Written Statement of

Grant Schneider

Senior Director of Cybersecurity Services, Venable LLP

United States Senate

Committee on

Homeland Security and Governmental Affairs and Reform

May 12, 2022

Chairman Peters, Ranking Member Portman, 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. I then spent 6 years at the Executive Office of the President involved with all aspects of federal and critical infrastructure cybersecurity. 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 working with agencies to secure federal systems. For the past 20 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 strategies as well as assisting with the preparation, response and recovery from various cyber incidents including ransomware attacks. I have also helped many clients who are working to navigate acquisition and compliance regimes necessary to do busines with the federal government.

I want to thank the Committee for taking up the very important issues related to the timely acquisition of goods and services by the government.

My first exposure to federal procurement was in the mid-90s when I was assigned as the DIA representative to work on a global IT support contract for the defense intelligence community. I was a GS 8 or 9 and met a would-be colleague and mentor, the Airforce representative for the project. One day I made a comment about the leverage the contract gave us over the contractor and what a good deal it was going to be for the government. The Airforce representative turned to me and said, "Look son, the point of the contract is to create a relationship that allows the government and industry to work together to deliver mission outcomes.

It's not there for us to beat each other over the head with." That forever changed the way I looked out the defense industrial base and acquisition. I experienced the mission success possible from a partnership between the contracting officer, the technologists, and the vendor. Unfortunately, most people I met throughout my career viewed contracts as an adversarial tool rather than a collaborative opportunity.

Federal agencies, like nearly all organizations today, are dependent on technology to develop and deliver critical services in support of our nation. This includes everything from developing advanced military capabilities, to processing student loans, to making Social Security payments. As we have seen during the pandemic, services that were routinely done in person are being moved on-line. 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. This evolution to a more digital experience means federal information technology investments are more critical than ever before.

And the federal government invests a lot in information technology, more than $90 billion per year. Most of that money is spent on goods and services provided by industry partners and acquired through federal procurement processes.

For the government to be innovative in its delivery of capabilities, it must be able to harness the innovative tools, technologies, and services available across the private sector. Federal agencies need agility within the procurement system to leverage these capabilities in a timely manner. Here are five actions government can take to enhance procurement innovation:

1. Provide greater flexibilities for contracting officers to prioritize the mission interests of the government during procurements. This includes recognizing that time to market, for both the procurement

process and the vendor's delivery, is a key metric for every technology acquisition. Contracting professionals should be incentivized to consider the various mission interests when considering the risks associated with the acquisition approach and selection criteria. Senior leadership should drive their organizations to focus on mission delivery rather than the liabilities associated with compliance activities and fear of protests.

2. Establish strong partnerships between technology and acquisition professionals. Each of these groups work in specialized areas with a high level of compliance and associated oversight activity. To acquire innovative solutions, the two teams must understand and appreciate, the complexities of each other's environments. I recommend creating joint teams of acquisition and technology professionals who can focus on mission delivery to address agencies most pressing technology procurement needs.

3. Develop procurement vehicles that allow for technical refresh throughout their life cycle so new technologies can be made available to agencies without necessitating a new procurement process. The government cannot afford taking years to acquire "new" technologies.

4. Consider the supply chain risks associated with goods and services in technology acquisitions. This includes the quality and provenance of the items being procured, the trustworthiness of the provider and any legal influence a hostile entity could exert on the provider. Additionally, the government should take steps to help ensure there is a trusted international marketplace available for public and private sector acquisitions.

5. Drive consistent compliance and security requirements across the Department of Defense (DoD) and federal civilian acquisitions. DoD and civilian agencies are seeking many of the same innovative commodity technologies available in the private sector, however increasing divergence in compliance requirements

increases the cost to the private sector to develop and provide solutions to both communities.

When you acquire a product, you also inherit any risks associated with its supply chain. Expanding on item four above, organizations must take steps during the acquisition process to ensure the security of their environments, including the application of supply chain risk management principles for technology acquisitions. These could include:

1) Trusted Market Place: In supply chain, there is often a lot of discussion around what not to do with respect to technology purchases. Do not purchase equipment form a particular provider or country of origin. This may be appropriate in some instances; however, we must also focus on the creation of a trusted international marketplace from which public and private sector organizations can make purchases.

2) Trusted Products in Critical Markets: Not all organizations, inside or outside of government, have the same risk profile. We need a flexible marketplace that can meet the various risk profiles at acceptable price points.

3) Trusted Suppliers: Trusted suppliers should be able to operate between and among industry verticals. There are security and economic benefits of encouraging trusted suppliers to support multiple industry sectors such as Information Technology, Operational Technology, Energy, Transportation, Retail, and Biopharmaceuticals.

4) Manufacturing process and Manufacturer intentions ("Trustworthiness"): Government and industry purchasers need to evaluate the goods and services they bring into their environments from both a quality and trustworthiness perspective. This includes understanding any legal influence an entity could exert on the provider.

5) Standard Supply Chain Assessments: There is significant value in standardizing or normalizing supply chain assessments, particularly when they are done by various entities within the government.

6) Information Sharing: Sharing with government and between/among public sector entities should be encouraged and include liability protections.

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