Proposed modification of

115TH CONGRESS
1ST SESSION

H. R. 1224

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

FEBRUARY 27, 2017

Mr. ABRAHAM (for himself, Mr. SMITH of Texas, Mr. LUCAS, Mrs. COMSTOCK, and Mr. KNIGHT) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

---

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".

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.—The Institute shall promote the implementation by Federal agencies of the Framework for Improving Critical Infrastructure Cybersecurity (in this section 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, guid-

ance 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.

"(b) GUIDANCE.—The guidance required under subsection (a) shall—

"(1) 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;

"(2) 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;

"(3) include a template for Federal agencies on how to use the Framework, and recommend procedures for streamlining and harmonizing existing and future cybersecurity-related requirements, in support of the goal of using the Framework to supplement Federal agency practices in compliance with chapter 35 of title 44, United States Code;

"(4) 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

"(5) be updated, as the Institute considers necessary, to reflect what the Institute learns from ongoing research, evaluations, and audits or analytical examinations conducted pursuant to section 3555 of title 44, United States Code, the information compiled by the Federal working group established pursuant to subsection (c), and the annual reports published pursuant to subsection (d).

"(c) FEDERAL WORKING GROUP.—Not later than 3 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act, 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 Management and Budget, the Office of Science and Technology Policy, and other appropriate Federal agencies, which shall—

"(1) not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act, develop outcome-based and quantifiable metrics to help Federal agen-

cies in their analysis and assessment of the effectiveness of the Framework in protecting their information and information systems;

"(2) update such metrics as the Federal working group considers necessary;

"(3) compile information from Federal agencies on their use of the Framework and the results of the analysis and assessment described in paragraph (1); and

"(4) assist the Office of Management and Budget and the Office of Science and Technology Policy in publishing the annual report required under subsection (d).

"(d) REPORT.—The Office of Management and Budget and 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 Offices shall use the information compiled by the Federal working group pursuant to subsection (c)(3).

"SEC. 20B. CYBERSECURITY ASSESSMENT.

"(a) IN GENERAL.—Not later than 6 months after the date of enactment of the NIST Cybersecurity Framework, Assessment, and Auditing Act, the Institute shall complete an initial assessment of the cybersecurity pre-

paredness of the agencies described in subsection (b). 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.

"(b) AGENCIES.—The agencies referred to in subsection (a) 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).

"(c) NATIONAL SECURITY SYSTEMS.—The requirement under subsection (a) shall not apply to national security systems (as defined in section 3552(b) of title 44, United States Code).".

SEC. 4. CYBERSECURITY AUDITS.

Subchapter II of chapter 35 of title 44, United States Code, is amended—

(1) in section 3553(c), by inserting "and the Director of the National Institute of Standards and Technology" after "the Secretary";

(2) in section 3554(c)(1)(A)—

(A) by inserting ", the Director of the National Institute of Standards and Technology" after "the Secretary"; and

(B) by inserting ", Space, and Technology" after "Science"; and

(3) in section 3555—

(A) in subsection (a)(2)—

(i) by redesignating subparagraph (C) as subparagraph (D); and

(ii) by inserting after subparagraph (B) the following:

"(C) an audit or other analytical examination to determine the extent to which the agency is meeting the information security standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and is effectively using the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (or any successor document), which shall include obtaining evidence of an agency's information security protections to determine if such protections are commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency and information systems used or

operated by an agency or by a contractor of an agency or other organization on behalf of an agency; and";

(B) in subsection (b), by inserting "subsection (i)(1) and" after "Subject to";

(C) in subsection (e)—

(i) in paragraph (1), by inserting "and to the Director of the National Institute of Standards and Technology" after "to the Director"; and

(ii) in paragraph (2), by inserting "and to the Director of the National Institute of Standards and Technology" after "to the Director";

(D) by amending subsection (i) to read as follows:

"(i) EVALUATION AND AUDITING TECHNICAL ASSISTANCE.—

"(1) NIST.—Subject to subsection (c), and notwithstanding subsection (d), the National Institute of Standards and Technology shall provide technical assistance and other expert input for each evaluation under this section and shall directly support the audit or other analytical examination described in

subsection (a)(2)(C) with determinations and recommendations for inclusion in each such evaluation.

"(2) GAO.—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures."; and

(E) in subsection (j)—

(i) by striking "The Director" and inserting "(1) The Director";

(ii) by inserting "the Director of the National Institute of Standards and Technology," after "the Secretary,"; and

(iii) by adding at the end the following:

"(2) The Council of the Inspectors General on Integrity and Efficiency, in collaboration with the Director of the National Institute of Standards and Technology, may provide training on how to implement the guidance described in paragraph (1) to Inspectors General, independent external auditors described in subsection (b), and other interested parties as appropriate.".