

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.

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 Stand-
9 ards and Technology Act (15 U.S.C. 278g–3(a)(1)) is

1 amended by inserting “, emphasizing the principle that ex-
2 panding cybersecurity threats require engineering security
3 from the beginning of an information system’s life cycle,
4 building more trustworthy and secure components and
5 systems from the start, and applying well-defined security
6 design principles throughout” before the semicolon.

7 **SEC. 3. IMPLEMENTATION OF CYBERSECURITY FRAME-**
8 **WORK.**

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

12 **“SEC. 20A. FRAMEWORK FOR IMPROVING CRITICAL INFRA-**
13 **STRUCTURE CYBERSECURITY.**

14 “(a) IMPLEMENTATION BY FEDERAL AGENCIES.—

15 “(1) IN GENERAL.—The Institute shall promote
16 the implementation by Federal agencies of the
17 Framework for Improving Critical Infrastructure
18 Cybersecurity (in this section and section 20B re-
19 ferred to as the ‘Framework’) by providing to the
20 Office of Management and Budget, the Office of
21 Science and Technology Policy, and all other Federal
22 agencies, not later than 6 months after the date of
23 enactment of the NIST Cybersecurity Framework,
24 Assessment, and Auditing Act of 2017, guidance
25 that Federal agencies may use to incorporate the

1 Framework into their information security risk man-
2 agement efforts, including practices related to com-
3 pliance with chapter 35 of title 44, United States
4 Code, and any other applicable Federal law.

5 “(2) GUIDANCE.—The guidance required under
6 paragraph (1) shall—

7 “(A) describe how the Framework aligns
8 with or augments existing agency practices re-
9 lated to compliance with chapter 35 of title 44,
10 United States Code, and any other applicable
11 Federal law;

12 “(B) identify any areas of conflict or over-
13 lap between the Framework and existing cyber-
14 security requirements, including gap areas
15 where additional policies, standards, guidelines,
16 or programs may be needed to encourage Fed-
17 eral agencies to use the Framework and im-
18 prove the ability of Federal agencies to manage
19 cybersecurity risk;

20 “(C) include a template for Federal agen-
21 cies on how to use the Framework, and rec-
22 ommend procedures for streamlining and har-
23 monizing existing and future cybersecurity-re-
24 lated requirements, in support of the goal of
25 using the Framework to supplant Federal agen-

1 cy practices in compliance with chapter 35 of
2 title 44, United States Code;

3 “(D) recommend other procedures for com-
4 pliance with cybersecurity reporting, oversight,
5 and policy review and creation requirements
6 under such chapter 35 and any other applicable
7 Federal law; and

8 “(E) be updated, as the Institute considers
9 necessary, to reflect what the Institute learns
10 from ongoing research, the audits conducted
11 pursuant to section 20B(b), the information
12 compiled by the Federal working group estab-
13 lished pursuant to paragraph (3), the informa-
14 tion compiled by the public-private working
15 group established pursuant to subsection (b)(1),
16 the annual reports published pursuant to para-
17 graph (4), and the annual reports published
18 pursuant to subsection (b)(2).

19 “(3) FEDERAL WORKING GROUP.—Not later
20 than 3 months after the date of enactment of the
21 NIST Cybersecurity Framework, Assessment, and
22 Auditing Act of 2017, the Institute shall establish
23 and chair a working group (in this section referred
24 to as the ‘Federal working group’), including rep-
25 resentatives of the Office of Science and Technology

1 Policy and other appropriate Federal agencies, which
2 shall—

3 “(A) not later than 6 months after the
4 date of enactment of the NIST Cybersecurity
5 Framework, Assessment, and Auditing Act of
6 2017, develop outcome-based and quantifiable
7 metrics, in coordination with the public-private
8 working group established pursuant to sub-
9 section (b), to help Federal agencies in their
10 analysis and assessment of the effectiveness of
11 the Framework in protecting their information
12 and information systems;

13 “(B) update such metrics as the Federal
14 working group considers necessary;

15 “(C) compile information from Federal
16 agencies on their use of the Framework and the
17 results of the analysis and assessment described
18 in subparagraph (A); and

19 “(D) assist the Office of Science and Tech-
20 nology Policy in publishing the annual report
21 required under paragraph (4).

22 “(4) REPORT.—The Office of Science and
23 Technology Policy shall develop and make publicly
24 available an annual report on agency adoption rates
25 and the effectiveness of the Framework. In pre-

1 paring such report, the Office shall use the informa-
2 tion compiled by the Federal working group pursu-
3 ant to paragraph (3)(C).

4 “(b) IMPLEMENTATION BY PRIVATE ENTITIES.—

5 “(1) PUBLIC-PRIVATE WORKING GROUP.—Not
6 later than 6 months after the date of enactment of
7 the NIST Cybersecurity Framework, Assessment,
8 and Auditing Act of 2017, the Institute shall, in co-
9 ordination with industry stakeholders, establish a
10 working group (in this section referred to as the
11 ‘public-private working group’) which shall—

12 “(A) not later than 1 year after the date
13 of enactment of the NIST Cybersecurity
14 Framework, Assessment, and Auditing Act of
15 2017, develop specific Framework implementa-
16 tion models and measurement tools that private
17 entities can use to adopt the Framework;

18 “(B) not later than 1 year after the date
19 of enactment of the NIST Cybersecurity
20 Framework, Assessment, and Auditing Act of
21 2017, develop, in coordination with the Federal
22 working group, industry-led, consensus and out-
23 come-based metrics that quantify the effective-
24 ness and benefits of the Framework to enable
25 private entities to voluntarily analyze and as-

1 sess their individual corporate cybersecurity
2 risks;

3 “(C) update the models and tools devel-
4 oped pursuant to subparagraph (A) and the
5 metrics developed pursuant to subparagraph
6 (B), as the public-private working group con-
7 siders necessary;

8 “(D) compile information, derived from the
9 metrics developed pursuant to subparagraph
10 (B), voluntarily submitted by private entities on
11 their use of the Framework and on the effec-
12 tiveness and benefits of such use;

13 “(E) analyze the information compiled
14 pursuant to subparagraph (D) and provide such
15 information and analysis to—

16 “(i) the Institute, for the purpose of
17 enabling the Institute to make improve-
18 ments to the Framework; and

19 “(ii) private entities, for the purpose
20 of providing such entities with a greater
21 understanding of the benefits of the
22 Framework to enable them to use the
23 Framework more effectively to improve
24 their cybersecurity; and

1 “(F) assist the Office of Science and Tech-
2 nology Policy in publishing the annual report
3 required under paragraph (2).

4 “(2) REPORT.—The Office of Science and
5 Technology Policy shall develop and make publicly
6 available an annual report on industry adoption
7 rates and the effectiveness of the Framework. In
8 preparing such report, the Office shall use informa-
9 tion compiled by the public-private working group
10 pursuant to paragraph (1)(D).

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

12 “(a) INITIAL ASSESSMENT.—

13 “(1) REQUIREMENT.—Not later than 6 months
14 after the date of enactment of the NIST Cybersecu-
15 rity Framework, Assessment, and Auditing Act of
16 2017, the Institute shall complete an initial assess-
17 ment of the cybersecurity preparedness of the agen-
18 cies described in paragraph (2). Such assessment
19 shall be based on information security standards de-
20 veloped under section 20, and may also be informed
21 by work done or reports published by other Federal
22 agencies or officials.

23 “(2) AGENCIES.—The agencies referred to in
24 paragraph (1) are the agencies referred to in section
25 901(b) of title 31, United States Code, and any

1 other agency that has reported a major incident (as
2 defined in the Office of Management and Budget
3 Memorandum—16–03, published on October 30,
4 2015, or any successor document).

5 “(3) NATIONAL SECURITY SYSTEMS.—The re-
6 quirement under paragraph (1) shall not apply to
7 national security systems (as defined in section
8 3552(b) of title 44, United States Code).

9 “(b) AUDITS.—

10 “(1) REQUIREMENT.—Not later than 6 months
11 after the date of enactment of the NIST Cybersecu-
12 rity Framework, Assessment, and Auditing Act of
13 2017, the Institute shall initiate an individual cyber-
14 security audit of each agency described in subsection
15 (a)(2), to assess the extent to which the agency is
16 meeting the information security standards devel-
17 oped under section 20.

18 “(2) RELATION TO FRAMEWORK.—Audits con-
19 ducted under this subsection shall—

20 “(A) to the extent applicable and available,
21 be informed by the report on agency adoption
22 rates and the effectiveness of the Framework
23 described in section 20A(a)(4); and

24 “(B) if the agency is required by law or
25 Executive order to adopt the Framework, be

1 based on the guidance described in section
2 20A(a)(2) and metrics developed under section
3 20A(a)(3)(A).

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

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

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

20 “(4) REPORT.—A report of each audit con-
21 ducted under this subsection shall be transmitted by
22 the Institute to—

23 “(A) the Office of Management and Budg-
24 et;

1 “(B) the Office of Science and Technology
2 Policy;

3 “(C) the Government Accountability Of-
4 fice;

5 “(D) the agency being audited;

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

8 “(F) Congress, including the Committee on
9 Science, Space, and Technology of the House of
10 Representatives and the Committee on Com-
11 merce, Science, and Transportation of the Sen-
12 ate.”.

○