Bills to Help Small Businesses Prepare for Cyber Attacks Working Way Through Congress

By: Kevin D. Pomfret & Anthony H. Anikeeff

05.18.2017

On May 2, the U.S. House Committee on Science, Space, and Technology unanimously approved H.R. 2105, the ?NIST Small Business Cybersecurity Act of 2017.? The Senate Commerce, Science, and Transportation Committee reported favorably on a similar bill on April 5.

The legislation calls on the National Institute of Standards and Technology (NIST) to provide small businesses with guidance to help them identify, assess, manage, and reduce cybersecurity risks. Specifically, the legislation directs NIST, in consultation with other federal agencies, to disseminate clear and concise guidelines, tools, best practices, standards and methodologies, based on the NIST Framework for Improving Critical Infrastructure Cybersecurity, to help small businesses identify, assess, manage, and reduce their cybersecurity risks. These guidelines and best practices should be made available on government websites within a year of the enactment of the Act.

Over the past several years, businesses of all sizes have become targets of cyberattacks. As a result, there has been increased pressure on Congress for assistance. The initial NIST Framework for Improving Critical Infrastructure Cybersecurity referenced in the bill was published in February, 2014 (the ?Framework?). It was prepared in response to President Obama?s Executive Order 13636, ?Improving Critical Infrastructure Cybersecurity,? which was published on February 12, 2013. (Earlier this year NIST circulated a version 1.1 draft of the Framework; comments were due on April 10th).

Critics of the Framework believe that small and medium-sized businesses do not have the necessary resources or skills for risk-based analysis. It is unclear whether the proposed legislation will become law. And even if the legislation does become law, it will be some time before NIST publishes guidelines or best practices for small businesses. In the meantime, small businesses should review the Framework and Small Business Information Security: The Fundamentals published by NIST in November, 2016.

The need for guidance and assistance for small businesses engaged in government contracting as a

prime or subcontractor is particularly acute. Besides the inherent threat posed by cyber attacks, government contractors are required by contract to ensure that their information systems through which federal information not intended for public disclosure may pass or be stored complies with some 14 security criteria. The Defense Department is mandating compliance by December 31, 2017. In addition, contractors and subcontractors that maintain ?Covered Defense Information,? which includes various forms of controlled unclassified information, will face similar security requirements. Although the government considers NIST-like standards to be prudent business practices, smaller businesses are struggling to understand, implement and stay current in this evolving area.

Related People

- Anthony H. Anikeeff ? 703.760.5206 ? aanikeeff@williamsmullen.com
- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity