

Proposed modification

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”.

1 **SEC. 2. NIST MISSION TO ADDRESS CYBERSECURITY**
2 **THREATS.**

3 Section 20(a)(1) of the National Institute of Stand-
4 ards and Technology Act (15 U.S.C. 278g–3(a)(1)) is
5 amended by inserting “, emphasizing the principle that ex-
6 panding cybersecurity threats require engineering security
7 from the beginning of an information system’s life cycle,
8 building more trustworthy and secure components and
9 systems from the start, and applying well-defined security
10 design principles throughout” before the semicolon.

11 **SEC. 3. IMPLEMENTATION OF CYBERSECURITY FRAME-**
12 **WORK.**

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

16 **“SEC. 20A. FRAMEWORK FOR IMPROVING CRITICAL INFRA-**
17 **STRUCTURE CYBERSECURITY.**

18 “(a) IMPLEMENTATION BY FEDERAL AGENCIES.—
19 The Institute shall promote the implementation by Fed-
20 eral agencies of the Framework for Improving Critical In-
21 frastructure Cybersecurity (in this section referred to as
22 the ‘Framework’) by providing to the Office of Manage-
23 ment and Budget, the Office of Science and Technology
24 Policy, and all other Federal agencies, not later than 6
25 months after the date of enactment of the NIST Cyberse-
26 curity Framework, Assessment, and Auditing Act, guid-

1 ance that Federal agencies may use to incorporate the
2 Framework into their information security risk manage-
3 ment efforts, including practices related to compliance
4 with chapter 35 of title 44, United States Code, and any
5 other applicable Federal law.

6 “(b) GUIDANCE.—The guidance required under sub-
7 section (a) shall—

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

12 “(2) identify any areas of conflict or overlap be-
13 tween the Framework and existing cybersecurity re-
14 quirements, including gap areas where additional
15 policies, standards, guidelines, or programs may be
16 needed to encourage Federal agencies to use the
17 Framework and improve the ability of Federal agen-
18 cies to manage cybersecurity risk;

19 “(3) include a template for Federal agencies on
20 how to use the Framework, and recommend proce-
21 dures for streamlining and harmonizing existing and
22 future cybersecurity-related requirements, in support
23 of the goal of using the Framework to supplement
24 Federal agency practices in compliance with chapter
25 35 of title 44, United States Code;

1 “(4) recommend other procedures for compli-
2 ance with cybersecurity reporting, oversight, and
3 policy review and creation requirements under such
4 chapter 35 and any other applicable Federal law;
5 and

6 “(5) be updated, as the Institute considers nec-
7 essary, to reflect what the Institute learns from on-
8 going research, evaluations, and audits or analytical
9 examinations conducted pursuant to section 3555 of
10 title 44, United States Code, the information com-
11 piled by the Federal working group established pur-
12 suant to subsection (c), and the annual reports pub-
13 lished pursuant to subsection (d).

14 “(c) FEDERAL WORKING GROUP.—Not later than 3
15 months after the date of enactment of the NIST Cyberse-
16 curity Framework, Assessment, and Auditing Act, the In-
17 stitute shall establish and chair a working group (in this
18 section referred to as the ‘Federal working group’), includ-
19 ing representatives of the Office of Management and
20 Budget, the Office of Science and Technology Policy, and
21 other appropriate Federal agencies, which shall—

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

1 cies in their analysis and assessment of the effective-
2 ness of the Framework in protecting their informa-
3 tion and information systems;

4 “(2) update such metrics as the Federal work-
5 ing group considers necessary;

6 “(3) compile information from Federal agencies
7 on their use of the Framework and the results of the
8 analysis and assessment described in paragraph (1);
9 and

10 “(4) assist the Office of Management and
11 Budget and the Office of Science and Technology
12 Policy in publishing the annual report required
13 under subsection (d).

14 “(d) REPORT.—The Office of Management and
15 Budget and the Office of Science and Technology Policy
16 shall develop and make publicly available an annual report
17 on agency adoption rates and the effectiveness of the
18 Framework. In preparing such report, the Offices shall
19 use the information compiled by the Federal working
20 group pursuant to subsection (c)(3).

21 **“SEC. 20B. CYBERSECURITY ASSESSMENT.**

22 “(a) IN GENERAL.—Not later than 6 months after
23 the date of enactment of the NIST Cybersecurity Frame-
24 work, Assessment, and Auditing Act, the Institute shall
25 complete an initial assessment of the cybersecurity pre-

1 paredness of the agencies described in subsection (b).
2 Such assessment shall be based on information security
3 standards developed under section 20, and may also be
4 informed by work done or reports published by other Fed-
5 eral agencies or officials.

6 “(b) AGENCIES.—The agencies referred to in sub-
7 section (a) are the agencies referred to in section 901(b)
8 of title 31, United States Code, and any other agency that
9 has reported a major incident (as defined in the Office
10 of Management and Budget Memorandum—16—03, pub-
11 lished on October 30, 2015, or any successor document).

12 “(c) NATIONAL SECURITY SYSTEMS.—The require-
13 ment under subsection (a) shall not apply to national secu-
14 rity systems (as defined in section 3552(b) of title 44,
15 United States Code).”.

16 **SEC. 4. CYBERSECURITY AUDITS.**

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

19 (1) in section 3553(c), by inserting “and the
20 Director of the National Institute of Standards and
21 Technology” after “the Secretary”;

22 (2) in section 3554(c)(1)(A)—

23 (A) by inserting “, the Director of the Na-
24 tional Institute of Standards and Technology”
25 after “the Secretary”; and

1 (B) by inserting “, Space, and Tech-
2 nology” after “Science”; and

3 (3) in section 3555—

4 (A) in subsection (a)(2)—

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

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

9 “(C) an audit or other analytical examina-
10 tion to determine the extent to which the agen-
11 cy is meeting the information security stand-
12 ards developed under section 20 of the National
13 Institute of Standards and Technology Act (15
14 U.S.C. 278g-3) and is effectively using the Na-
15 tional Institute of Standards and Technology
16 Framework for Improving Critical Infrastruc-
17 ture Cybersecurity (or any successor document),
18 which shall include obtaining evidence of an
19 agency’s information security protections to de-
20 termine if such protections are commensurate
21 with the risk and magnitude of the harm result-
22 ing from unauthorized access, use, disclosure,
23 disruption, modification, or destruction of infor-
24 mation collected or maintained by or on behalf
25 of an agency and information systems used or

1 operated by an agency or by a contractor of an
2 agency or other organization on behalf of an
3 agency; and”;

4 (B) in subsection (b), by inserting “sub-
5 section (i)(1) and” after “Subject to”;

6 (C) in subsection (e)—

7 (i) in paragraph (1), by inserting
8 “and to the Director of the National Insti-
9 tute of Standards and Technology” after
10 “to the Director”; and

11 (ii) in paragraph (2), by inserting
12 “and to the Director of the National Insti-
13 tute of Standards and Technology” after
14 “to the Director”;

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

17 “(i) EVALUATION AND AUDITING TECHNICAL AS-
18 SISTANCE.—

19 “(1) NIST.—Subject to subsection (c), and not-
20 withstanding subsection (d), the National Institute
21 of Standards and Technology shall provide technical
22 assistance and other expert input for each evaluation
23 under this section and shall directly support the
24 audit or other analytical examination described in

1 subsection (a)(2)(C) with determinations and rec-
2 ommendations for inclusion in each such evaluation.

3 “(2) GAO.—The Comptroller General may pro-
4 vide technical assistance to an Inspector General or
5 the head of an agency, as applicable, to assist the
6 Inspector General or head of an agency in carrying
7 out the duties under this section, including by test-
8 ing information security controls and procedures.”;
9 and

10 (E) in subsection (j)—

11 (i) by striking “The Director” and in-
12 serting “(1) The Director”;

13 (ii) by inserting “the Director of the
14 National Institute of Standards and Tech-
15 nology,” after “the Secretary,”; and

16 (iii) by adding at the end the fol-
17 lowing:

18 “(2) The Council of the Inspectors General on Integ-
19 rity and Efficiency, in collaboration with the Director of
20 the National Institute of Standards and Technology, may
21 provide training on how to implement the guidance de-
22 scribed in paragraph (1) to Inspectors General, inde-
23 pendent external auditors described in subsection (b), and
24 other interested parties as appropriate.”.