[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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity Responsibility and Accountability Act of 2016''.

SEC. 2. DEFINITIONS.

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

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

(2) by inserting after paragraph (5) the following new paragraph:

''(6) The term 'major cybersecurity incident'has the meaning given the term 'major incident' in Office of Management and Budget Memorandum —16-03, dated October 30, 2015, or any successor document.''.

SEC. 3. AUTHORITY AND FUNCTIONS OF THE DIRECTOR OF NIST.

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

(1) by redesignating subsections (c) through (j) as subsections (d) through (k), respectively; and

(2) by inserting after subsection (b) the following new subsection:

''(c) DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Director of the National Institute of Standards and Technology shall further develop and update as necessary the standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) to fulfill the additional objectives and requirements of the Cybersecurity Responsibility and Accountability Act of

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

''(1) provide to the Director of the Office of Management and Budget a framework and process for agency implementation of such standards and guidelines;

''(2) provide support to agency heads for the implementation of such standards and guidelines and their application to information security policies and principles, as well as with the development of information security training and certification for agency heads;

''(3) conduct cybersecurity research—

''(A) to identify and address prevalent information security challenges, concerns, and knowledge gaps identified by agencies, including those manifested in any of the reports, evaluations, assessments, and plans described in this subchapter that may undermine agencies' information security policies and practices;

''(B) to assess the sufficiency of the current statutory requirements of the Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act of 2014, and their effectiveness

in requiring agencies to implement standards and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and authorized by the Cybersecurity Responsibility and Accountability Act of 2016 regarding information security policies and practices; and

''(C) that shall require the Director of the Office of Management and Budget, the Secretary of Homeland Security, and the heads of other Federal agencies to provide the Director of the National Institute of Standards and Technology any resources, including reports, evaluations, assessments, and plans, that may be required for such research; and

''(4) develop, publish, and update as necessary information security standards and guidelines for national security systems based on established standards and guidelines for information systems.''.

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

(1) in the item relating to section 3553 in the table of sections, by striking ''and the Secretary'' and inserting '', the Secretary, and the Director of

the National Institute of Standards and Technology'';

(2) in the section heading for section 3553, by striking ''**and the Secretary**'' and inserting ''**, the Secretary, and the Director of the National Institute of Standards and Technology**'';

(3) in section 3553(e), as so redesignated by subsection (a)(1) of this section, by striking ''subsection (c)'' and inserting ''subsection (d)'';

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

(A) by striking ''subsection (d)'' and inserting ''subsection (e)''; and

(B) by striking ''subsection (e)'' and inserting ''subsection (f)'';

(5) in section 3554(a)(1)(B)(v), by striking ''section 3553(h)'' and inserting ''section 3553(i)''; and

(6) in section 3555(g)(1), by striking ''section 3553(c)'' and inserting ''section 3553(d)''.

SEC. 4. AGENCY HEADS.

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

(1) in paragraph (1)—

(A) in subparagraph (A)—

(i) in the matter before clause (i), by inserting ''head'' after ''affected agency''; and

(ii) in clause (ii)(IV), by inserting ''head'' after ''when the agency''; and

(B) in subparagraph (B)—

(i) by inserting ''head of the'' after ''notice by the''; and

(ii) by striking ''agency discovers'' inserting ''agency head discovers'';

(2) in paragraph (3)(A)(ii), by striking ''section 3553(c)'' and inserting ''section 3553(d)''; and

(3) in paragraph (4), by inserting ''the National Institute of Standards and Technology and'' after ''such notice to''.

SEC. 5. FEDERAL AGENCY HEAD RESPONSIBILITIES.

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

(1) in subsection (a)(3)(A)—

(A) by striking ''designating a senior agency information security officer'' and inserting ''collaborating with the agency head to designate a Chief Information Security Officer'';

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

(C) by inserting before clause (ii), as so redesignated, the following new clause:

''(i) have the job description and responsibilities that shall be provided in guidance issued by the Director, developed in consultation with the Director of the National Institute of Standards and Technology and the Secretary, within 6 months after the date of enactment of the Cybersecurity Responsibility and Accountability Act of 2016;'';

(D) in clause (iv), as so redesignated, by striking ''and'' at the end;

(E) in clause (v), as so redesignated, by inserting ''and'' after the semicolon at the end; and

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

''(vi) be designated without increasing the number of full-time equivalent employee positions at the agency;'';

(2) in subsection (b)—

(A) by redesignating paragraphs (5) through (8) as paragraphs (6) through (9), respectively; and

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

''(5) mandatory annual information security training and certification designed specifically for the agency head, developed and updated as necessary by the National Institute of Standards and Technology, the purpose of which shall be to ensure that the agency head has an understanding of Federal cybersecurity policy, including an understanding of—

''(A) the information and information systems that support the operations and assets of the agency, using nontechnical terms as much as possible;

''(B) the potential impact of common types of cyber-attacks and data breaches on the agency's operations and assets;

''(C) how cyber-attacks and data breaches occur;

''(D) steps the agency head and agency employees should take to protect their information and information systems, including not

using private messaging system software or private e-mail servers for official communications; and

''(E) the annual reporting requirements required of the agency head under subsection (c), including the certifications required under subsection (c)(1)(A)(iv);'';

(3) in subsection (c)—

(A) in paragraph (1)(A)—

(i) by striking ''Each agency'' and inserting ''The head of each agency'';

(ii) by inserting ''the Director of the National Institute of Standards and Technology,'' after ''the Director, the Secretary,'';

(iii) by inserting '', Space, and Technology'' after ''the Committee on Science'';

(iv) by striking ''and'' at the end of clause (iii)(II);

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

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

''(iv) specific written certification by the agency head that—

''(I) certifies that information security standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) are being met by the agency;

''(II) identifies the security controls in place at the agency and how they each meet the relevant information security standard;

''(III) may be based on or informed by the assessment described in section 3553(d)(4); and

''(IV) for any information security standard that the agency does not meet, provides the reasons therefor and includes documentation of the Director's certification of the agency not meeting the standard; and''; and

(B) in paragraph (2), by striking ''Each agency'' and inserting ''The head of each agency'';

(4) in subsection (d), by striking ''each agency'' and inserting ''the head of each agency'';

(5) by redesignating subsection (e) as subsection (f);

(6) by inserting after subsection (d) the following new subsection:

''(e) PLANS FOR IMPLEMENTATION OF RECOMMENDATIONS.—

''(1) COMPTROLLER GENERAL RECOMMENDATIONS.—

''(A) IN GENERAL.—In addition to the requirements of subsections (c) and (d), each agency head shall, not later than 6 months after the date of enactment of the Cybersecurity Responsibility and Accountability Act of 2016, develop a plan, in consultation with the Comptroller General, to implement all of the Comptroller General's recommendations regarding information security controls relevant to that agency.

''(B) PLAN.—The plan required under subparagraph (A)—

''(i) shall be submitted to the agencies and committees described in subsection (c)(1)(A);

''(ii) shall include a schedule for implementation of the Comptroller General's

recommendations, including a completion deadline;

''(iii) shall be updated annually, and such annual updates shall be included in the annual report described in subsection (c)(1)(A); and

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

''(C) IF NO RECOMMENDATIONS.—If the Comptroller General does not have any relevant recommendations for an agency head to implement relative to information security controls, then the agency head shall accordingly notify the agencies and committees described in subsection (c)(1)(A).

''(D) REASONS FOR FAILURE TO IMPLEMENT.—If there are any Comptroller General recommendations that an agency head does not implement, the agency head shall provide the reasons for that failure to the Director for the Director's approval. For each unimplemented recommendation, the plan shall include either the Director's approval or a certification by the

Director of the agency head's failure to implement such recommendation.

''(2) INSPECTOR GENERAL RECOMMENDATIONS.—

''(A) IN GENERAL.—In addition to the requirements of subsections (c) and (d), each agency head shall, not later than 6 months after the date of enactment of the Cybersecurity Responsibility and Accountability Act of 2016, develop a plan, in consultation with its Inspector General, to implement all of the Inspector General's recommendations regarding the agency's information security program.

''(B) PLAN.—The plan required under subparagraph (A)—

''(i) shall be submitted to the agencies and committees described in subsection (c)(1)(A);

''(ii) shall include a schedule for implementation of the Inspector General's recommendations, including a completion deadline;

''(iii) shall be updated annually, and such annual updates shall be included in

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

''(iv) may, as appropriate, be based on or informed by recommendations included in—

''(I) the evaluation described in section 3555(b)(1); or

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

''(C) IF NO RECOMMENDATIONS.—If the Inspector General does not have any relevant information security control recommendations for the agency head to implement, then the agency head shall accordingly notify the agencies and committees described in subsection (c)(1)(A).

''(D) REASONS FOR FAILURE TO IMPLEMENT.—If there are any Inspector General recommendations that the agency head does not implement, the agency head shall provide the reasons for that failure to the Director for the Director's approval. For each unimplemented recommendation, the plan shall include either the Director's approval or a certification by the

Director of the agency head's failure to implement such recommendation.''; and

(7) in subsection (f), as so redesignated, by striking ''Each agency'' and inserting ''The head of each agency''.

SEC. 6. ANNUAL INDEPENDENT EVALUATION.

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

(1) in subsection (a)(1), by inserting ''head'' after ''each agency'';

(2) in subsection (b)(1), by inserting ''and evaluations required by section 3555a'' after ''required by this section'';

(3) in subsection (c), by striking ''that portion of the evaluation required by this section'' and inserting ''the portions of evaluations required by this section or section 3555a'';

(4) in subsection (e)(2), by inserting ''or section 3555a'' after ''required under this section'';

(5) in subsection (f), by striking ''Agencies'' and inserting ''In carrying out this section and section 3555a, agencies'';

(6) in subsection (g)(3), by inserting ''under this section or section 3555a'' after ''Evaluations'';

(7) in subsection (i)—

(A) by striking ''the head of an agency'' and inserting ''an agency head'';

(B) by striking ''head of an agency'' and inserting ''agency head''; and

(C) by inserting ''or section 3555a'' after ''under this section''; and

(8) in subsection (j), by inserting ''the Director of the National Institute of Standards and Technology,'' after ''with the Secretary,''.

SEC. 7. MAJOR CYBERSECURITY INCIDENT INDEPENDENT EVALUATIONS.

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

''§ 3555a. Major cybersecurity incident independent evaluations

''(a) REQUIREMENT.—Each time an agency experiences a major cybersecurity incident, the agency head shall have performed an independent evaluation of such incident.

''(b) INCLUSIONS.—An evaluation of a major cybersecurity incident under this section shall be transmitted by the agency head to the agencies and committees described in section 3554(c)(1)(A), and shall include—

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

''(A) threats and threat actors, vulnerabilities, and impacts, including whether the incident involved information that is classified, controlled unclassified information proprietary, controlled unclassified information privacy, or controlled unclassified information other, as these terms are defined in Office of Management and Budget Memorandum —16-03, dated October 30, 2015, or any successor document;

''(B) risk assessments conducted on the system before the incident;

''(C) the status of compliance of the affected information system with information security requirements at the time of the incident, including—

''(i) information security control recommendations made by the agency's Inspector General that are part of the plan described in section 3554(e)(2);

''(ii) information security control recommendations made by the Comptroller

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

''(iii) National Institute of Standards and Technology information security standards that are part of the agency head's certification described in section 3554(c)(1)(A)(iv);

''(D) the detection, response, and remediation actions the agency has completed; and

''(E) recommendations for research, process, and policy actions the agency should consider taking in response to the incident and to help prevent future incidents of a similar nature; and

''(2) for each major cybersecurity incident involving a breach of personally identifiable information—

''(A) the number of individuals whose information was affected by the incident and a description of the information that was breached or exposed;

''(B) an assessment of the risk of harm to affected individuals; and

''(C) details of whether and when the agency provided notice to affected individuals about

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

''(c) ENFORCEMENT.—

''(1) IN GENERAL.—If an evaluation of a major cybersecurity incident described in subsection (a) determines that the major cybersecurity incident occurred in part or in whole because the agency head had failed to comply sufficiently with the information security requirements, recommendations, or standards described in subsection (b)(1)(C), the Director shall, within 60 days of receiving the evaluation, take action under paragraph (2).

''(2) ENFORCEMENT ACTIONS.—Enforcement actions the Director may take under this subsection are—

''(A) actions described in section 11303(b)(5) of title 40, United States Code; and

''(B) either—

''(i) recommending to the President the removal or demotion of the agency head; or

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

mission of the explanation required under paragraph (3).

''(3) EXPLANATION.—The Director shall provide a detailed explanation for enforcement actions taken under paragraph (2), or for a decision not to act, to the committees described in section 3554(c)(1)(A).''.

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

''3555a. Major cybersecurity incident independent evaluations.''.