CAROLYN B. MALONEY
CHAIRWOMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
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
http://oversight.house.gov

MEMORANDUM

July 10, 2020

To: Members of the Committee on Oversight and Reform

Fr: Majority Staff

Re: Hearing on U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act

On **Wednesday, July 15, 2020, at 12:00 p.m. E.T.**, the Committee on Oversight and Reform will host a remote hearing to examine U.S. cybersecurity preparedness and H.R. 7331, the National Cyber Director Act, which would create the position of a National Cyber Director within the White House to lead national-level coordination of cyber strategy and policy.

I. BACKGROUND

Cyberattacks are a critical, complex, prevalent, and growing threat to the nation's safety and economic security, touching nearly every aspect of daily life. The most recent Worldwide Threat Assessment of the U.S. Intelligence Community lists cyberattacks as a top global threat, with China, Russia, Iran, and North Korea waging a silent war capable of shutting down critical infrastructure, breaching sensitive information systems, and jeopardizing critical sectors in America and globally.[1]

Cyberattacks have long been a tool of choice for nation-state and non-state actors intent on disrupting American security and prosperity.[2] In addition to decades of intellectual property theft with damages in the hundreds of billions of dollars, Chinese hackers have successfully launched multiple major cyberattacks on American government and corporate systems since 2014, compromising the sensitive information of hundreds of millions of federal employees and civilians.[3] Russian-backed cyberthreats have succeeded in damaging public trust in our elections

[1] Office of the Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (Jan. 29, 2019) (online at www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf).

[2] The White House, *National Cyber Strategy of the United States of America* (Sept. 2018) (online at www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf).

[3] United States Cyberspace Solarium Commission, *Final Report* (Mar. 2020) (online at drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view).

and democratic institutions.[4] North Korea has attempted to steal more than $1.1 billion from financial institutions worldwide, including the successful theft of approximately $81 million from the New York Federal Reserve account of Bangladesh's central bank.[5]

Ransomware and other cyberattacks pose daily threats to American citizens and to the core functions of government entities, corporations, and non-profit organizations. Internet of Things (IoT) devices, or omnipresent everyday objects that act as network-connected data sensors, have been hacked for nation-state reconnaissance, to shut down internet access for millions of Americans simultaneously, to knock out websites, and to seize control of power grids.[6]

In 2019, more than 200,000 entities, including the city of New Orleans, were attacked by ransomware that froze their computer systems and ground operations to a halt.[7] Over the last three years, ransomware has cost American businesses hundreds of millions of dollars and forced many small and medium businesses to close their doors.[8] In 2018, the White House Council of Economic Advisors estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.[9]

The coronavirus crisis serves as a prime example of the extent to which sophisticated cybercriminals rapidly adapt their tactics to target perceived vulnerabilities by exploiting catastrophes. Hackers linked to Iran reportedly targeted the World Health Organization during the outbreak,[10] and warnings from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigations (FBI) indicate the targeting of COVID-19 research organizations by Chinese actors.[11] By the end of March,

---

[4] Benjamin Jensen, Brandon Valeriano, and Ryan Maness, *Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist*, Journal of Strategic Studies, no. 42 (2019) (online at www.tandfonline.com/doi/abs/10.1080/01402390.2018.1559152).

[5] *Id.*

[6] *What Is the Internet of Things? A WIRED Guide*, WIRED (Feb. 10, 2020) (online at www.wired.com/story/wired-guide-internet-of-things/).

[7] *Ransomware Attacks Grow, Crippling Cities and Businesses*, New York Times (Feb. 9, 2020) (online at www.nytimes.com/2020/02/09/technology/ransomware-attacks.html)

[8] *NotPetya Costs Merck, FedEx, Maersk $800M*, Cyber Security Hub (Oct. 31, 2017) (online at www.cshub.com/attacks/news/notpetya-costs-merck-fedex-maersk-800m); *Ransomware Shuts Down 1 in 5 Small Businesses after it Hits*, CNet (Aug. 2, 2017) (online at www.cnet.com/news/malwarebytes-state-of-ransomware-shutting-down-1-in-5-affected-small-businesses/)

[9] The White House, Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (February 2018) (online at www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf).

[10] *Exclusive: Hackers Linked to Iran Target WHO Staff Email During Coronavirus*, Reuters (Apr. 2, 2020) (online at www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC).

[11] Cybersecurity and Infrastructure Security Agency, *Press Release: FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations* (May 13, 2020) (online at www.cisa.gov/news/2020/05/13/fbi-and-cisa-warn-against-chinese-targeting-covid-19-research-organizations).

every country in the world had seen at least one attack aimed at exploiting the coronavirus crisis.[12]

Cybercriminals have also taken advantage of the pandemic to lure new victims into their schemes. In April, Google observed 18 million malware and phishing Gmail messages per day related to COVID-19, in addition to more than 240 million COVID-related daily spam messages.[13]

II. H.R. 7331, THE NATIONAL CYBER DIRECTOR ACT

The Cyberspace Solarium Commission, a body comprised of Congressional, executive branch, and private sector representatives, was established by the FY 2019 National Defense Authorization Act to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."[14] A key recommendation of the Commission's report is the creation of a National Cyber Director in the Executive Office of the President.

Federal cybersecurity responsibilities are spread across multiple agencies and subject to a constantly evolving cyberthreat landscape:

- CISA is responsible for coordinating civilian cybersecurity activities, liaising between the Federal government and non-Federal entities, developing cybersecurity policies and implementation guidance for Federal agencies, deploying cybersecurity tools, and supporting sector-specific cybersecurity.[15]

- The FBI leads the multiagency National Cyber Investigative Joint Task Force responsible for law enforcement-related cyberthreat information sharing and analysis.[16]

- The Cyber Threat Intelligence Integration Center at the Office of the Director of National Intelligence is responsible for leading intelligence support for cyber incident response.[17]

---

[12] *Exploiting a Crisis: How Cybercriminals Behaved During the Outbreak*, Microsoft Threat Protection Intelligence Team (June 16, 2020) (online at www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/)

[13] *Findings on COVID-19 and Online Security Threats*, Google Threat Analysis Group (Apr. 22, 2020) (online at blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/).

[14] Pub. L. No. 115-232 (2018).

[15] Congressional Research Service, *DHS's Cybersecurity Mission—An Overview* (Dec. 19, 2018) (online at crsreports.congress.gov/product/pdf/IF/IF10683).

[16] Congressional Research Service, *Cybersecurity: Federal Agency Roles* (Feb. 13, 2017) (online at crsreports.congress.gov/product/pdf/IF/IF10602).

[17] Office of the Director of National Intelligence, *Cyber Threat Intelligence Integration Center Quick Facts* (online at www.dni.gov/index.php/ctiic-features/1722-ctiic-quick-facts) (accessed July 10, 2020).

- U.S. Cybercommand is responsible for directing, synchronizing, and coordinating cyberspace planning and operations from a national security perspective and in collaboration with domestic and international partners.[18]

- An array of other Federal agencies have cybersecurity roles, including building relations with their associated critical infrastructure sectors.[19]

The stated intent of the National Cyber Director position as envisioned by H.R. 7331 is to coordinate across these various planning, integration, and response activities. The position would create strategic leadership at the White House to develop a comprehensive approach, enforce coordination across departments and agencies, streamline priorities, lead planning for defensive cyber activities, integrate the Federal government effort with the private sector and with state and local governments, and coordinate initial incident response. The Director also would engage in international efforts on cybersecurity with the goal of projecting U.S. leadership and enhancing the global coordination essential for success in managing cyberthreats.

During the George W. Bush Administration, a cybersecurity coordinator role was established at the White House to streamline cyber efforts across the Federal government.[20] The role was elevated and expanded in 2009 by President Barack Obama,[21] but eliminated in 2018 by then National Security Adviser John Bolton.[22]

The National Cyber Director recommended by the Commission would fulfill a similar policy role to the previous cybersecurity coordinator, but the new position would be backed with additional resources and statutory authority to lead strategic planning efforts, review cybersecurity budgets, and coordinate national incident response.

Under H.R. 7331, the National Cyber Director would be appointed by the President subject to Senate confirmation and would head an office of 75 people within the Executive Office of the President. The Director would serve as the principal advisor to the President on cybersecurity strategy and policy and would develop and oversee implementation of a National Cyber Strategy to defend the nation's interests and secure critical infrastructure against malicious cyber actors. The Director would plan for, oversee, and coordinate Federal government incident response activities, collaborate with private sector entities, and participate in meetings of the National Security Council and Homeland Security Council. The Director also would work with the State Department to coordinate international engagement on cybersecurity.

---

[18] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Apr. 2018) (online at cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010#:~:text=Our%20purpose%20is%20to%20achieve,to%20shift%20resources%20to%20defense).

[19] *Id.*

[20] *Bolton Eliminates White House Cybersecurity Position*, CyberScoop (May 15, 2018) (online at www.cyberscoop.com/white-house-cybersecurity-coordinator/)

[21] *Obama Names Howard Schmidt as Cybersecurity Coordinator*, Washington Post (Dec. 22, 2009) (online at www.washingtonpost.com/wp-dyn/content/article/2009/12/22/AR2009122201429.html).

[22] *White House Eliminates Cybersecurity Coordinator Role,* New York Times (May 15, 2018) (online at www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html).

H.R. 7331 was introduced on June 25, 2020 by Cyberspace Solarium Commissioner, Congressman Jim Langevin; Solarium Commission Co-Chair, Congressman Mike Gallagher; Oversight Committee Chairwoman Maloney; Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure and Innovation Ranking Member John Katko; former House Intelligence Committee Ranking Member C. A. Dutch Ruppersberger; and House Intelligence Committee Subcommittee on Intelligence Modernization and Readiness Ranking Member Will Hurd.

III. WITNESSES

Panel 1

The Honorable James R. Langevin
Commissioner, U.S. Cyberspace Solarium Commission
Member of Congress

The Honorable Mike Gallagher
Co-Chair, U.S. Cyberspace Solarium Commission
Member of Congress

Panel 2

The Honorable Michael J. Rogers
David Abshire Chair, Center for the Study of the Presidency & Congress
Chairman, House Permanent Select Committee on Intelligence (2011-2015)

J. Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance
White House Cybersecurity Coordinator (2012-2017)

Amit Yoran
Chairman and Chief Executive Officer, Tenable
Founding Director, U.S. Computer Emergency Readiness Team (US-CERT) (2003-2004)

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

Jamil N. Jaffer
Founder & Executive Director, National Security Institute
George Mason University

Staff contacts: Emily Burns or Mark Stephenson at (202) 225-5051.