Committee on Science, Space, and Technology
H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017
Introduced by Rep. Ralph Abraham
Cosponsored by Chairman Smith, Vice-Chairman Lucas, Chairwoman Comstock and Rep. Knight

Background

Over the course of the 114th Session of Congress, the House Science, Space, and Technology Committee held a dozen hearings related to Federal cybersecurity issues based on its jurisdiction over the National Institute of Standards and Technology (NIST). The hearings included examination of data breaches at the Office of Personnel Management (OPM), the Internal Revenue Service (IRS), and the Federal Deposit Insurance Corporation (FDIC).

On February 14, 2017, the Research and Technology Subcommittee held a hearing titled, "Strengthening U.S. Cybersecurity Capabilities." Witness testimony included a review and discussion of recommendations provided by two recent reports: the *Report on Securing and Growing the Digital Economy* published by the Commission on Enhancing National Cybersecurity in December 2016, and *From Awareness to Action – A Cybersecurity Agenda for the 45th President*, published by the Center for Strategic and International Studies (CSIS) in January 2017.

These hearings underscore the immediate need for a vigorous approach to protecting U.S. cybersecurity capabilities. H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, implements key ideas to help strengthen Federal government cybersecurity.

Summary of Major Provisions

- **MISSION** -- Amends NIST's mission for developing standards and guidelines for information systems to emphasize the principle that expanding cyber threats require the engineering of security from the beginning of an information system's life cycle through building more trustworthy and secure components.
- **GUIDANCE** -- Promotes the implementation of the NIST *Framework for Improving Critical Infrastructure Cybersecurity (Framework)* by providing guidance that Federal agencies may use to incorporate the Framework into their information security risk management efforts.
- **FEDERAL WORKING GROUP** -- Establishes a Federal working group to develop outcome-based and quantifiable metrics to help Federal agencies analyze and assess the effectiveness of the Framework in protecting their information and information systems. Compiles information from Federal agencies for an Office of Management and Budget and Office of Science and Technology Policy (OSTP) report.
- **PUBLIC-PRIVATE WORKING GROUP** -- Establishes a public-private working group, in coordination with industry stakeholders, to develop specific Framework implementation models and measurement tools that private entities can use to adopt the Framework. The group shall also develop industry-led consensus and outcome-based metrics that quantify the effectiveness and benefits of the Framework to enable private entities to voluntarily analyze and assess their individual corporate cybersecurity risks. Further, the public-private working group shall compile information voluntarily submitted by private entities on their use of the Framework and on the effectiveness and benefits of such use. Compiles the voluntarily provided information for an OSTP report.
- **ASSESSMENT** -- Directs NIST to complete an initial assessment of the cybersecurity preparedness of priority Federal agencies.
- **AUDITS** -- Directs NIST to initiate individual cybersecurity audits of priority Federal agencies to determine the extent to which each agency is meeting the information security standards developed by the Institute.
- **SCHEDULE** -- Directs NIST to establish a schedule such that priority agencies whose information security risk is high shall have audits completed not later than one year after the bill's enactment into law, and then annually thereafter. Priority agencies that do not fall into this category shall have the initial audit completed not later than two years after the bill's enactment, and then biennially thereafter.
- **FRAMEWORK** -- If agencies are required by law or Executive Order to implement the Framework, then the NIST audits of each Federal agency shall be based on the guidance it provides to agencies (described above) and the metrics developed by the Federal working group (described above).
- **AUDIT REPORT** -- A report of each audit shall be transmitted to the Office of Management and Budget, OSTP, the U.S. Government Accountability Office, the agency being audited, the agency's Office of Inspector General if it has one, and Congress, including the House Science, Space, and Technology Committee and the Senate Committee on Commerce, Science, and Transportation.