Testimony of Renee P. Wynn

Chief Executive Officer of RP Wynn Consulting, LLC

FOR A HEARING ON

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

BEFORE THE

House of Representatives

Committee on Oversight and Reform

January 11, 2022

Washington, D.C.

Good morning, Chairwoman Maloney, Ranking Member Comer, and distinguished members of the Committee. I am honored to testify today on the importance of cybersecurity to examine the dramatic transformation of the cyberthreat landscape since the Federal Information Security Modernization Act was created and updated. Now is the ideal time to update this premier cybersecurity law to meet the evolving cyberthreats.

The original Act, Federal Information Security Management Act (FISMA) of 2002 set the US federal government on a path to strengthen its approach to information security. A bold and necessary move by Congress. The Act recognized the importance of information security to our economic and national security interests and the importance of protecting individuals' data. This Act required each agency to develop, document and implement a program to provide security for the information and systems that support their operations and assets, including those provided or managed by another agency, contractor, or other sources. [1] Agencies were slow to implement this Act and thus leading to major cyber-security incidents, including the infamous OPM breach of June of 2015. It took this event and ensuing crisis to truly get the US federal agencies to act.

Congress felt compelled to update the FISMA of 2002 through the Federal Information Security Modernization Act of 2014 to address the rapidly evolving information security landscape. The modification included the use of continuous monitoring in systems, focused reporting on areas that could be used to gain access into networks and pushed for additional changes in federal government policy to focus on risk-based policy for cost-effective security.

Continuing to upgrade information security laws, regulations and policies for the US federal government is a must if we are to maintain our economic position in the world and national security. As Congress contemplates a refresh, I urge you to continue a risk-based approach that emphasizes all types of technology: Information Technology (IT), Operational Technology (OT) and the fastest growing segment, Internet of Things (IoT). All these elements of technology are used by the federal government to improve mission effectiveness, efficiencies, and the customer experience.

Examples of each type of technology are as follows:

- Information Technology: personal computers, computer networks, mobile phones
- Operational Technology: HVAC units, refrigerators, cars
- Internet of Things: Amazon Echo, Google Home, Apple Watch, home security systems

The elements of technology have information security vulnerabilities that present risk to the user and the US federal government. The risks are compounded when the devices are interconnected; thus, information security laws must be updated to address and anticipate the risks posed by the devices and their interconnected nature.

[1] National Institute of Standards: FISMA Overview, csrc.nist.gov.

FISMA Success Factors

There are numerous US federal government successes in implementing FISMA. The success factors are establishing a risk framework, adopting metrics aligned with that framework and implementing culture changes. The framework and supporting metrics gave Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) a way to discuss information security risks and progress against the risks with mission and mission support elements of Departments and Agencies. The metrics created accountability as well as the ability to hold effective Congressional hearings on how well Departments and Agencies were doing to address information security risks. The hearings, in some cases, were a wake-up call for the heads of Departments and Agencies so the "tone at the top" began to sway towards making information security a top enterprise risk. All these factors began to take hold, and previously neglected information security risks were begining to be addressed.

There is another success factor that contributed greatly to understanding information security risks across the US federal government: the Continuous Diagnostic and Mitigation (CDM) program. The CDM program provides cybersecurity tools, integration services and dashboards to participating Agencies to support them in improving their respective cybersecurity posture.[2] For many CIOs and CISOs, CDM implementation was a path forward, the only one for many, to identify and address information security risks. They were able to begin answering two key and basic questions: who and what are on our networks? This can be simultaneously frightening and energizing. CDM gave a first peak at what was truly happening on federal government networks.

The work to address information security is never done and thus an evolution of FISMA is both natural and needed.

FISMA Improvements

Government worker and contractors who contribute to addressing cybersecurity risks should be lauded for the success of FISMA to date. They led the way to protect our national security and economic stability from cyberthreats.

As Congress contemplates the next iteration of FISMA, there are several areas ripe for consideration: cyber aspects of supply chain risk management, internet of things, and the interconnectivity of government operations.

The next iteration of FISMA should include provisions on addressing the cyber risks posed through the information and communications technology (ICT) supply chain used by the federal government. US federal government operations are dependent upon ICT solutions for mission and mission support delivery. To this end, the US government must assess the potential risk posed through the ICT supply chain prior to purchasing and deploying on federal networks. There are well-resourced nation state cyber threat actors that intentionally target all tiers of the ICT supply chain by imbedding malicious functionality. Adding to this risk is the fact that most US

[2] https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_CDM%20Program%20Overview_Fact%20Sheet_1.pdf

government procurements are public and open, and are thus more vulnerable to nation states because they know what to target. These attacks are often sophisticated and difficult to detect. [3]

The advent of technological advances provides opportunities for government operations to be more effective and efficient. These advances also increase complexity and risk, including cybersecurity risk. The growth of telehealth and use of internet of things medical devices (for example blood pressure cuffs, scales, heart monitors) during the pandemic has allowed medical services to be delivered during a trying time, but they add risk. The next iteration of FISMA must mandate that the US federal government use secure IoT, especially for medical purposes. Mandates from law could accelerate the development of more secure IoT. Departments and Agencies should also report on the use of IoT and how it is being secured. These reports should not be made public because the more nation state threat actors know about federal operations; the operations become more vulnerable.

The US federal government relies upon networks and devices that are interconnected between Departments and Agencies. For example, there are only a few service centers for processing federal payments. Thus, every Department and Agency is connected to transmit payment data. These points of connection, if not properly upgraded, managed, and monitored, create greater cyber risk, including the easy transmission of malicious code amongst Departments and Agencies. Also, the data while in transit are at risk of compromise if poor cybersecurity practices are employed. A lack of attention to proper cybersecurity interconnectivity practices was a cause of the OPM breach in 2015. More and more government operations will be dependent upon cross-agency interconnectedness thus the laws must be updated to encompass this.

In addition to legislative changes, Congress must continue to hold the heads of Departments and Agencies accountable for addressing cybersecurity risks. This is about ensuring a culture attentive to cybersecurity risks. This doesn't require legislative changes. Simply, Congress can include cybersecurity questions during budget, authorization, and large program hearings. Some questions for consideration are as follows: What are your biggest cybersecurity risks and what are you doing to mitigate them? Are they included in your enterprise risk management or program management strategies? What critical systems are being modernized? What's the status of modernization? Congress has a role in advancing the federal government's culture of cybersecurity through accountability.

Conclusion

The US federal government's adoption of all types of technology has provided and will continue to provide opportunities to better serve the public. The adoption of technology adds complexity and risk, especially cyber risks. Congress must continue to ensure the nation's laws are updated to keep pace with the growing complexity and risk associated with technological advances.

[3] GAO-21-171, INFORMATION TECHNOLOGY: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks

Thank you for the opportunity to appear before the Committee today and testify on the changing cyberthreat landscape and modernizing FISMA to meet this challenge. I stand ready to answer your questions.