House Oversight and Reform Committee
Hybrid Public Hearing
Cybersecurity for the New Frontier: Reforming the Federal Information Security Management Act
Tuesday, January 11, 2022
10:00 a.m.

Opening Statement

Thank you, Chairwoman Maloney and Ranking Member Comer, for holding this important hearing. And thank you to all the witnesses for joining us today. I appreciate your contributions to improving FISMA.

Technology is ever evolving, and IT systems are inherently at risk and vulnerable to cyberattack. In 2002, FISMA became law, requiring each federal agency to put an agency-wide program in place to ensure the security of its information and systems. Since the enactment of this legislation in 2002 and a subsequent update in 2014, the cyberthreat landscape has transformed remarkably.

The slew of harmful cyberattacks have exposed vulnerabilities and revealed some of the flaws in our existing law. The fact that DarkSide, a cybercrime group with Russian ties, was able to force the Colonial Pipeline Company to shut down the largest pipeline in the United States, is a threat to our national security.

In September of 2020, the Ashtabula County Medical Center, a northeast Ohio hospital, spent more than a week offline after being hit by a cyberattack. Just a few months ago, Southern Ohio Medical Center, another hospital in my home state, suffered a cyberattack that resulted in continued cancellations of patient appointments a week later. These attacks are deeply concerning because they have profound impact on the lives of real people in addition to our national security.

I thank the Chairwoman and Ranking Member for working to address emerging cyber threats and finding ways to better protect our cyber infrastructure, and I look forward to making positive changes to FISMA that create a clear, coordinated, and holistic approach to federal information security to meet the ever-changing cyber frontier.

Questions Section

The bipartisan draft legislation reforming FISMA clearly acknowledges the need for continuous risk monitoring by establishing layers of assessments to be conducted by the primary entities responsible for governmentwide cybersecurity, as well as our individual agencies.

It also amends the frequency of risk assessment reports and the elements they must include.

Questions for Ms. Jennifer Franks (Director of Information Technology and Cybersecurity, GAO):

Ms. Franks, let me ask you what GAO is learning about the effectiveness of risk assessment metrics during its review of FISMA implementation.

1. How is the data that is incorporated into risk assessments currently collected and reported?

2. Does GAO have preliminary recommendations about how to improve coordination between government agencies responsible for ongoing risk assessment?

Questions for Ms. Renee Wynn (CEO, RP Wynn Consulting LLC; former CIO of NASA):

In the past, agencies have had to focus much of their time on making sure they are compliant with FISMA and other cybersecurity measures, which often means they focus *less* of their time on risk management.

I applaud the updated guidance on FISMA implementation that OMB released last month, which aims to shift the focus of FISMA assessments from compliance to actual, observable security outcomes.

The draft legislation that the Chairwoman and Ranking Member released today recognizes this shift by requiring ongoing and continuous risk assessments instead of periodic, point-in-time assessments.

1. Ms. Wynn, can you explain to us how performing risk assessments on a continuous basis will strengthen an agency's system security?

Optional Questions

Questions for Mr. Ross Nodurft (ED, Alliance for Digital Innovation)

The Chairwoman's draft legislation also calls for a pilot to test a risk-based budget model.

1. Mr. Nodurft, what is a risk-based budget model, and do you think a pilot program is the best way to assess its efficacy in the FISMA framework?