CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
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

**MEMORANDUM**

**January 6, 2022**

**To: Members of the Committee on Oversight and Reform**

**Fr: Committee Staff**

**Re: Hearing on "Cybersecurity for the New Frontier: Reforming the Federal Information Security Modernization Act"**

On **Tuesday, January 11, 2022, at 10:00 a.m. ET**, the Committee on Oversight and Reform will hold a hybrid hearing **in room 2154 of the Rayburn House Office Building and on the Zoom video platform**. The hearing will examine the dramatic transformation in the cyberthreat landscape since the Federal Information Security Modernization Act was enacted and last updated, as well as the importance of modernizing this premier cybersecurity law to meet these challenges.

## I. BACKGROUND

The Federal Information Security Management Act (FISMA), signed into law on December 17, 2002, requires each federal civilian agency to establish an agency-wide program to ensure the security of the agency's information and systems. Last updated in 2014, FISMA lays out the roles and responsibilities of federal agencies related to the security of federal information systems and data as described below.

- **The National Institute for Standards and Technology (NIST)** develops standards and guidance on cybersecurity practices for federal agencies, contractors, and other system operators and data processors that perform services on behalf of the federal government.

- **The Office of Management and Budget (OMB)** oversees the information security and privacy practices of federal agencies and ensures agency adoption of NIST standards, setting policy and promulgating guidance through the issuance of mandatory memoranda and circulars. OMB also oversees and enforces agency adoption of cybersecurity practices through its oversight of agency budgets. Additionally, OMB must define a major incident, which agencies must report to Congress within seven days of identification. OMB's Office of the Federal Chief

Information Officer (CIO) executes these responsibilities with the Federal Chief Information Security Officer.

- **The Department of Homeland Security (DHS)** provides operational and technical support to agencies, including by issuing binding operational directives, in implementing the cybersecurity policies, principles, standards, and guidelines issued by OMB. This responsibility was delegated to the Cybersecurity and Infrastructure Security Agency (CISA), which is a component of DHS, after CISA's creation in 2018. CISA also provides shared services like the National Cybersecurity Protection System, which scans the internet traffic of federal agencies for threats, and the Continuous Diagnostics and Mitigation Program, which monitors agency networks for vulnerabilities.

- **Agency heads** bear ultimate responsibility for their organization's risks and delegate the management of cybersecurity risk to the agency CIO or another senior agency information security official. Agencies report progress on implementation of NIST standards and other cybersecurity initiatives using requirements developed by OMB and CISA, known as CIO FISMA metrics and Inspector General (IG) FISMA metrics. Agencies also report annually on effective management of the personally identifiable information of individuals through Senior Agency Official for Privacy metrics. Agencies impacted by cyber incidents are ultimately responsible for determining if an incident should be designated as major, thereby triggering congressional reporting requirements.

- **Inspectors General** conduct annual evaluations of the adequacy of agency IT security programs and posture using the IG FISMA Metrics developed by OMB and CISA.[1]

The evolution of technology and information systems during the lifespan of FISMA has had profound ramifications for federal cybersecurity. According to OMB, federal agencies reported 30,819 cybersecurity incidents in Fiscal Year 2020—an increase of 8% compared to the previous year—and six major incidents.[2] Since then, a series of major incidents and newly discovered vulnerabilities have profoundly affected the federal information security landscape:

- **SolarWinds Breach.** In December 2020, a major breach was identified in software issued by SolarWinds, a technology company providing IT management products. The breach allowed Russian actors to infiltrate and roam the networks

[1] Congressional Research Service, *Federal Cybersecurity: Background and Issues for Congress* (Sept. 29, 2021) (online at www.crs.gov/Reports/R46926?source=search&guid=77977e31397146e1927d294c71627c87&index=3#_Toc83897007).

[2] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2020* (May 2021) (online at www.whitehouse.gov/wp-content/uploads/2021/05/FY-2020-FISMA-Report-to-Congress.pdf).

of at least nine federal agencies and 100 private sector companies for seven months prior to discovery of the breach.[3]

- **Cyber Espionage by China.** In March 2021, Microsoft announced an attack in which Hafnium, a group of hackers operating on behalf of China, exploited four vulnerabilities of the Microsoft Exchange Server to steal data and embed in compromised networks.[4] The attack marked the eighth time in 12 months that Microsoft announced nation-state actors targeting institutions critical to civil society.[5] In July, the United States joined the European Union, the United Kingdom, the North Atlantic Treaty Organization (NATO), and other allies in condemning China's use of criminal contract hackers to conduct cyber espionage, including through the exploitation of the Microsoft Exchange Server vulnerabilities.[6]

- **Major Ransomware Attacks.** On May 7, 2021, a ransomware attack by DarkSide, a cybercrime group linked to Russia, on Colonial Pipeline Company shut down the largest fuel pipeline in the United States and limited fuel supplies to the East Coast. The company was breached through a dormant virtual private network account accessed using a leaked password that had been posted on the dark web, and DarkSide threatened to release 100 gigabytes of stolen data from Colonial.[7] The company paid the demanded ransom of $4.4 million, about half of which was recovered by the Department of Justice.[8] Additional major ransomware attacks were waged against JBS USA, a U.S.-based meat producer, and Kaseya, an American software firm, by REvil, a Russian ransomware-as-a-service organization.[9]

---

[3] The White House, Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger (Feb. 17, 2021) (online at www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/).

[4] Microsoft, *Hafnium Targeting Exchange Servers with 0-Day Exploits*, (Mar. 2, 2021) (online at www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/).

[5] Microsoft, *New Nation-State Cyberattacks* (Mar. 2, 2021) (online at https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/).

[6] The White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China* (July 19, 2021) (online at www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/).

[7] *Hackers Breached Colonial Pipeline Using Compromised Password*, Bloomberg (June 4, 2021) (online at www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password).

[8] *How a Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back,* National Public Radio (June 8, 2021) (online at www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac).

[9] *Meritalk's Top 10 Cybersecurity Moments of 2021,* MeriTalk (Dec. 29, 2021) (online at www.meritalk.com/articles/meritalks-top-10-cybersecurity-moments-of-2021/).

- **Log4j Software Vulnerability.** On December 9, 2021, a vulnerability was discovered in freely available and widely used open-source software provided by the Apache Foundation called Log4j. Mitigation is ongoing, but because the software has been used to build a vast array of web services for almost a decade, identifying vulnerable applications and servers is difficult. Deploying the remediated version of Log4j is complex.[10] The Director of CISA has called the Log4j vulnerability the most serious vulnerability she has seen in her decades-long career.[11]

## II. HEARING PURPOSE

The purpose of the hearing is to examine the dramatic transformations in the cyberthreat landscape since FISMA was created in 2002 and last updated in 2014. The hearing will also examine flaws and missed opportunities in the current law, and evaluate reforms to FISMA to create a clear, coordinated, whole-of-government approach to federal cybersecurity.

## III. WITNESSES

**Mr. Grant Schneider**
Senior Director of Cybersecurity Services, Venable
Federal Chief Information Security Officer,
Office of Management and Budget (2018-2020)
Senior Director for Cybersecurity Policy, National Security Council (2017-2020)

**Ms. Renee Wynn**
Chief Executive Officer, RP Wynn Consulting LLC
Chief Information Officer, National Aeronautics and Space Administration (2015-2020)

**Mr. Gordon Bitko**
Senior Vice President of Policy, Public Sector, Information Technology Industry Council
Chief Information Officer, Federal Bureau of Investigation (2016-2019)

**Ms. Jennifer R. Franks**
Director of Information Technology and Cybersecurity
Government Accountability Office

**Mr. Ross Nodurft**
Executive Director, Alliance for Digital Innovation
Chief, Office of Management and Budget Cybersecurity Team (2015-2018)

---

[10] Congressional Research Service, *Systemic Vulnerabilities in Information Technology—Log4Shell* (Dec. 21, 2021) (online at www.crs.gov/Reports/IN11824?source=search&guid=e42aa7479d57422eac92062f44be2527&index=0).

[11] *The "Most Serious" Security Breach Ever is Unfolding Right Now. Here's What You Need to Know*, Washington Post (Dec. 20, 2021) (online at www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/).

Staff contacts: Emily Burns, Courtney Callejas, Christina Parisi, Warner Dixon, and Eric Snyderman at (202) 225-5051.