Written Statement of

Ross Nodurft

Executive Director

Alliance for Digital Innovation (ADI)

US House Committee on Oversight and Reform

Cybersecurity for the New Frontier: Reforming the Federal Information Security Modernization Act

January 11, 2022

Thank you, Chairwoman Maloney, Ranking Member Comer and members of the Committee for holding this hearing on FISMA reform.

My name is Ross Nodurft. I am the Executive Director of the Alliance for Digital Innovation (ADI), a coalition of innovative, commercial companies whose mission is to bring IT modernization and emerging technologies to government. ADI engages with policy makers and thought leaders to break down bureaucratic, institutional, and cultural barriers to change, and to enable government access to secure, modern technology that can empower a truly digital government.

ADI focuses on four key areas in our federal advocacy efforts – accelerating technology modernization in government, enabling acquisition policies that facilitate greater use of innovative technologies, promoting cybersecurity initiatives to better protect the public and private sectors, and improving the federal government's technology workforce. Each of these areas must work closely with each other to allow for government mission owners to partner with industry to build a modern, digital government.

My experience prior to taking on the role of executive director for ADI includes both operational and strategic roles in the government and the private sector focused on cybersecurity. More specific to today's discussion, I led the Office of Management and Budget's (OMB) Cybersecurity team, reporting to the Federal CISO and CIO. During that time, my team was responsible for drafting the annual FISMA report to Congress, developing and reporting the

FISMA metrics, writing and implementing government-wide cybersecurity policies, aggregating and producing the annual cybersecurity budget, and managing the team that conducted the oversight of federal civilian agencies' cybersecurity programs. Since leaving government, I have worked closely with many companies to build, expand, and institutionalize their own cybersecurity programs, and to develop an approach to cybersecurity risk management that effectively uses resources to buy down and manage enterprise risk.

Since joining ADI, I have worked closely with some of the leading technology, cybersecurity and professional services providers to the public sector. The technologies and services delivered by ADI member companies underpin the federal government's modernization efforts and provide the backbone for many agencies' zero trust architectures and cybersecurity plans. Given the roles that many of our member companies play in the federal cybersecurity and technology ecosystem, ADI appreciates the committee's focus on this important topic.

With the spate of cybersecurity incidents and vulnerabilities over the last several years, the need for continued oversight and support from Congress is necessary to combat the constantly evolving threats facing federal departments and agencies. The proposed FISMA legislation that was recently approved in committee in the Senate contains several important changes, but could be more comprehensive in its handling of cybersecurity as a holistic public sector priority As Congress considers an update to FISMA, ADI encourages this committee and others in the House and the Senate to also look to update other key laws dealing with government

information technology policy, acquisition, and governance. Updating the E-Government Act[1], the Clinger Cohen Act[2] and the Federal Information Technology Acquisition Reform Act (FITARA)[3], and aligning other proposed legislation, such as the House-passed FedRAMP Authorization Act, would enable agencies – as well as the oversight entities and program offices that govern federal IT policy – to modernize and secure their environments more quickly.

On the topic of FISMA reform, ADI believes that there are several important areas that warrant attention from the members of this committee. These include the need to:

- *Update and Align Cybersecurity Roles and Authorities* – changes to FISMA should reflect the new roles and authorities of the National Cyber Director (NCD) as well as the responsibilities of the Federal CISO at OMB and the Director of the Cybersecurity and Infrastructure Security Agency (CISA), many of which have evolved in recent years;
- *Address Incident Response, Breach Notification, and Vulnerability Management* – given the proliferation of incidents, breaches, and vulnerabilities, updated FISMA legislation should codify practices and policies that keep Congress informed in a way that will allow for effective oversight while giving departments and agencies the flexibility and time to respond to and report incidents, breaches, and vulnerabilities without disrupting or impacting their responses;

[1] Public Law 107–347
[2] The Information Technology Management Reform Act (ITMRA) and the Federal Acquisition Reform Act (FARA) were signed into law as part of the National Defense Authorization Act for Fiscal Year 1996 and were subsequently designated the Clinger Cohen Act of 1996.
[3] Public Law 113–291

- *Reinforce the Government's Shift to Commercial Technologies, Use of Automation and Meaningful Reciprocity* – as the government's information technology ecosystem shifts to more modern, cloud-based solutions, agencies should embrace technologies and services that enable security in these zero trust environments and leverage best-in-class industry partners to assist with the buildout of those environments. This bill should make it easier for agencies to issue authorizations to operate through strategies that include use of automation and offer reciprocity across agencies and across compliance regimes;
- *Effectively Budget for Cybersecurity and Invest in Risk Management* – securing large enterprises, especially those that have legacy technology and modernization backlogs, can be expensive. Congress must encourage agencies to budget for technology and services that can effectively buy-down the risks to their environments. As agencies continue to modernize their systems, agencies should pivot their cybersecurity spend to move towards tools and services that enable zero trust environments; and
- *Modernize and Standardize Cybersecurity Performance Metrics and Measurements* – as agencies modernize technology, move to cloud-based environments, take steps to enhance security, and migrate to zero trust architectures, oversight offices must also modernize the measurements used to track agency progress and measure security. Successful cybersecurity must be defined through outcomes, and those outcome-driven, risk-based metrics must be consistent across the various oversight entities.

Thank you, again, to the committee, for the opportunity to discuss this important topic. I look forward to your questions.

Key Recommendations for FISMA Reform:

1. Update and Align Cybersecurity Roles and Authorities

2. Address Incident Response, Breach Notification, and Vulnerability Management

3. Reinforce the Government's Shift to Commercial Technologies

4. Effectively Budget for Cybersecurity and Investing in Risk Management

5. Modernize and Standardize Cybersecurity Performance Metrics and Measurements

1. Update and Align Cybersecurity Roles and Authorities

The current FISMA law essentially states that every agency owns its own risk. At the same time, FISMA authorizes OMB, DHS, and NIST to set strategic guidance, develop government-wide cybersecurity policy, promulgate operational directives, continuously monitor security authorizations, update standards, and oversee the successful development and implementation of agency cybersecurity programs. Since the last FISMA update, Congress has updated DHS's authorities by codifying the Cybersecurity and Infrastructure Security Agency (CISA) and authorized and funded the Office of the National Cyber Director in the White House. Additionally, the White House created the position of the Federal Chief Information Security Officer (CISO) to oversee the development and implementation of OMB's cybersecurity policies, and to work with agencies to effectively budget for cybersecurity.

Any update to FISMA should reflect the new roles and authorities of the National Cyber Director as well as the responsibilities of the Federal CISO at OMB and the Director of CISA vis-a-vis federal government networks and their defense. Further, FISMA should encourage reciprocity of authorizations to operate (ATOs) wherever possible, and recognize that shared risk across federal agencies can facilitate ATO reciprocity.

2. Address Incident Response, Breach Notification, and Vulnerability Management

Over the last 36 months, the United States has seen some of the most significant cybersecurity attacks, breaches, and vulnerabilities in our history. The Solar Winds supply chain attack, the Colonial Pipeline and JBS ransomware attacks, and the recent Log4j vulnerability all present different challenges to the way our government responds to the various cybersecurity incidents and vulnerabilities. Given this proliferation of incidents, breaches, and vulnerabilities, updated FISMA legislation should codify practices and policies that keep Congress informed in a way that allows for effective oversight, while still allowing departments and agencies the flexibility and time to respond to and report incidents, breaches, and vulnerabilities without disrupting or impacting their responses.

More specifically, as Congress considers defining major incidents or codifying vulnerability response policies, any legislation should be mindful of the dynamic nature of responding to cybersecurity challenges facing government networks. If Congress is overly prescriptive in its definition of an incident, it runs the risk of receiving so many notifications that the incidents which are truly severe are missed or effectively drowned out due to the frequency of reporting.

Along the same lines, codifying the need for vulnerability management programs is important. However, being prescriptive about the ways to prevent various vulnerabilities may create overly burdensome processes that could bog down agency response efforts to mitigate and eventually patch significant vulnerabilities. Language that reflects today's technology runs the risk of becoming obsolete when it comes to the systems of tomorrow.

3. <u>Reinforce the Government's Shift to Commercial Technologies</u>

For decades, federal departments and agencies built their networks and information technology architectures by building bespoke new systems and bolting on security solutions to protect those systems. In recent years, executive branch officials have explained that these bolted-on approaches to technology and security have left gaps that continue to be exploited by our adversaries.

Given these threats to government missions, coupled with a focus on providing more digital access to citizens, agencies and administration officials have embraced the idea of modernizing their environments to improve customer experience and security. To be effective, these modernization efforts must be grounded in policies that enable purchase and consumption of the most cutting-edge, modern commercial solutions available. While a preference for commercial software procurement is already enshrined in law, the hurdles to its widespread adoption are prevalent throughout FISMA and its single-agency approach to ATOs.

Modern enterprise technology providers are pioneering solutions that can provide government agencies with significantly higher levels of security while increasing the impact of the information technology capabilities leveraged by the agencies. FISMA, and other federal information technology laws and proposed legislation, should promote buying commercial technology solutions first before looking to build custom government tools and services. Not only will use of commercial technology enable faster pathways to more secure, modern environments, it will also enable ease of security monitoring and response across agencies and shared solutions.

Additionally, as government agencies shift to modern, cloud-based solutions, the federal government should embrace technologies and services that enable security in these new environments and leverage best-in-class industry partners to assist with the build out of those environments. Leveraging the private sector's experience and expertise to help agencies build out, monitor, and provide third party security audits will allow government agencies to embrace zero trust architectures that can grow and flex with complex federal agency technology needs.

Finally, to effectively drive modern security architectures and solutions, this legislation should make it easier for agencies to issue ATOs, continuously monitor those authorizations, and offer reciprocity across agencies and across compliance regimes. FISMA can promote these efforts by encouraging agencies to leverage automation to assist with their compliance and monitoring

effors as well as by encouraging government-wide compliance programs to better enable and encourage reuse across agencies and compliance programs.

4. Effectively Budget for Cybersecurity and Investing in Risk Management

One of the perennial challenges that agencies face when meeting security requirements is that of resources. Through FISMA reform, Congress has an opportunity to authorize changes that truly enhance agency security. Securing large enterprises, especially those that have legacy technology and modernization backlogs, can be expensive. Congress must encourage agencies to budget for technology and services that can effectively buy down the risks to their environments. As agencies continue to modernize their systems, they should pivot their cybersecurity spend to move towards tools and services that enable implementation of a zero trust strategy and effectively reduce their risk picture. FISMA should authorize the necessary resources, including revolving funds and flexible color of money, to meet the dynamic threat landscape facing departments and agencies while also encouraging those organizations to smartly prioritize their resources in order to efficiently reduce the greatest risks to their environments.

Currently, the government collects its budgeting data through legacy processes that are inaccurate and incomplete, such as the Capital Planning and Investment Control (CPIC) process authorized by the Clinger-Cohen Act. This process is antithetical to modern software development practices such as agile and human-centered design. Congress should consider updating the authorization language to allow for the effective understanding of where

cybersecurity funding and resources are allocated and spent, along with mandating alignment between the information technology leadership and the financial and mission leadership of an agency. This would enable agencies to budget for and to buy down risks to their enterprises more accurately and efficiently while taking advantage of the full suite of flexibilities that have become law in recent years.

5. Modernize and Standardize Cybersecurity Performance Metrics and Measurements

As agencies adopt modern technology, move to cloud-based environments, and migrate to zero trust architectures, oversight entities must also modernize the measurements used to track agency progress and measure security. Leveraging automation and continuous monitoring can provide agencies such as OMB, GSA, and CISA with a much deeper understanding of the federal government's security posture.

Additionally, a revised FISMA should direct OMB and CISA to modernize the FISMA metrics that agencies currently collect to build their reports. Successful cybersecurity can only be understood and tracked by measuring outcomes; and those outcome-driven, risk-based metrics must be consistent across the various oversight entities. Key oversight stakeholders that must be on board with a continuous monitoring posture are the Council of Inspectors General on Integrity and Efficiency (CIGIE) and the Government Accountability Office (GAO), both of which are more used to annual, check-the-box FISMA exercises that do not yield higher security. A revamped FISMA can direct these oversight organizations to work with OMB and CISA to define

new metrics that capture security outcomes as agencies work to modernize their approaches to enterprise technology and security.

Conclusion

In conclusion, ADI supports the efforts of the committee to modernize the government's approach to security and better equip our federal partners to protect against and quickly recover from significant cybersecurity threats. We are encouraged by the committee's work on reforming FISMA and support efforts by the committee to clarify roles and responsibilities for federal cybersecurity, address incident and vulnerability response processes, promote technology and security modernization, authorize necessary security resourcing, and update the government's approach to understanding its security posture.

We encourage Congress to provide federal agencies with resources to meet overall government-wide cybersecurity challenges, including the necessary funding to implement key elements of the President's May 12, 2021 cybersecurity executive order and other congressional and administrative cybersecurity requirements. Further, ADI believes that a reauthorization of FIMSA should be the start of efforts to update other foundational information technology laws to better enable modernization, enhance security, and drive true government-wide digital innovation. Now, more than ever, we need public sector institutions to embrace the digital innovations that America's commercial technology companies can provide. Whether the mission involves protecting our homeland or providing benefits to those who

need them most, such innovative technologies will better enable government agencies to continue to deliver critical services to our increasingly digital and interconnected country.

ADI appreciates this opportunity to participate in today's hearing and share our insights on improving and modernizing our government's approach to security.