.....

(Original Signature of Member)

115TH CONGRESS
1ST SESSION

H. R. _____

To amend the National Institute of Standards and Technology Act to implement a framework, assessment, and audits for improving United States cybersecurity.

IN THE HOUSE OF REPRESENTATIVES

Mr. ABRAHAM introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the National Institute of Standards and Technology Act to implement a framework, assessment, and audits for improving United States cybersecurity.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017''.

SEC. 2. NIST MISSION TO ADDRESS CYBERSECURITY THREATS.

Section 20(a)(1) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(1)) is amended by inserting '', emphasizing the principle that expanding cybersecurity threats require engineering security from the beginning of an information system's life cycle, building more trustworthy and secure components and systems from the start, and applying well-defined security design principles throughout'' before the semicolon.

SEC. 3. IMPLEMENTATION OF CYBERSECURITY FRAMEWORK.

The National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) is amended by inserting after section 20 the following:

''SEC. 20A. FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY.

''(a) IMPLEMENTATION BY FEDERAL AGENCIES.—

''(1) IN GENERAL.—The Institute shall promote the implementation by Federal agencies of the Framework for Improving Critical Infrastructure Cybersecurity (in this section and section 20B referred to as the 'Framework') by providing to the Office of Management and Budget, the Office of Science and Technology Policy, and all other Federal agencies, not later than 6 months after the date of

enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, guidance that Federal agencies may use to incorporate the Framework into their information security risk management efforts, including practices related to compliance with chapter 35 of title 44, United States Code, and any other applicable Federal law.

''(2) GUIDANCE.—The guidance required under paragraph (1) shall—

''(A) describe how the Framework aligns with or augments existing agency practices related to compliance with chapter 35 of title 44, United States Code, and any other applicable Federal law;

''(B) identify any areas of conflict or overlap between the Framework and existing cybersecurity requirements, including gap areas where additional policies, standards, guidelines, or programs may be needed to encourage Federal agencies to use the Framework and improve the ability of Federal agencies to manage cybersecurity risk;

''(C) include a template for Federal agencies on how to use the Framework, and recommend procedures for streamlining and har-

monizing existing and future cybersecurity-related requirements, in support of the goal of using the Framework to supplant Federal agency practices in compliance with chapter 35 of title 44, United States Code;

''(D) recommend other procedures for compliance with cybersecurity reporting, oversight, and policy review and creation requirements under such chapter 35 and any other applicable Federal law; and

''(E) be updated, as the Institute considers necessary, to reflect what the Institute learns from ongoing research, the audits conducted pursuant to section 20B(b), the information compiled by the Federal working group established pursuant to paragraph (3), the information compiled by the public-private working group established pursuant to subsection (b)(1), the annual reports published pursuant to paragraph (4), and the annual reports published pursuant to subsection (b)(2).

''(3) FEDERAL WORKING GROUP.—Not later than 3 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall establish

and chair a working group (in this section referred to as the 'Federal working group'), including representatives of the Office of Science and Technology Policy and other appropriate Federal agencies, which shall—

''(A) not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, develop outcome-based and quantifiable metrics, in coordination with the public-private working group established pursuant to subsection (b), to help Federal agencies in their analysis and assessment of the effectiveness of the Framework in protecting their information and information systems;

''(B) update such metrics as the Federal working group considers necessary;

''(C) compile information from Federal agencies on their use of the Framework and the results of the analysis and assessment described in subparagraph (A); and

''(D) assist the Office of Science and Technology Policy in publishing the annual report required under paragraph (4).

''(4) REPORT.—The Office of Science and Technology Policy shall develop and make publicly available an annual report on agency adoption rates and the effectiveness of the Framework. In preparing such report, the Office shall use the information compiled by the Federal working group pursuant to paragraph (3)(C).

''(b) IMPLEMENTATION BY PRIVATE ENTITIES.—

''(1) PUBLIC-PRIVATE WORKING GROUP.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall, in coordination with industry stakeholders, establish a working group (in this section referred to as the 'public-private working group') which shall—

''(A) not later than 1 year after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, develop specific Framework implementation models and measurement tools that private entities can use to adopt the Framework;

''(B) not later than 1 year after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, develop, in coordination with the Federal

working group, 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;

''(C) update the models and tools developed pursuant to subparagraph (A) and the metrics developed pursuant to subparagraph (B), as the public-private working group considers necessary;

''(D) compile information, derived from the metrics developed pursuant to subparagraph (B), voluntarily submitted by private entities on their use of the Framework and on the effectiveness and benefits of such use;

''(E) analyze the information compiled pursuant to subparagraph (D) and provide such information and analysis to—

''(i) the Institute, for the purpose of enabling the Institute to make improvements to the Framework; and

''(ii) private entities, for the purpose of providing such entities with a greater understanding of the benefits of the

Framework to enable them to use the Framework more effectively to improve their cybersecurity; and

''(F) assist the Office of Science and Technology Policy in publishing the annual report required under paragraph (2).

''(2) REPORT.—The Office of Science and Technology Policy shall develop and make publicly available an annual report on industry adoption rates and the effectiveness of the Framework. In preparing such report, the Office shall use information compiled by the public-private working group pursuant to paragraph (1)(D).

''SEC. 20B. CYBERSECURITY AUDITS.

''(a) INITIAL ASSESSMENT.—

''(1) REQUIREMENT.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall complete an initial assessment of the cybersecurity preparedness of the agencies described in paragraph (2). Such assessment shall be based on information security standards developed under section 20, and may also be informed by work done or reports published by other Federal agencies or officials.

''(2) AGENCIES.—The agencies referred to in paragraph (1) are the agencies referred to in section 901(b) of title 31, United States Code, and any other agency that has reported a major incident (as defined in the Office of Management and Budget Memorandum—16—03, published on October 30, 2015, or any successor document).

''(3) NATIONAL SECURITY SYSTEMS.—The requirement under paragraph (1) shall not apply to national security systems (as defined in section 3552(b) of title 44, United States Code).

''(b) AUDITS.—

''(1) REQUIREMENT.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, the Institute shall initiate an individual cybersecurity audit of each agency described in subsection (a)(2), to assess the extent to which the agency is meeting the information security standards developed under section 20.

''(2) RELATION TO FRAMEWORK.—Audits conducted under this subsection shall—

''(A) to the extent applicable and available, be informed by the report on agency adoption

rates and the effectiveness of the Framework described in section 20A(a)(4); and

''(B) if the agency is required by law or executive order to adopt the Framework, be based on the guidance described in section 20A(a)(2) and metrics developed under section 20A(a)(3)(A).

''(3) SCHEDULE.—The Institute shall establish a schedule for completion of audits under this subsection to ensure that—

''(A) audits of agencies whose information security risk is high, based on the assessment conducted under subsection (a), are completed not later than 1 year after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, and are audited annually thereafter; and

''(B) audits of all other agencies described in subsection (a)(2) are completed not later than 2 years after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, and are audited biennially thereafter.

''(4) REPORT.—A report of each audit conducted under this subsection shall be transmitted by the Institute to—

''(A) the Office of Management and Budget;

''(B) the Office of Science and Technology Policy;

''(C) the Government Accountability Office;

''(D) the agency being audited;

''(E) the Inspector General of such agency, if there is one; and

''(F) Congress, including the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.''.