ITI Promoting Innovation Worldwide

Testimony of

Gordon Bitko
Senior Vice President of Policy
Information Technology Industry Council (ITI)

before the

Committee on Oversight and Reform
United States House of Representatives

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

Tuesday, January 11, 2022

Gordon Bitko
Senior Vice President of Policy
Information Technology Industry Council (ITI)

before the

Committee on Oversight and Reform
United States House of Representatives

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

Tuesday, January 11, 2022

Chairwoman Maloney, Ranking Member Comer, and distinguished Members of the Committee. Thank you for inviting me to testify today on an issue as important as federal cybersecurity. My name is Gordon Bitko, and I am the Senior Vice President for Public Sector Policy at ITI, the Information Technology Industry Council. I have been in my current role since November 2019. Prior to that, I served more than 12 years at the Federal Bureau of Investigation (FBI) and was honored to conclude my career as the FBI's Chief Information Officer (CIO), a position in which I served for three and a half years. Additionally, I have worked on technology policy issues at the RAND Corporation and as an engineer and engineering manager at both large and small technology companies. These experiences have made me acutely aware of the challenges and opportunities confronting federal IT and cybersecurity.

Today, at ITI, I work with key policymakers in the United States and globally, on behalf of 80 of the world's leading information technology (IT) and cybersecurity companies, to promote innovation and growth by empowering the public sector to embrace the best available technologies to accomplish agency missions, protect government IT systems and sensitive information, while serving constituents. We believe that in an increasingly digital world, it has never been more important for the United States Government to work together with industry to promote effective, reliable, and secure government services through technological leadership.

--

The COVID-driven shift to increased remote work has greatly escalated the importance of government and industry cooperation to ensure that cybersecurity is paramount for both the federal workforce and citizens who rely on online government services and rightly expect federal agencies to carry out their missions effectively and efficiently. Constantly evolving threats from all directions, coupled with increasing expectations from the public, requires the government to adopt policies that enable secure and rapid use of commercial and commercial off-the-shelf (COTS) products and services. By designing these policies with security in mind, the government can enable systems that are designed to respond to the enormous growth in demand for digital services and data.

2021 began with the federal government responding to the sophisticated SolarWinds supply-chain cyber-attack that is widely believed to be of a nation-state origin and, at the time, was deemed one of the most widespread and damaging cyber intrusions ever.

2022 begins with the federal government responding to another widespread vulnerability in a very commonly used piece of open-source software. So prevalent is that software—"Log4j"—that this vulnerability is one of the most significant in at least the past decade.

These major cyber events, taking place only about a year apart, bookend multiple significant cyber-attacks on critical industries, service providers, the defense industrial base, and governments around the world. Cyber-attacks have become so commonplace that increasingly, there is usually a collective response only to the most harmful and attention-grabbing incidents, and almost only when such cases impose a significant cost to individuals, companies, or governments. But federal cybersecurity cannot be something that we only pay attention to after the highest profile failures. For too long there has been far too much emphasis on what follows a breach and the consequences of dealing with compromised data and operations, instead of actively mitigating risks to prevent cyber attacks in the first place.

Encouragingly, the federal government's response to the Log4j vulnerability so far has shown evidence of improvement, as compared to the response to SolarWinds; particularly with more rapid and effective sharing of information and shorter timelines for mitigation. Yet, regular Government Accountability Office (GAO) and Inspectors General (IG) findings have continued to show that agencies struggle to comply with existing requirements and the rapid evolution of the federal workplace to support increased and regular telework that, without updated systems, tools, resources, and approaches, will continue to put government IT systems, operations, and personal or sensitive data at risk.

Many federal agencies' struggles with cybersecurity can be attributed to the nature of the current Federal Information Security Management Act (FISMA) and, in particular, three issues related to it:

1) *The existing law's focus on inputs and compliance with planning requirements and process, rather than outcomes.* In its current form, FISMA requires careful adherence to procedure and outputs like detailed inventories of systems, the use of approved security controls to protect information, and annual reports on the state of agency programs. But it has few direct provisions to actually evaluate and assess the effectiveness of those security measures in real time, and therefore does not promote real risk management.
2) *FISMA's requirements that create duplication of effort across agencies.* FISMA requires each agency to develop its own information security programs with no incentive for leveraging shared services or accepting security assessments or best practices from other agencies. This leads to significant duplication of effort across agencies, as agency security officials are frequently unable or unwilling to leverage work done elsewhere in the government.
3) *A lack of comprehensive real-time information under the current FISMA.* Too much information collection across agencies is provided through manual processes, annual updates, and in accordance with agency specific interpretations or definitions. As a result, it is nearly impossible for CISA or OMB to obtain a clear and timely view of the state of information security across the whole of the federal enterprise, because so much work must go into managing the existing data and reports in very manual and inefficient ways. At the same time, the lack of standardization and inconsistent definitions makes cross agency re-use of information, such as what could be included in a security assessment, difficult to accomplish.

--

Constantly evolving threats necessitate a dynamic cybersecurity program that can adapt and should be evaluated based on how effective it is. Any modernized federal cybersecurity legislation must be vastly more adaptable, facilitate better collaboration and security across-government, all while enabling standardized and high-quality ongoing assessments of agency cyber risk management resulting in government agencies that are constantly aware of and accounting for cyber risks at all levels and in real-time. That awareness and better collaboration and communication, in turn, will enable federal network defenders and CISA to have a much more comprehensive view of the federal IT infrastructure as a whole, thereby enabling more cohesive and better defended networks and systems. At the same time, effective risk management should drive a better balance between proactive and preventative efforts, including hunting and risk mitigation, and after-the-fact incident response and recovery. Historically, a disproportionate emphasis has been placed on the latter when the former is better suited to prevent future cyber breaches, and both are important components of an effective cybersecurity program.

Achieving these objectives in totality will involve a process that requires legislative as well as administrative and cultural changes to implement numerous specific reforms. The federal government has made initial progress with the release of Executive Order 14028, entitled Improving the Nation's Cybersecurity, and the Office of Management and Budget (OMB) Memorandum M-22-05: Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements. Still, there is much more work that must be done.

Modernization of the foundational legislation that provides authorities, gives direction, sets requirements, establishes oversight, and orients resources is central to the success of future federal cybersecurity. Without a strong legislative foundation, the complexity of federal cybersecurity, the number of different stakeholders, and the constant need for those stakeholders to be dealing with ongoing urgent threats suggests that piecemeal reform would be accomplished too slowly and could encounter real resistance and lack of buy-in from the existing security infrastructure and silos of responsibility for security dotted across the federal government landscape.

I appreciate the opportunity to appear before the Committee today to highlight some of the most important changes that should be reflected in any legislative update of FISMA or associated federal cybersecurity policies and frameworks. I offer the following recommendations for your consideration, which I am convinced are needed to ensure any reforms to FISMA are set up for success:

A) Promote a risk-based approach with a focus on outcomes;
B) Establish formal processes to promote the reciprocity of security reviews across government, focusing on accepting previously developed evidence supporting the system authorization process;
C) Ensure additional alignment between security requirements for national security systems and non-national security systems;
D) Ensure consistency through a holistic, governmentwide approach to updating FISMA in line with other federal cybersecurity frameworks, including drawing on best practices and lessons learned from private industry;
E) Drive automation of assessment processes, including adopting standardized information-sharing procedures across government; and
F) Improve audits of FISMA compliance through widespread and continuous monitoring.

These recommendations are discussed in further detail below. While no recommendations can offer ironclad protection against a novel incident such as Log4j or SolarWinds, these important measures are necessary to ensure that the government is well prepared to quickly identify and respond even in the worst cases, and not just against the wide range of known threats. These recommendations will help ensure agencies have a thorough understanding of their cyber risks and invest resources appropriately, increase confidence in the effectiveness of cyber defenses and cyber incident response preparations, and ensure that federal organizations coordinate and contribute effectively to the whole of the U.S. government's cybersecurity. As well, these principles help to guarantee that entities responsible for broader US government cybersecurity, especially the Cybersecurity and Infrastructure Security Agency (CISA), the National Cyber Director and the Office of Management and Budget, have the visibility they need, in real-time, into existing vulnerabilities and mitigating actions, without requiring laborious, time-consuming, and suboptimal manual data calls.

A) *Promote a risk-based approach with a focus on outcomes.*

The goal of any security framework should be to effectively manage risk as an outcome. Unfortunately, as presently written, FISMA does not measure outcomes, but focuses on outputs such as annual certifications and the existence of security plans. Routine requirements are often needed but are themselves far from sufficient to provide real insights into current risks.

FISMA must be reformed to better promote a risk-based approach in at least two ways. In so doing, it will help to erode cultures and processes that are more or even primarily focused on compliance "on paper" and "box checking" exercises over effectiveness. First, an improved FISMA should empower agencies to make risk-based decisions, including about leveraging new technology, while also enabling them to meaningfully leverage compliance, evaluation, or authorization documentation from other federal assessments. Second, it should help agencies strengthen their approach to the foundational steps of risk assessment and prioritize risk management activities. The law ought to establish requirements and processes that clarify how agencies can use the Risk Management Framework (RMF) and the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST), building on and enforcing implementation of the guidance issued in Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

FISMA should promote outcomes-focused security baselines (i.e., allowing flexibility in the application of security controls as long as a required result or security posture is achieved) while also recognizing the value of more prescriptive controls guidance. It should enable agencies to establish processes that make appropriate use of both outcomes and prescriptive controls, depending on agency needs and the nature of particular security threats. Baselines that are outcomes-focused enable greater flexibility and innovation in an agency's security approach and are critical to supporting agencies' use of state-of-art security services and capabilities. Alternatively, well-developed prescriptive approaches, such as the zero-trust guidance in EO 14028: Executive Order on Improving the Nation's Cybersecurity, articulate specific steps that information security practitioners can use to achieve a desired security outcome. A reformed FISMA needs to enable an information security program that accounts for both approaches.

B) *Establish formal processes to promote the reciprocity of security reviews across government, focusing on accepting previously developed evidence supporting the system authorization process.*

Some of the most significant challenges with FISMA are the lack of statutorily required reciprocity of existing authorizations between agencies and the absence of information-sharing related to cybersecurity performance across the federal government. For example, contractors providing the same product or service to multiple agencies must currently support multiple System Security Plans (SSPs) and receive numerous authorizations to operate (ATOs). Requirements for developing, documenting, and sharing the body of evidence leading to an ATO may differ based on the preference or experience of each agency's authorizing official (AO), which too often leads to confusion and redundant efforts for contractors. Standard quality assurance requirements and mechanisms for sharing documented results will help address reluctance about and barriers to interagency adoption of SSPs while enabling easier sharing across agencies.

Privacy controls are another area in which unnecessary duplicative efforts currently exist. For systems containing Personally Identifiable Information (PII), ISSOs participate in separate Privacy Impact Assessments (PIAs), based on requirements in the Privacy Act and the E-Government Act. This is despite many privacy controls already being documented in the SSPs, resulting in unnecessary and duplicative paperwork.

FISMA should be reformed to maximize the incentives for agency CIOs and AOs to evaluate and accept existing bodies of evidence, previously developed by other agencies, to support their own risk-based decisions. Incentives could include faster approvals based on reduced documentation and better information exchange, and could also be extended to budgetary benefits, such as providing additional Working Capital Fund investments or eliminating Technology Modernization Fund (TMF) payback requirements for projects funded through the TMF. Further in the future, this incentive may be used to reward agencies that have demonstrated maturity in tangential areas like cyber supply chain risk management (C-SCRM). The Office of Management and Budget (OMB) could also consider adding an assessment of agencies' information-sharing and use of shared risk-based decisions as part of its regular PortfolioStat reviews.

Wherever additional security controls are required that exceed standard baselines (e.g., due to a unique configuration of a common product), agency CIOs and AOs should be required to justify the additional control layers and accreditation requirements.

C) *Ensure additional alignment between security requirements for national security systems and non-national security systems.*

The security requirements applicable to FISMA-reportable systems versus those for national security systems are ambiguous and frequently interpreted differently across the government. This results in the inconsistent application of FISMA security requirements and controls across national security systems and non-national security systems, which in turn weakens agencies' security posture. FISMA should be reformed to streamline and clarify security requirements for each class of systems, including more precise criteria for designating systems as FISMA-reportable.

D) *Ensure consistency through a holistic, government-wide approach to updating FISMA in line with other federal cybersecurity frameworks, including drawing on best practices and lessons learned from private industry.*

FISMA reform must not be considered within a vacuum, but must align with other cybersecurity requirements, such as those enumerated by EO 14028. FISMA reform efforts should also take into account existing industry best practices, rather than unnecessarily creating new and conflicting requirements that will fragment the cybersecurity landscape between the public and private sectors to a greater extent. This includes alignment of proposed FISMA requirements in areas such as incident reporting, vulnerability disclosure and threat intelligence sharing.

E) *Drive automation of assessment processes, including adopting standardized information-sharing procedures across government.*

Effective cybersecurity policy implementation and any reforms to FISMA should include a mandate that SSP information and status of security control deployment be shared within the federal government. This will require agencies to shift from manual documentation of controls to automated, machine-readable formats that can be easily exchanged and evaluated for reuse. Presently, the implementation and continuous monitoring of security controls are often represented in non-replicable formats that require data conversion and manual effort to produce meaningful insights.

Improvements to FISMA ought to require a standardized framework that can be applied to information systems throughout government to document and continuously assess the effectiveness of security measures (controls) in preventing or minimizing risk. By moving security controls and control baselines from a text-based and manual approach (e.g., using word processors or spreadsheets) to a set of standardized and machine-readable formats, security professionals will be able to automate security assessment, auditing, and continuous monitoring processes. Doing so will help to free up scarce federal personnel resources to better monitor, detect, and prevent cyber-attacks against government systems.

OMB is already working toward promoting the adoption of automation for federal reporting mechanisms. In memorandum M-22-05, the Federal Chief Information Security Officer (CISO) directs agencies to develop a strategy to collect and report performance data in an automated and machine-readable manner. Any modernized federal cybersecurity legislation should build on this important directive and provide additional clarity on the discrete requirements to ensure a standardized approach throughout the federal government.

F) *Improve audits of FISMA compliance through widespread and continuous monitoring.*

The FISMA audit process is in considerable need of reform. Currently, agency Inspectors General (IGs) assess FISMA compliance by performing annual audits of a small sample of systems. Unfortunately, this does not accurately reflect an agency's overall cybersecurity posture. Actual compliance should instead be assessed through a combination of a representative sampling of systems to facilitate evidence-based reviews, continuous monitoring and evaluation of agency IT systems on a large scale including independent vulnerability assessments, and actual penetration testing activities designed to test agency cybersecurity operations. Vulnerability scans should also consider the full cybersecurity profile of an agency, including legacy IT, and CIOs need to be allowed to make risk-based decisions about how and where to best mitigate cyber risks.

To facilitate these goals, agency IGs should be equipped to monitor systems on an ongoing basis, rather than conducting one-time "spot checks." IGs should hire technical staff who understand, from a technical perspective, the implementation of security controls at all stages of a system's lifecycle. Additionally, IGs should consider investing in software and other tools to perform continuous monitoring of systems.

Execution of these recommendations should be accompanied by necessary updates to the Federal Information Technology Acquisition Reform Act (FITARA) scorecard that measure and report on the key behaviors discussed already and ensure that Congress has appropriate visibility into the totality of the federal IT landscape, including an increased emphasis on cybersecurity.

--

The federal government must modernize its existing cybersecurity frameworks to respond to today's dynamic threat landscape. The federal government should take additional steps to promote and codify a consistent cybersecurity strategy that is built around risk management, process automation, and inter-agency cooperation. This will enable the government to deliver more secure services to its constituents and raise the United States' level of preparedness to respond to global threats.

Thank you again for inviting me, and I look forward to your questions.