Opening Statement
Ranking Member Gerald E. Connolly
"Safeguarding the Federal Software Supply Chain"
Cybersecurity, Information Technology, and Government Innovation
Wednesday, November 29, 2023

For the entirety of the 118th Congress, Democrats have single-handily conducted oversight into agencies' compliance with the Federal Information Technology Acquisition Reform Act, also known as FITARA. It is deeply concerning our Chairwoman is willing to abandon this eight-year, formerly bipartisan, collaboration, which has saved American taxpayers more than $30 billion over its lifetime. Our constituents and our peers have entrusted us with the responsibility of conducting vigorous oversight into issues related to *quote* "government-wide federal information technology (IT) management and innovation," which is one-third of our subcommittee's jurisdiction.

I understand that it isn't the flashiest issue. It does not grab headlines like robot dogs and ChatGPT-written statements. But it is the hard work of government, and it must get done. I am committed to continuing to hold the executive branch accountable when it comes to IT modernization, robust cybersecurity, effective encryption, and safely moving to the cloud. FITARA oversight will continue, with or without participation from the Republican leadership of this Committee.

Our hearing today is on how to best safeguard our federal government's software supply chain. Gartner, an American technological research and consulting firm, estimates the world will spend more than $916 billion on software in 2023 and predicts spending will grow to over $1 trillion by 2024.[1] That increase is almost a 14% jump in just one year and bad actors all over the world are taking notice. Every day, cyber criminals are developing new, more sophisticated strategies that exploit vulnerabilities and attack all points of a software's supply chain. It is

[1] https://www.gartner.com/en/newsroom/press-releases/2023-10-18-gartner-forecasts-worldwide-it-spending-to-grow-8-percent-in-2024

essential we protect all parts of the supply chain because a software's security is only as strong as its weakest link.

Just this Thanksgiving weekend, Microsoft reported that a North Korean nation-state actor, linked to the notorious cybercrime group Lazarus, stole a software signing key and inserted malware into a legitimate application developed by the Taiwanese multimedia software and AI developer, Cyberlink. The malware, known as "LambLoad," infiltrates a system by dropping a fake PNG file to deploy malicious code. This code enables unauthorized users to steal sensitive data, establish persistent access to traditionally protected systems, and corrupt other connected systems. Hackers used LambLoad to successfully compromise more than 100 devices in multiple countries, including Japan, Taiwan, Canada and the United States. The full extent of the attack's damage has yet to be determined.

Unfortunately, these kinds of attacks are nothing new. The 2020 SolarWinds attack penetrated the IT systems of thousands of organizations globally, including an unprecedented U.S. federal government data breach. Tens of thousands of SolarWinds customers across both the public and private sectors scrambled to protect their own data as attackers stole sensitive documents, abused authentication credentials, and exposed private emails.

Information security has been on the Government Accountability Office's (GAO) High-Risk List since 1997. Securing the federal software supply chain is one crucial step toward shoring up national security. That is why I championed enactment of the FedRAMP Authorization Act, which in the previous Congress codified FedRAMP, the program that certifies appropriate cybersecurity protections in the federal government's cloud service products.

Earlier this year, the FedRAMP Joint Authorization Board (JAB) released and approved its updated catalog of security and privacy controls for cloud products, also known as FedRAMP Revision 5

Baselines. Government procurement experts use this catalog to assess, authorize, and determine whether a cloud product or service incorporates security features suitable for government use. JAB updated the FedRAMP Revision 5 Baselines to align with the National Institute of Standards and Technology's (NIST) guidance and added two new supply chain related control categories[2] to help group and organize the over 421 controls FedRAMP uses to determine a product's risk otherwise known as an impact level.

The first is Supply Chain Risk Management, which more comprehensively addresses the risks associated with the acquisition, development, and maintenance of information systems and components associated with third-party and vendor services, products, and supply chains. The second is Coordination with Supply Chain, which requires that information related to cybersecurity incidents be reported to organizations involved in the supply chain or supply chain governance.

The Biden-Harris Administration has also taken important and novel steps to improve IT supply chain security. In 2021, President Biden issued Executive Order (EO) 14028: Improving the Nation's Cybersecurity, which required agencies to enhance cybersecurity and software supply chain integrity. This EO resulted in a September 14, 2022, Office of Management and Budget (OMB) Memorandum that directed agencies only to use software that complies with government-specified minimum secure software development practices.

The memorandum instructed tech vendors to provide their federal government clients with a software bill of materials, or an "SBOM [*ESS-BOMB*]," which is similar to an ingredient list on the back of a cereal box. And the memo provided agencies with additional compliance guidance. I hope our witnesses will share the best ways to enforce these directives and optimize these cyber defense measures.

[2] NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

The FITARA Scorecard also tracks and assesses federal agencies' supply chain security practices and policies within its Federal Information Security Modernization Act (FISMA) category. The FISMA category was a much-needed addition, crafted in collaboration with former Republican Rep. Will Hurd.

The grade is a composite of two different assessments. The first comes from the "Identity" function of the Inspectors General (IG) assessments – which identifies an agency's supply chain risk management strategy including priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks. The second uses metrics from Federal Cybersecurity Progress Reports published on Performance.gov.

Last year, as Chair of the Government Operations Subcommittee, I pushed the Office of Management and Budget to build off President Biden's cutting-edge Executive Order 14028 and update their cybersecurity metrics. Federal Chief Information Security Officer Chris DeRusha successfully completed this task resulting in the creation of quarterly Federal Cybersecurity Progress Reports made up of modernized metrics that more closely align to the NIST Cybersecurity Framework. NIST's framework strengthens our cybersecurity supply chain risk management, helps agencies achieve observable security outcomes, and operationalizes hard-learned lessons from the SolarWinds attack.

I also applaud OMB's recent memorandum update, which extends the timelines for agencies to collect attestations from software producers and provides supplemental guidance for those still in the attestation collection process. The federal government must navigate the tension of buying safe and secure IT responsibly while leveraging cost-effective and innovative technologies that serve our constituents. This Subcommittee looks forward to partnering with the private sector to ensure the federal government maintains the delicate balance between

embracing innovation and securing our critical infrastructure to safeguard the federal software supply chain.