

Union Calendar No. 276

115TH CONGRESS
1ST SESSION

H. R. 1224

[Report No. 115–376]

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

OCTOBER 31, 2017

Additional sponsor: Mr. SESSIONS

OCTOBER 31, 2017

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on February 27, 2017]

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 *This Act may be cited as the “NIST Cybersecurity*
5 *Framework, Assessment, and Auditing Act of 2017”.*

6 **SEC. 2. NIST MISSION TO ADDRESS CYBERSECURITY**
7 **THREATS.**

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

16 **SEC. 3. IMPLEMENTATION OF CYBERSECURITY FRAME-**
17 **WORK.**

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

21 **“SEC. 20A. FRAMEWORK FOR IMPROVING CRITICAL INFRA-**
22 **STRUCTURE CYBERSECURITY.**

23 *“(a) IMPLEMENTATION BY FEDERAL AGENCIES.—The*
24 *Institute shall promote the implementation by Federal*
25 *agencies of the Framework for Improving Critical Infra-*

1 *structure Cybersecurity (in this section and section 20B re-*
2 *ferred to as the ‘Framework’) by providing to the Office of*
3 *Management and Budget, the Office of Science and Tech-*
4 *nology Policy, and all other Federal agencies, not later than*
5 *6 months after the date of enactment of the NIST Cybersecu-*
6 *rity Framework, Assessment, and Auditing Act of 2017,*
7 *guidance that Federal agencies may use to incorporate the*
8 *Framework into their information security risk manage-*
9 *ment efforts, including practices related to compliance with*
10 *chapter 35 of title 44, United States Code, and any other*
11 *applicable Federal law.*

12 “(b) *GUIDANCE.—The guidance required under sub-*
13 *section (a) shall—*

14 “(1) *describe how the Framework aligns with or*
15 *augments existing agency practices related to compli-*
16 *ance with chapter 35 of title 44, United States Code,*
17 *and any other applicable Federal law;*

18 “(2) *identify any areas of conflict or overlap be-*
19 *tween the Framework and existing cybersecurity re-*
20 *quirements, including gap areas where additional*
21 *policies, standards, guidelines, or programs may be*
22 *needed to encourage Federal agencies to use the*
23 *Framework and improve the ability of Federal agen-*
24 *cies to manage cybersecurity risk;*

1 “(3) include a template for Federal agencies on
2 how to use the Framework, and recommend proce-
3 dures for streamlining and harmonizing existing and
4 future cybersecurity-related requirements, in support
5 of the goal of using the Framework to supplant Fed-
6 eral agency practices in compliance with chapter 35
7 of title 44, United States Code;

8 “(4) recommend other procedures for compliance
9 with cybersecurity reporting, oversight, and policy re-
10 view and creation requirements under such chapter
11 35 and any other applicable Federal law; and

12 “(5) be updated, as the Institute considers nec-
13 essary, to reflect what the Institute learns from ongo-
14 ing research, the audits conducted pursuant to section
15 20B(c), the information compiled by the Federal
16 working group established pursuant to subsection (c),
17 and the annual reports published pursuant to sub-
18 section (d).

19 “(c) *FEDERAL WORKING GROUP*.—Not later than 3
20 months after the date of enactment of the NIST Cybersecu-
21 rity Framework, Assessment, and Auditing Act of 2017, the
22 Institute shall establish and chair a working group (in this
23 section referred to as the ‘Federal working group’), includ-
24 ing representatives of the Office of Management and Budget,

1 *the Office of Science and Technology Policy, and other ap-*
2 *propriate Federal agencies, which shall—*

3 “(1) *not later than 6 months after the date of en-*
4 *actment of the NIST Cybersecurity Framework, As-*
5 *essment, and Auditing Act of 2017, develop outcome-*
6 *based and quantifiable metrics to help Federal agen-*
7 *cies in their analysis and assessment of the effective-*
8 *ness of the Framework in protecting their information*
9 *and information systems;*

10 “(2) *update such metrics as the Federal working*
11 *group considers necessary;*

12 “(3) *compile information from Federal agencies*
13 *on their use of the Framework and the results of the*
14 *analysis and assessment described in paragraph (1);*
15 *and*

16 “(4) *assist the Office of Management and Budget*
17 *and the Office of Science and Technology Policy in*
18 *publishing the annual report required under sub-*
19 *section (d).*

20 “(d) *REPORT.—The Office of Management and Budget*
21 *and the Office of Science and Technology Policy shall de-*
22 *velop and make publicly available an annual report on*
23 *agency adoption rates and the effectiveness of the Frame-*
24 *work. In preparing such report, the Offices shall use the*

1 *information compiled by the Federal working group pursu-*
 2 *ant to subsection (c)(3).*

3 **“SEC. 20B. CYBERSECURITY AUDITS.**

4 *“(a) INITIAL ASSESSMENT.—*

5 *“(1) REQUIREMENT.—Not later than 6 months*
 6 *after the date of enactment of the NIST Cybersecurity*
 7 *Framework, Assessment, and Auditing Act of 2017,*
 8 *the Institute shall complete an initial assessment of*
 9 *the cybersecurity preparedness of the agencies de-*
 10 *scribed in paragraph (2). Such assessment shall be*
 11 *based on information security standards developed*
 12 *under section 20, and may also be informed by work*
 13 *done or reports published by other Federal agencies or*
 14 *officials.*

15 *“(2) AGENCIES.—The agencies referred to in*
 16 *paragraph (1) are the agencies referred to in section*
 17 *901(b) of title 31, United States Code, and any other*
 18 *agency that has reported a major incident (as defined*
 19 *in the Office of Management and Budget Memo-*
 20 *randum—16—03, published on October 30, 2015, or*
 21 *any successor document).*

22 *“(3) NATIONAL SECURITY SYSTEMS.—The re-*
 23 *quirement under paragraph (1) shall not apply to na-*
 24 *tional security systems (as defined in section 3552(b)*
 25 *of title 44, United States Code).*

1 “(b) *AUDIT PLAN.*—Not later than 6 months after the
 2 date of enactment of this Act, the Institute shall prepare
 3 a needs-based plan for carrying out the audits of agencies
 4 as required under subsection (c). Such plan shall include
 5 a description of staffing plans, workforce capabilities, meth-
 6 ods for conducting such audits, coordination with agencies
 7 to support such audits, expected timeframes for the comple-
 8 tion of audits, and other information the Institute considers
 9 relevant. The plan shall be transmitted by the Institute to
 10 the congressional entities described in subsection (c)(4)(F).

11 “(c) *AUDITS.*—

12 “(1) *REQUIREMENT.*—Not later than 6 months
 13 after the date of enactment of the NIST Cybersecurity
 14 Framework, Assessment, and Auditing Act of 2017,
 15 the Institute shall initiate an individual cybersecurity
 16 audit of each agency described in subsection (a)(2), to
 17 assess the extent to which the agency is meeting the
 18 information security standards developed under sec-
 19 tion 20.

20 “(2) *RELATION TO FRAMEWORK.*—Audits con-
 21 ducted under this subsection shall—

22 “(A) to the extent applicable and available,
 23 be informed by the report on agency adoption
 24 rates and the effectiveness of the Framework de-
 25 scribed in section 20A(d); and

1 “(B) if the agency is required by law or ex-
2 ecutive order to adopt the Framework, be based
3 on the guidance described in section 20A(b) and
4 metrics developed under section 20A(c)(1).

5 “(3) *SCHEDULE.*—The Institute shall establish a
6 schedule for completion of audits under this sub-
7 section to ensure that—

8 “(A) audits of agencies whose information
9 security risk is high, based on the assessment
10 conducted under subsection (a), are completed
11 not later than 1 year after the date of enactment
12 of the NIST Cybersecurity Framework, Assess-
13 ment, and Auditing Act of 2017, and are audited
14 annually thereafter; and

15 “(B) audits of all other agencies described
16 in subsection (a)(2) are completed not later than
17 2 years after the date of enactment of the NIST
18 Cybersecurity Framework, Assessment, and Au-
19 diting Act of 2017, and are audited biennially
20 thereafter.

21 “(4) *REPORT.*—A report of each audit conducted
22 under this subsection shall be transmitted by the In-
23 stitute to—

24 “(A) the Office of Management and Budget;

1 “(B) *the Office of Science and Technology*
2 *Policy;*
3 “(C) *the Government Accountability Office;*
4 “(D) *the agency being audited;*
5 “(E) *the Inspector General of such agency,*
6 *if there is one; and*
7 “(F) *Congress, including the Committee on*
8 *Science, Space, and Technology of the House of*
9 *Representatives and the Committee on Com-*
10 *merce, Science, and Transportation of the Sen-*
11 *ate.”.*

Union Calendar No. 276

115TH CONGRESS
1ST Session

H. R. 1224

[Report No. 115-376]

A BILL

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

OCTOBER 31, 2017

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed