Statement of Congressman Gerald E. Connolly (VA-11)
Committee on Oversight and Government Reform
Full Committee Business Meeting
Thursday, February 2, 2022

I thank Chairwoman Maloney for bringing these important pieces of legislation to the Committee's attention today. These bills will help the federal government plan for, track, and mitigate the security risk for its information technology (IT) and for the nation's supply chains; ensure an equal playing field for individuals applying to federal jobs; streamline the operations of the Government Accountability Office (GAO) so it can focus on congressional priorities; and require the District of Columbia's Commanding General of the District of Columbia (D.C.) National Guard to reside in D.C.

The Federal Information Security Modernization Act of 2022 (H.R. 6497)

I am proud to be an original co-sponsor of Chairwoman Maloney's Federal Information Security Modernization Act of 2022 (FISMA 2022). Over the past several years, we have witnessed the ramifications of poor cybersecurity posture across the federal government's IT landscape, leaving sensitive IT systems and data vulnerable to cyberattacks and incurring significant disruptions and costs.

FISMA 2022 updates the Federal Information Security Modernization Act (FISMA), which Congress passed in 2002 and amended in 2014. GAO continues to list federal cybersecurity strategy and implementation on its High-Risk List, which it has done since 1997. Despite FISMA's positive contributions to improving federal cybersecurity, Congress has a critical role in ensuring that it evolves to accommodate and anticipate new realities.

When FISMA first passed, many of today's key cyber stakeholders had yet to be established, like the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Director (NCD). FISMA 2022 incorporates these new stakeholders, clearly assigning federal cybersecurity policy development and oversight responsibilities to the Office of Management and Budget (OMB), operational coordination responsibilities to the CISA, and overall cybersecurity strategy responsibilities to the NCD. It also codifies the OMB Federal Chief Information Security Officer, extends the Federal Acquisition Security Council until 2026, and extends the Chief Data Officer Council until 2030.

In addition, government officials have cited FISMA requirements as onerous and overly focused on compliance, rather than on mitigating potential cyber threats. FISMA 2022 streamlines reporting requirements by reducing the frequency of FISMA assessments and requiring ongoing and continuous risk assessments that allow agencies to prioritize cybersecurity risks with accurate, real-time information about their cybersecurity posture. The bill also imposes more rigorous reporting requirements on agencies for major incidents so that the federal government can respond more quickly and aggressively to cyberattacks.

Finally, as technology evolves, so must our approach to securing our nation's IT infrastructure. FISMA 2022 promotes key tenets of President Biden's Executive Order on "Improving the Nation's Cybersecurity," including zero trust architecture and vulnerability disclosure programs. It also promotes pillars of IT modernization like cloud migration, automation, and shared services.

By utilizing shared services, the government can promote efficiency, cost savings, and best practices. Similar security and acquisition principles are advanced by the government-wide Federal Risk and Authorization Management Program (FedRAMP), which provides a standardized approach to cyber security assessment, authorization, and continuous monitoring for federal cloud products and services.

For the past five years, I have worked to improve and codify the FedRAMP program, through my FedRAMP Authorization Act (H.R. 21). The bill passed the House with bipartisan support twice in the last Congress, once under suspension by voice vote and again as an amendment to the House National Defense Authorization Act for FY2021. It passed another two times this Congress, once after I introduced it in January of last year and again as an amendment to the FY2022 NDAA. In fact, FedRAMP was the first bill to pass the House in the 117th Congress. I welcome action on the bill by the Senate Committee on Homeland Security and Government Affairs, and I reiterate the call the Chairwoman made during our FISMA hearing, for the full Senate to act on H.R. 21 immediately. As this Committee is demonstrating with expedited consideration of FISMA 2022, we cannot allow critical cybersecurity legislation to languish. FedRAMP offers an agile and secure way for federal agencies to transition to the cloud so that the government can protect the public's information while also delivering services seamlessly in a cost-effective manner.

The Fair Chance Improvement Act (H.R. 6419)

The Fair Chance Improvement Act amends the Fair Chance to Compete for Jobs Act, or the Fair Chance Act, which was enacted as part of the National Defense Authorization Act for Fiscal Year 2020. The Fair Chance Act, which had broad bipartisan support in both the House and Senate, prohibits the federal government from asking candidates for employment about any criminal history before a conditional offer is made. It put the same prohibition on federal contractors who are hiring for positions associated with both civilian agency and defense contracts.

Under the law, enforcement of the law's provisions for federal contractors is assigned to the General Services Administration (GSA) and Department of Defense. H.R. 6419 transfers this authority to the Secretary of Labor, which is better equipped to carry out this enforcement role because of its existing procedures and infrastructure

The Supply Chain Security Training Act (H.R. 5962)

The Supply Chain Security Training Act would require the General Services Administration (GSA) to establish a training program for federal agency personnel with responsibilities related to supply chain risk management. A GAO report found that no federal agencies surveyed had fully implemented supply chain risk management standards for information and communication technology at the time the SolarWinds breach was discovered. This bill would better equip officials to identify and mitigate such supply chain security risks throughout the acquisition lifecycle.

The bill would require the GSA Administrator to update the program as determined necessary and in coordination with the Federal Acquisition Security Council, the Secretary of Homeland Security, and the Director of the Office of Personnel Management.

The GAO Mandates Revision Act (H.R. ____)

The GAO Mandates Revision Act would modify existing legislative mandates for GAO to perform financial statement audits or reviews of several agencies, ensuring that GAO can focus its resources on Congressional priorities instead of on superfluous audits.

Specifically, the bill shifts responsibility for annual financial statement audits from GAO to other auditing entities, including audits for the Federal Housing Finance Agency, the Consumer Financial Protection Bureau, the Congressional Award Foundation, the Patient-Centered Outcomes Research Institute, and the Export-Import Loan and Guarantee Transactions Act. It also reduces reporting requirements for certain outdated or completed programs and modifies GAO's required reporting

frequency under the Government Performance and Results Act Modernization Act of 2010 from every four years to periodic.

The District of Columbia National Guard Commanding General Residency Act (H.R. 6361)

The District of Columbia National Guard Commanding General Residency Act would require the Commanding General of the District of Columbia National Guard to reside in the District of Columbia. The Commanding General of the D.C. National Guard, who is the top official in the D.C. National Guard, is appointed by the President and is a federal official.

Thank you again to the Chairwoman for calling this business meeting. This slate of legislation deserves our full attention—among other things, it will transform government's approach to cybersecurity and supply chain risk and streamline oversight operations of GAO. I look forward to working with my colleagues on these important issues.