Written Statement of

Grant Schneider

Senior Director of Cybersecurity Services, Venable LLP

Congress of the United States

House of Representatives

Committee on Oversight and Reform

January 11, 2022

Chairwoman Maloney, Ranking Member Comer, members of the Committee, and your staff thank you for the privilege to appear before you today.

I have spent my entire 30-year career focused on our nation's security. This includes over 20 years at the Defense Intelligence Agency, 7 of which I served as the Chief Information Officer charged with the delivery of secure and resilient technology solutions to a global customer set. I then spent 6 years at the Executive Office of the President during the Obama and Trump Administrations focused on all aspects of federal and critical infrastructure cybersecurity. During that time, I served as a Senior Director for Cybersecurity Policy on the National Security Council staff and most recently as the Federal Chief Information Security Officer (CISO) executing the Office of Management and Budget (OMB) Director's authorities provided under the Federal Information Security Modernization Act (FISMA) of 2014. For the past 16 months I have been a Senior Director of Cybersecurity Services at the law firm Venable where I help our clients, both large and small companies from across all sectors, enhance their cybersecurity programs through the development and implementation of risk management programs as well as assisting with the preparation, response and recovery from various cyber incidents including ransomware.

I want to thank the Committee for taking up the important issues related to the security of the nation's federal information and information systems. The Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act of 2014, each known as FISMA, have been instrumental in driving creation of risk management programs and the implementation of cybersecurity capabilities at federal agencies. In short, the FISMA legislation has focused agencies attention on cybersecurity and made them more secure. However, FISMA must evolve just as the threats and the nature of our Information Technology environments continue to evolve.

The threat surface of federal agencies, and private sector organizations, increases as organizations interconnect systems and move more sensitive information and transactions online. This started well before the global pandemic and has accelerated during the past two years. To be clear these digital enhancements increase productivity, increase convenience, and increase access to services. At the same time malicious cyber actors have increased their capabilities and demonstrated a willingness to exploit any system to achieve their objectives, whether they be monetary gain, espionage, or some form of activism. Most recently public and private sector organizations have been responding to exploitation of the Log4J vulnerability. Over the past year organizations have responded to the attack on SolarWinds, the Hafnium Microsoft Exchange Server incident and countless ransomware attacks including the one involving Colonial Pipeline. These are but a few of the many incidents highlighting the importance of cybersecurity.

I believe we need a whole of government approach to address the challenges we face in cyberspace. This includes diplomatic efforts and offensive cyber operations to deter and disrupt nation state and criminal malicious cyber actors. However, our primary line of defense is defensive in nature. Public and private organizations must take measures to create secure capabilities and effectively protect their systems.

FISMA is focused on directing federal agencies to develop and implement risk management programs to secure federal information and information systems. There are many areas where agencies need to focus their attention. As you consider updates to this keystone piece of legislation, I encourage you to address five key areas.

1. Clarify key federal cybersecurity roles and responsibilities: Since the last update to FISMA, Congress has established the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security as well as the National Cyber Director (NCD) within the Executive Office of the President. These have been important additions to the federal cybersecurity ecosystem and require clarification of roles and responsibilities with respect to federal cybersecurity. I recommend Congress clarify the roles and responsibilities at a high level and direct the President to clarify them in more detail. At a high level I see the roles and responsibilities with respect to federal cybersecurity as:

    - NCD - Overall cybersecurity strategy of the United States
    - OMB – Policy development and oversight (including agency reporting and accountability) of federal cybersecurity
    - CISA - Operational cybersecurity coordination to assist federal agencies with the protection of their systems
    - NIST – Develop cybersecurity standards and guidelines
    - Agencies - Develop and implement their risk management programs

2. Codify the role of the Federal Chief Information Security Officer as a Presidentially appointed position within OMB with appropriate budget and oversight authorities, including:

    - Serve as Deputy National Cyber Director
    - Chair the Federal Acquisition Security Council (FASC)
    - Serve as a permanent member of the TMF board
    - Approval authority for the CISA budget
    - Approval authority of agency cybersecurity budgets

3. As part of their risk management programs, require agencies to have greater situational awareness of their technology environments. This includes real-time inventories of hardware and software; supply chain assessments of those inventories; understanding of the actions being performed within their environment; and fully inspecting network sessions to identify and mitigate the techniques used to compromise systems. All these items can contribute to or complement an agency's move to a Zero Trust environment.

4. Hold OMB accountable for maintaining the definition of a major incident to ensure the right level of information is being reported to Congress. Additionally, an annual or bi-annual briefing from OMB, the NCD, and CISA to Congressional staff could be required to review federal cybersecurity incidents.

5. Require greater alignment of core cybersecurity requirements based on National Institute of Standards and Technology guidance for both National Security Systems and non-National Security Systems. This will help streamline industry's ability to develop and

provide solutions for the Department of Defense, the Intelligence Community, and Federal Civilian Agencies.

Thank you again for the opportunity to be with you today and I look forward to your questions.