

[DISCUSSION DRAFT]

SEPTEMBER 13, 2016

114TH CONGRESS
2D SESSION

H. R. _____

To enforce Federal cybersecurity responsibility and accountability.

IN THE HOUSE OF REPRESENTATIVES

M. _____ introduced the following bill; which was referred to the
Committee on _____

A BILL

To enforce Federal cybersecurity responsibility and
accountability.

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 “Cybersecurity Respon-
5 sibility and Accountability Act of 2016”.

6 **SEC. 2. DEFINITIONS.**

7 Section 3552 of title 44, United States Code, is
8 amended—

1 (1) by redesignating paragraphs (6) and (7) as
2 paragraphs (7) and (8), respectively; and

3 (2) by inserting after paragraph (5) the fol-
4 lowing new paragraph:

5 “(6) The term ‘major cybersecurity incident’ has
6 the meaning given the term ‘major incident’ in Of-
7 fice of Management and Budget Memorandum —16-
8 03, dated October 30, 2015, or any successor docu-
9 ment.”.

10 **SEC. 3. AUTHORITY AND FUNCTIONS OF THE DIRECTOR OF**
11 **NIST.**

12 (a) AMENDMENT.—Section 3553 of title 44, United
13 States Code, is amended—

14 (1) by redesignating subsections (e) through (j)
15 as subsections (d) through (k), respectively; and

16 (2) by inserting after subsection (b) the fol-
17 lowing new subsection:

18 “(c) DIRECTOR OF THE NATIONAL INSTITUTE OF
19 STANDARDS AND TECHNOLOGY.—The Director of the Na-
20 tional Institute of Standards and Technology shall further
21 develop and update as necessary the standards and guide-
22 lines under section 20 of the National Institute of Stand-
23 ards and Technology Act (15 U.S.C. 278g–3) to fulfill the
24 additional objectives and requirements of the
25 Cybersecurity Responsibility and Accountability Act of

1 2016. Further, the Director of the National Institute of
2 Standards and Technology shall—

3 “(1) provide to the Director of the Office of
4 Management and Budget a framework and process
5 for agency implementation of such standards and
6 guidelines;

7 “(2) provide support to agency heads for the
8 implementation of such standards and guidelines
9 and their application to information security policies
10 and principles, as well as with the development of in-
11 formation security training and certification for
12 agency heads;

13 “(3) conduct cybersecurity research—

14 “(A) to identify and address prevalent in-
15 formation security challenges, concerns, and
16 knowledge gaps identified by agencies, including
17 those manifested in any of the reports, evalua-
18 tions, assessments, and plans described in this
19 subchapter that may undermine agencies’ infor-
20 mation security policies and practices;

21 “(B) to assess the sufficiency of the cur-
22 rent statutory requirements of the Federal In-
23 formation Security Management Act of 2002
24 and the Federal Information Security Mod-
25 ernization Act of 2014, and their effectiveness

1 in requiring agencies to implement standards
2 and guidelines developed under section 20 of
3 the National Institute of Standards and Tech-
4 nology Act (15 U.S.C. 278g–3) and authorized
5 by the Cybersecurity Responsibility and Ac-
6 countability Act of 2016 regarding information
7 security policies and practices; and

8 “(C) that shall require the Director of the
9 Office of Management and Budget, the Sec-
10 retary of Homeland Security, and the heads of
11 other Federal agencies to provide the Director
12 of the National Institute of Standards and
13 Technology any resources, including reports,
14 evaluations, assessments, and plans, that may
15 be required for such research; and

16 “(4) develop, publish, and update as necessary
17 information security standards and guidelines for
18 national security systems based on established
19 standards and guidelines for information systems.”.

20 (b) CONFORMING AMENDMENTS.—Subchapter II of
21 chapter 35 of title 44, United States Code, is amended—

22 (1) in the item relating to section 3553 in the
23 table of sections, by striking “and the Secretary”
24 and inserting “, the Secretary, and the Director of

1 the National Institute of Standards and Tech-
2 nology”;

3 (2) in the section heading for section 3553, by
4 striking “**and the Secretary**” and inserting “,
5 **the Secretary, and the Director of the Na-**
6 **tional Institute of Standards and Tech-**
7 **nology**”;

8 (3) in section 3553(e), as so redesignated by
9 subsection (a)(1) of this section, by striking “sub-
10 section (c)” and inserting “subsection (d)”;

11 (4) in section 3553(i)(1)(B), as so redesignated
12 by subsection (a)(1) of this section—

13 (A) by striking “subsection (d)” and in-
14 serting “subsection (e)”;

15 (B) by striking “subsection (e)” and in-
16 serting “subsection (f)”;

17 (5) in section 3554(a)(1)(B)(v), by striking
18 “section 3553(h)” and inserting “section 3553(i)”;

19 and

20 (6) in section 3555(g)(1), by striking “section
21 3553(c)” and inserting “section 3553(d)”.

22 **SEC. 4. AGENCY HEADS.**

23 Section 2(d) of the Federal Information Security
24 Modernization Act of 2014 (44 U.S.C. 3553 note) is
25 amended—

1 (1) in paragraph (1)—

2 (A) in subparagraph (A)—

3 (i) in the matter before clause (i), by
4 inserting “head” after “affected agency”;

5 and

6 (ii) in clause (ii)(IV), by inserting
7 “head” after “when the agency”; and

8 (B) in subparagraph (B)—

9 (i) by inserting “head of the” after
10 “notice by the”; and

11 (ii) by striking “agency discovers” in-
12 serting “agency head discovers”;

13 (2) in paragraph (3)(A)(ii), by striking “section
14 3553(e)” and inserting “section 3553(d)”; and

15 (3) in paragraph (4), by inserting “the National
16 Institute of Standards and Technology and” after
17 “such notice to”.

18 **SEC. 5. FEDERAL AGENCY HEAD RESPONSIBILITIES.**

19 Section 3554 of title 44, United States Code, is
20 amended—

21 (1) in subsection (a)(3)(A)—

22 (A) by striking “designating a senior agen-
23 cy information security officer” and inserting
24 “collaborating with the agency head to des-
25 ignate a Chief Information Security Officer”;

1 (B) by redesignating clauses (i) through
2 (iv) as clauses (ii) through (v), respectively;

3 (C) by inserting before clause (ii), as so re-
4 designated, the following new clause:

5 “(i) have the job description and re-
6 sponsibilities that shall be provided in
7 guidance issued by the Director, developed
8 in consultation with the Director of the
9 National Institute of Standards and Tech-
10 nology and the Secretary, within 6 months
11 after the date of enactment of the
12 Cybersecurity Responsibility and Account-
13 ability Act of 2016;”;

14 (D) in clause (iv), as so redesignated, by
15 striking “and” at the end;

16 (E) in clause (v), as so redesignated, by in-
17 serting “and” after the semicolon at the end;
18 and

19 (F) by adding at the end the following new
20 clause:

21 “(vi) be designated without increasing
22 the number of full-time equivalent em-
23 ployee positions at the agency;”;

24 (2) in subsection (b)—

1 (A) by redesignating paragraphs (5)
2 through (8) as paragraphs (6) through (9), re-
3 spectively; and

4 (B) by inserting after paragraph (4) the
5 following new paragraph:

6 “(5) mandatory annual information security
7 training and certification designed specifically for
8 the agency head, developed and updated as nec-
9 essary by the National Institute of Standards and
10 Technology, the purpose of which shall be to ensure
11 that the agency head has an understanding of Fed-
12 eral cybersecurity policy, including an understanding
13 of—

14 “(A) the information and information sys-
15 tems that support the operations and assets of
16 the agency, using nontechnical terms as much
17 as possible;

18 “(B) the potential impact of common types
19 of cyber-attacks and data breaches on the agen-
20 cy’s operations and assets;

21 “(C) how cyber-attacks and data breaches
22 occur;

23 “(D) steps the agency head and agency
24 employees should take to protect their informa-
25 tion and information systems, including not

1 using private messaging system software or pri-
2 vate e-mail servers for official communications;
3 and

4 “(E) the annual reporting requirements re-
5 quired of the agency head under subsection (c),
6 including the certifications required under sub-
7 section (c)(1)(A)(iv);”;

8 (3) in subsection (c)—

9 (A) in paragraph (1)(A)—

10 (i) by striking “Each agency” and in-
11 sserting “The head of each agency”;

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

16 (iii) by inserting “, Space, and Tech-
17 nology” after “the Committee on Science”;

18 (iv) by striking “and” at the end of
19 clause (iii)(II);

20 (v) by redesignating clause (iv) as
21 clause (v); and

22 (vi) by inserting after clause (iii) the
23 following new clause:

24 “(iv) specific written certification by
25 the agency head that—

1 “(I) certifies that information se-
2 curity standards developed under sec-
3 tion 20 of the National Institute of
4 Standards and Technology Act (15
5 U.S.C. 278g-3) are being met by the
6 agency;

7 “(II) identifies the security con-
8 trols in place at the agency and how
9 they each meet the relevant informa-
10 tion security standard;

11 “(III) may be based on or in-
12 formed by the assessment described in
13 section 3553(d)(4); and

14 “(IV) for any information secu-
15 rity standard that the agency does not
16 meet, provides the reasons therefor
17 and includes documentation of the Di-
18 rector’s certification of the agency not
19 meeting the standard; and”;

20 (B) in paragraph (2), by striking “Each
21 agency” and inserting “The head of each agen-
22 cy”;

23 (4) in subsection (d), by striking “each agency”
24 and inserting “the head of each agency”;

1 (5) by redesignating subsection (e) as sub-
2 section (f);

3 (6) by inserting after subsection (d) the fol-
4 lowing new subsection:

5 “(e) PLANS FOR IMPLEMENTATION OF REC-
6 COMMENDATIONS.—

7 “(1) COMPTROLLER GENERAL RECOMMENDA-
8 TIONS.—

9 “(A) IN GENERAL.—In addition to the re-
10 quirements of subsections (c) and (d), each
11 agency head shall, not later than 6 months
12 after the date of enactment of the Cybersecurity
13 Responsibility and Accountability Act of 2016,
14 develop a plan, in consultation with the Comp-
15 troller General, to implement all of the Comp-
16 troller General’s recommendations regarding in-
17 formation security controls relevant to that
18 agency.

19 “(B) PLAN.—The plan required under sub-
20 paragraph (A)—

21 “(i) shall be submitted to the agencies
22 and committees described in subsection
23 (c)(1)(A);

24 “(ii) shall include a schedule for im-
25 plementation of the Comptroller General’s

1 recommendations, including a completion
2 deadline;

3 “(iii) shall be updated annually, and
4 such annual updates shall be included in
5 the annual report described in subsection
6 (c)(1)(A); and

7 “(iv) may, as appropriate, be based on
8 or informed by recommendations included
9 in the evaluation and report described in
10 section 3555(h).

11 “(C) IF NO RECOMMENDATIONS.—If the
12 Comptroller General does not have any relevant
13 recommendations for an agency head to imple-
14 ment relative to information security controls,
15 then the agency head shall accordingly notify
16 the agencies and committees described in sub-
17 section (c)(1)(A).

18 “(D) REASONS FOR FAILURE TO IMPLE-
19 MENT.—If there are any Comptroller General
20 recommendations that an agency head does not
21 implement, the agency head shall provide the
22 reasons for that failure to the Director for the
23 Director’s approval. For each unimplemented
24 recommendation, the plan shall include either
25 the Director’s approval or a certification by the

1 Director of the agency head's failure to imple-
2 ment such recommendation.

3 “(2) INSPECTOR GENERAL RECOMMENDA-
4 TIONS.—

5 “(A) IN GENERAL.—In addition to the re-
6 quirements of subsections (c) and (d), each
7 agency head shall, not later than 6 months
8 after the date of enactment of the Cybersecurity
9 Responsibility and Accountability Act of 2016,
10 develop a plan, in consultation with its Inspec-
11 tor General, to implement all of the Inspector
12 General's recommendations regarding the agen-
13 cy's information security program.

14 “(B) PLAN.—The plan required under sub-
15 paragraph (A)—

16 “(i) shall be submitted to the agencies
17 and committees described in subsection
18 (c)(1)(A);

19 “(ii) shall include a schedule for im-
20 plementation of the Inspector General's
21 recommendations, including a completion
22 deadline;

23 “(iii) shall be updated annually, and
24 such annual updates shall be included in

1 the annual report described in subsection
2 (c)(1)(A); and

3 “(iv) may, as appropriate, be based on
4 or informed by recommendations included
5 in—

6 “(I) the evaluation described in
7 section 3555(b)(1); or

8 “(II) if the agency does not have
9 an Inspector General, the evaluation
10 described in section 3555(b)(2).

11 “(C) IF NO RECOMMENDATIONS.—If the
12 Inspector General does not have any relevant
13 information security control recommendations
14 for the agency head to implement, then the
15 agency head shall accordingly notify the agen-
16 cies and committees described in subsection
17 (c)(1)(A).

18 “(D) REASONS FOR FAILURE TO IMPLE-
19 MENT.—If there are any Inspector General rec-
20 ommendations that the agency head does not
21 implement, the agency head shall provide the
22 reasons for that failure to the Director for the
23 Director’s approval. For each unimplemented
24 recommendation, the plan shall include either
25 the Director’s approval or a certification by the

1 Director of the agency head’s failure to imple-
2 ment such recommendation.”; and

3 (7) in subsection (f), as so redesignated, by
4 striking “Each agency” and inserting “The head of
5 each agency”.

6 **SEC. 6. ANNUAL INDEPENDENT EVALUATION.**

7 Section 3555 of title 44, United States Code, is
8 amended—

9 (1) in subsection (a)(1), by inserting “head”
10 after “each agency”;

11 (2) in subsection (b)(1), by inserting “and eval-
12 uations required by section 3555a” after “required
13 by this section”;

14 (3) in subsection (c), by striking “that portion
15 of the evaluation required by this section” and in-
16 serting “the portions of evaluations required by this
17 section or section 3555a”;

18 (4) in subsection (e)(2), by inserting “or section
19 3555a” after “required under this section”;

20 (5) in subsection (f), by striking “Agencies”
21 and inserting “In carrying out this section and sec-
22 tion 3555a, agencies”;

23 (6) in subsection (g)(3), by inserting “under
24 this section or section 3555a” after “Evaluations”;

25 (7) in subsection (i)—

1 (A) by striking “the head of an agency”
2 and inserting “an agency head”;

3 (B) by striking “head of an agency” and
4 inserting “agency head”; and

5 (C) by inserting “or section 3555a” after
6 “under this section”; and

7 (8) in subsection (j), by inserting “the Director
8 of the National Institute of Standards and Tech-
9 nology,” after “with the Secretary,”.

10 **SEC. 7. MAJOR CYBERSECURITY INCIDENT INDEPENDENT**
11 **EVALUATIONS.**

12 (a) AMENDMENT.—Subchapter II of chapter 35 of
13 title 44, United States Code, is amended by inserting after
14 section 3555 the following new section:

15 **“§ 3555a. Major cybersecurity incident independent**
16 **evaluations**

17 “(a) REQUIREMENT.—Each time an agency experi-
18 ences a major cybersecurity incident, the agency head
19 shall have performed an independent evaluation of such
20 incident.

21 “(b) INCLUSIONS.—An evaluation of a major
22 cybersecurity incident under this section shall be trans-
23 mitted by the agency head to the agencies and committees
24 described in section 3554(c)(1)(A), and shall include—

1 “(1) a description of each major cybersecurity
2 incident including—

3 “(A) threats and threat actors,
4 vulnerabilities, and impacts, including whether
5 the incident involved information that is classi-
6 fied, controlled unclassified information propri-
7 etary, controlled unclassified information pri-
8 vacy, or controlled unclassified information
9 other, as these terms are defined in Office of
10 Management and Budget Memorandum —16-
11 03, dated October 30, 2015, or any successor
12 document;

13 “(B) risk assessments conducted on the
14 system before the incident;

15 “(C) the status of compliance of the af-
16 fected information system with information se-
17 curity requirements at the time of the incident,
18 including—

19 “(i) information security control rec-
20 ommendations made by the agency’s In-
21 spector General that are part of the plan
22 described in section 3554(e)(2);

23 “(ii) information security control rec-
24 ommendations made by the Comptroller

1 General that are part of the plan described
2 in section 3554(e)(1); and

3 “(iii) National Institute of Standards
4 and Technology information security
5 standards that are part of the agency
6 head’s certification described in section
7 3554(c)(1)(A)(iv);

8 “(D) the detection, response, and remedi-
9 ation actions the agency has completed; and

10 “(E) recommendations for research, proc-
11 ess, and policy actions the agency should con-
12 sider taking in response to the incident and to
13 help prevent future incidents of a similar na-
14 ture; and

15 “(2) for each major cybersecurity incident in-
16 volving a breach of personally identifiable informa-
17 tion—

18 “(A) the number of individuals whose in-
19 formation was affected by the incident and a
20 description of the information that was
21 breached or exposed;

22 “(B) an assessment of the risk of harm to
23 affected individuals; and

24 “(C) details of whether and when the agen-
25 cy provided notice to affected individuals about

1 the data breach, including what protections
2 were offered by the breached agency.

3 “(c) ENFORCEMENT.—

4 “(1) IN GENERAL.—If an evaluation of a major
5 cybersecurity incident described in subsection (a) de-
6 termines that the major cybersecurity incident oc-
7 curred in part or in whole because the agency head
8 had failed to comply sufficiently with the informa-
9 tion security requirements, recommendations, or
10 standards described in subsection (b)(1)(C), the Di-
11 rector shall, within 60 days of receiving the evalua-
12 tion, take action under paragraph (2).

13 “(2) ENFORCEMENT ACTIONS.—Enforcement
14 actions the Director may take under this subsection
15 are—

16 “(A) actions described in section
17 11303(b)(5) of title 40, United States Code;
18 and

19 “(B) either—

20 “(i) recommending to the President
21 the removal or demotion of the agency
22 head; or

23 “(ii) action to ensure the agency head
24 does not receive any cash or pay awards or
25 bonuses for a period of 1 year after sub-

1 mission of the explanation required under
2 paragraph (3).

3 “(3) EXPLANATION.—The Director shall pro-
4 vide a detailed explanation for enforcement actions
5 taken under paragraph (2), or for a decision not to
6 act, to the committees described in section
7 3554(e)(1)(A).”.

8 (b) TABLE OF SECTIONS AMENDMENT.—The table of
9 sections for such subchapter is amended by inserting after
10 the item relating to section 3555 the following new item:

“3555a. Major cybersecurity incident independent evaluations.”.