Director through H.R. 7331 implement the best practices of the private sector to improve the functioning of the federal government? Why or why not?

3. H.R. 7331 requires the Office of the National Cyber Director to consult with private sector stakeholders on developing relevant operational or response plans to substantial cyberattacks, on emerging technologies, and on cybersecurity issues more generally. How would the National Cyber Strategy and federal cybersecurity posture be improved through consultation with the private sector as required in H.R. 7331?

4. Your written testimony and our dialogue during the hearing addressed the lack of diversity in the cybersecurity sector and how it contributes to the overall shortage of talent in the cybersecurity workforce, indicating that "the nation needs a bold, new cyber workforce strategy that develops and advances the ranks of people from all walks of life." For example, you point out that minorities make up 26% of the U.S. cybersecurity workforce, and that women make up just 14% of the cybersecurity workforce in North America.

    a. Can you provide additional detail on what this strategy should include?

    b. Do you believe such an effort would advance innovation and give the U.S. a competitive edge globally?

    c. Do you think such a strategy should be included in the National Cyber Strategy?

5. Do you think that most Americans are aware of the cyberthreat exposure they face daily, and how would H.R. 7331 reduce this exposure? What are the potential risks to Americans if commonly used apps, sites, and devices lack the infrastructure or ability to keep up with evolving cyberthreats, and how are those risks compounded if we fail to establish a centralized federal response?

6. You mentioned that "a modest amount of funding, coordination, and policy directed from the federal government [to state and local governments] could have a disproportionately huge impact on better protecting the nation" from cyberthreats." How would you design such a program?

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. Amit Yoran:

1. "Hack back" legislation has been proposed in Congress. Private industry would be offered the authority to respond in kind if a company becomes the target of a cyber-attack. Do you support such legislation?

2. Could you please describe a hypothetical situation that sufficiently characterizes the cyber threats posed to industrial control systems security and how those threats can be remediated?

3. If you had the power to immediately require the U.S. government to focus in on one specific component of cybersecurity, what would it be?