

.....  
(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.

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”.

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 **“(1) IN GENERAL.—**The Institute shall promote  
20 the implementation by Federal agencies of the  
21 Framework for Improving Critical Infrastructure  
22 Cybersecurity (in this section and section 20B re-  
23 ferred to as the ‘Framework’) by providing to the  
24 Office of Management and Budget, the Office of  
25 Science and Technology Policy, and all other Federal  
26 agencies, not later than 6 months after the date of

1 enactment of the NIST Cybersecurity Framework,  
2 Assessment, and Auditing Act of 2017, guidance  
3 that Federal agencies may use to incorporate the  
4 Framework into their information security risk man-  
5 agement efforts, including practices related to com-  
6 pliance with chapter 35 of title 44, United States  
7 Code, and any other applicable Federal law.

8 “(2) GUIDANCE.—The guidance required under  
9 paragraph (1) shall—

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

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

23 “(C) include a template for Federal agen-  
24 cies on how to use the Framework, and rec-  
25 ommend procedures for streamlining and har-

1 monizing existing and future cybersecurity-re-  
2 lated requirements, in support of the goal of  
3 using the Framework to supplant Federal agen-  
4 cy practices in compliance with chapter 35 of  
5 title 44, United States Code;

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

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

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

1 and chair a working group (in this section referred  
2 to as the ‘Federal working group’), including rep-  
3 resentatives of the Office of Science and Technology  
4 Policy and other appropriate Federal agencies, which  
5 shall—

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

16 “(B) update such metrics as the Federal  
17 working group considers necessary;

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

22 “(D) assist the Office of Science and Tech-  
23 nology Policy in publishing the annual report  
24 required under paragraph (4).

1           “(4) REPORT.—The Office of Science and  
2           Technology Policy shall develop and make publicly  
3           available an annual report on agency adoption rates  
4           and the effectiveness of the Framework. In pre-  
5           paring such report, the Office shall use the informa-  
6           tion compiled by the Federal working group pursu-  
7           ant to paragraph (3)(C).

8           “(b) IMPLEMENTATION BY PRIVATE ENTITIES.—

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

16                 “(A) not later than 1 year after the date  
17                 of enactment of the NIST Cybersecurity  
18                 Framework, Assessment, and Auditing Act of  
19                 2017, develop specific Framework implementa-  
20                 tion models and measurement tools that private  
21                 entities can use to adopt the Framework;

22                 “(B) not later than 1 year after the date  
23                 of enactment of the NIST Cybersecurity  
24                 Framework, Assessment, and Auditing Act of  
25                 2017, develop, in coordination with the Federal

1 working group, industry-led, consensus and out-  
2 come-based metrics that quantify the effective-  
3 ness and benefits of the Framework to enable  
4 private entities to voluntarily analyze and as-  
5 sess their individual corporate cybersecurity  
6 risks;

7 “(C) update the models and tools devel-  
8 oped pursuant to subparagraph (A) and the  
9 metrics developed pursuant to subparagraph  
10 (B), as the public-private working group con-  
11 siders necessary;

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

17 “(E) analyze the information compiled  
18 pursuant to subparagraph (D) and provide such  
19 information and analysis to—

20 “(i) the Institute, for the purpose of  
21 enabling the Institute to make improve-  
22 ments to the Framework; and

23 “(ii) private entities, for the purpose  
24 of providing such entities with a greater  
25 understanding of the benefits of the

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

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

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

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

15 “(a) INITIAL ASSESSMENT.—

16 “(1) REQUIREMENT.—Not later than 6 months  
17 after the date of enactment of the NIST  
18 Cybersecurity Framework, Assessment, and Auditing  
19 Act of 2017, the Institute shall complete an initial  
20 assessment of the cybersecurity preparedness of the  
21 agencies described in paragraph (2). Such assess-  
22 ment shall be based on information security stand-  
23 ards developed under section 20, and may also be in-  
24 formed by work done or reports published by other  
25 Federal agencies or officials.

1           “(2) AGENCIES.—The agencies referred to in  
2 paragraph (1) are the agencies referred to in section  
3 901(b) of title 31, United States Code, and any  
4 other agency that has reported a major incident (as  
5 defined in the Office of Management and Budget  
6 Memorandum—16—03, published on October 30,  
7 2015, or any successor document).

8           “(3) NATIONAL SECURITY SYSTEMS.—The re-  
9 quirement under paragraph (1) shall not apply to  
10 national security systems (as defined in section  
11 3552(b) of title 44, United States Code).

12           “(b) AUDITS.—

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

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

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

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

3 “(B) if the agency is required by law or ex-  
4 ecutive order to adopt the Framework, be based  
5 on the guidance described in section 20A(a)(2)  
6 and metrics developed under section  
7 20A(a)(3)(A).

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

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

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

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

4                   “(A) the Office of Management and Budg-  
5                   et;

6                   “(B) the Office of Science and Technology  
7                   Policy;

8                   “(C) the Government Accountability Of-  
9                   fice;

10                  “(D) the agency being audited;

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

13                  “(F) Congress, including the Committee on  
14                  Science, Space, and Technology of the House of  
15                  Representatives and the Committee on Com-  
16                  merce, Science, and Transportation of the Sen-  
17                  ate.”.