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. J. Michael Daniel
President and Chief Executive Officer
Cyber Threat Alliance
1001 19th Street North, Suite 1200
Arlington, VA 22209

Dear Mr. Daniel:

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. J. Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance
Questions from Chairwoman Carolyn B. Maloney

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

---

1. The cyber breach of Office of Personnel Management records in 2013 by Chinese hackers resulted in the theft of the private data of more than 21 million federal workers. If H.R. 7331 had been fully implemented prior to the breach, how might the incident have been handled differently?

2. In 2017, Chinese military-backed hackers breached the systems of the credit reporting agency Equifax, compromising the sensitive data of 145 million Americans. A 2018 report released by former Oversight Committee Chairman Elijah Cummings outlined four reforms to help prevent future cyberattacks, including holding federal financial regulatory agencies accountable for their oversight responsibilities, requiring that federal contractors comply with established cybersecurity standards, and setting clear standards for how data breach victims should be notified.

    a. Has been done at the federal level to prevent future attacks like the Equifax hack?

    b. Is a National Cyber Director needed to ensure that the former Chairman's recommendations are implemented in a coordinated, whole-of-government manner?

3. Describe the cybersecurity responsibilities currently spread across federal departments and agencies.

    a. Does stove-piping across the various agencies create unintentional gaps and vulnerabilities?

    b. Is it possible to estimate the cost savings to the federal budget of a centralized coordinating authority in the Executive Office of the President tasked with streamlining these responsibilities and eliminating these gaps?

    c. In detail, how could they be better streamlined by a National Cyber Director, and what specificity is needed in the legislation to ensure both new and existing roles and responsibilities are clearly defined?

4. The Office of Management and Budget (OMB) currently requires agencies to coordinate their cybersecurity requirements and assessments, but enforcement remains a challenge. A report released in May 2020 by the Government Accountability Office, titled "Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States," identified the disparate cybersecurity requirements of various federal agencies that states are required to follow when using federal data. According to the report, variances in the cybersecurity requirements of federal agencies most often increased costs to states moderately, greatly, or very greatly. Among the four federal agencies examined, between 49% and 79% of their cybersecurity requirements were actually in conflict.

    a. How would a National Cyber Director improve the effectiveness and efficiency of the federal government's partnerships with state, local, and Tribal governments?

    b. Are these difficulties mirrored in the private sector for companies that need to work across multiple federal agencies or departments?

    c. Given the potential cost savings associated with reducing regulatory incompatibilities and redundancies for public and private sector partners, in addition to those associated with reductions in costly cyberattacks and IP theft, is it reasonable to expect that an Office of the National Cyber Director could more than pay for itself?

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. Michael Daniel:

1. The National Cyber Investigative Joint Task Force (NCIJTF) was officially established in 2008. It describes its coordination function on its website: "As a unique multi-agency cyber center, the NCIJTF has the primary responsibility to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation."
    a. In your time with the Obama Administration, was the NCIJTF failing, and if not, why wouldn't we choose to support its coordination functions across the entire government and with foreign partners?
    b. Would the NCIJTF be subsumed into an office of the National Cyber Director?
    c. How would a National Cyber Director oversee the NCIJTF?

2. Under the current legislative construct, will the new NCD office and official have authority over departments and agencies in conducting cybersecurity policy, planning, and operations?

a. What teeth would the new office have to enforce its mandates or directives?
b. Would the National Cyber Director become the sole voice providing all cyber-related insight to the president? And vice-versa, why couldn't a president choose to obtain advice directly from Department Secretaries rather than the NCD?
c. Because the NCD would be a Senate-confirmed official, is there any requirement for a president to nominate someone even if the president is not interested in filling the position?
d. 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?

3. Are we aware whether the concepts and processes in Presidential Policy Directive-41 for coordinating federal cyber response were ever triggered?
    a. Has there been a federal, government-wide response to a real cyber-attack where coordination was tested?
    b. If so, what were the results?