SECTION BY SECTION

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

Sec. 1. Short Title
This section establishes the short title of the bill as the "NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017."

Sec. 2. NIST Mission to Address Cybersecurity Threats.
This section amends NIST's mission under the Computer Standards Program (15 USC 278g-3(a)(1)). It directs the Institute to emphasize the principle that expanding cybersecurity threats require the engineering of security from the beginning of an information system's life cycle through building more trustworthy and secure components, and by applying well-defined security design principles throughout the system's life span.

Sec. 3. Implementation of Cybersecurity Framework.
This section creates two new sections in the NIST statute:

Sec. 20A – Framework for Improving Critical Infrastructure Cybersecurity (Framework):

> MISSION AND GUIDANCE -- Promotes the implementation of the Framework by providing guidance that Federal agencies may use to incorporate the Framework into their information security risk management efforts, including compliance with the Federal Information Security Modernization Act (44 USC 35), and any other applicable Federal law. The guidance shall be provided to the Office of Management and Budget (OMB), the Office of Science and Technology Policy (OSTP), and all other Federal agencies within 6 months of the bill's enactment, and then updated as necessary.
>
> FEDERAL WORKING GROUP -- Creates a Federal working group, established and chaired by NIST, to develop outcome-based and quantifiable metrics, updated as necessary, to help Federal agencies analyze and assess the effectiveness of the Framework in protecting their information and information systems. The Federal working group will develop these metrics in coordination with the public-private working group described below. The Federal working group shall be established within 3 months of the bill's enactment, and the metrics not later than 6 months after the bill's enactment. The Federal working group shall also compile information from Federal agencies on their use of the Framework and results of their analysis and assessment, which shall be published in an annual report by OMB and OSTP.
>
> PUBLIC-PRIVATE WORKING GROUP -- Creates a public-private working group, established by NIST, in coordination with industry stakeholders, to develop specific Framework implementation models and measurement tools, updated as necessary, that private entities can use to adopt the Framework. The public-private working group shall also develop industry-led consensus and outcome-based metrics, updated as necessary, that quantify the effectiveness and benefits of the Framework to enable private entities to

voluntarily analyze and assess their individual corporate cybersecurity risks. The public-private working group will develop these metrics in coordination with the Federal working group described above. The public-private working group shall be established within six months of the bill's enactment, and the models and measurement tools, as well as the metrics, shall be developed not later than one year after the bill's enactment. 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. This information will help NIST make improvements to the Framework and assist private entities to better understand the benefits of the Framework so they use it more effectively. The compiled information shall be published in an annual report by OSTP.

SEC. 20B. Cybersecurity Audits:

ASSESSMENT -- Directs NIST to complete an initial assessment of the cybersecurity preparedness of the 24 CFO-Act Federal agencies, and any other Federal agencies that have reported a major cybersecurity incident, based on the information security standards developed by NIST, not later than 6 months after the bill's enactment into law. This assessment may also be informed by work done or reports published by other Federal agencies or officials.

AUDITS -- Not later than six months after the bill's enactment into law, directs the Institute to initiate individual cybersecurity audits of each agency covered under the initial group assessment 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 for these audits based on the initial assessment. 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. Agencies that do not fall into this category shall have the initial audit completed no later than two years after the bill's enactment, and then biennially thereafter.

RELATION TO FRAMEWORK -- If Federal agencies are required by law or Executive Order to implement the Framework, then the NIST audits of each 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 Federal agency audit shall be transmitted to OMB, 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.