

114TH CONGRESS
1ST SESSION

S. _____

To improve federal network security and authorize and enhance an existing intrusion detection and prevention system for civilian federal networks.

IN THE SENATE OF THE UNITED STATES

Mr. CARPER (for himself and Mr. JOHNSON) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To improve federal network security and authorize and enhance an existing intrusion detection and prevention system for civilian federal networks.

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 “Federal Cybersecurity
5 Enhancement Act of 2015”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act—

1 (1) the term “agency” has the meaning given
2 the term in section 3502 of title 44, United States
3 Code;

4 (2) the term “agency information system” has
5 the meaning given the term in section 228 of the
6 Homeland Security Act of 2002, as added by section
7 3(a);

8 (3) the term “appropriate congressional com-
9 mittees” means—

10 (A) the Committee on Homeland Security
11 and Governmental Affairs of the Senate; and

12 (B) the Committee on Homeland Security
13 of the House of Representatives;

14 (4) the terms “cybersecurity risk” and “infor-
15 mation system” have the meanings given those
16 terms in section 227 of the Homeland Security Act
17 of 2002, as so redesignated by section 3(a);

18 (5) the term “Director” means the Director of
19 the Office of Management and Budget;

20 (6) the term “intelligence community” has the
21 meaning given the term in section 3(4) of the Na-
22 tional Security Act of 1947 (50 U.S.C. 3003(4));
23 and

24 (7) the term “Secretary” means the Secretary
25 of Homeland Security.

1 **SEC. 3. IMPROVED FEDERAL NETWORK SECURITY.**

2 (a) IN GENERAL.—Subtitle C of title II of the Home-
3 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-
4 ed—

5 (1) by redesignating section 228 as section 229;

6 (2) by redesignating section 227 as subsection
7 (c) of section 228, as added by paragraph (4), and
8 adjusting the margins accordingly;

9 (3) by redesignating the second section des-
10 igned as section 226 (relating to the national cy-
11 bersecurity and communications integration center)
12 as section 227;

13 (4) by inserting after section 227, as so redesign-
14 nated, the following:

15 **“SEC. 228. CYBERSECURITY PLANS.**

16 **“(a) DEFINITIONS.—**In this section—

17 **“(1)** the term ‘agency information system’
18 means an information system used or operated by an
19 agency, by a contractor of an agency, or by another
20 entity on behalf of an agency;

21 **“(2)** the terms ‘cybersecurity risk’ and ‘infor-
22 mation system’ have the meanings given those terms
23 in section 227;

24 **“(3)** the term ‘information sharing and analysis
25 organization’ has the meaning given the term in sec-
26 tion 212(5); and

1 “(4) the term ‘intelligence community’ has the
2 meaning given the term in section 3(4) of the Na-
3 tional Security Act of 1947 (50 U.S.C. 3003(4)).

4 “(b) INTRUSION ASSESSMENT PLAN.—

5 “(1) REQUIREMENT.—The Secretary, in coordi-
6 nation with the Director of the Office of Manage-
7 ment and Budget, shall develop and implement an
8 intrusion assessment plan to identify and remove in-
9 truders in agency information systems.

10 “(2) EXCEPTION.—The intrusion assessment
11 plan required under paragraph (1) shall not apply to
12 the Department of Defense or an element of the in-
13 telligence community.”;

14 (5) in section 228(c), as so redesignated, by
15 striking “section 226” and inserting “section 227”;
16 and

17 (6) by inserting after section 229, as so redesign-
18 ated, the following:

19 **“SEC. 230. FEDERAL INTRUSION DETECTION AND PREVEN-**
20 **TION SYSTEM.**

21 “(a) DEFINITIONS.—In this section—

22 “(1) the term ‘agency’ has the meaning given
23 that term in section 3502 of title 44, United States
24 Code;

1 “(2) the term ‘agency information’ means infor-
2 mation collected or maintained by or on behalf of an
3 agency;

4 “(3) the term ‘agency information system’ has
5 the meaning given the term in section 228; and

6 “(4) the terms ‘cybersecurity risk’ and ‘infor-
7 mation system’ have the meanings given those terms
8 in section 227.

9 “(b) REQUIREMENT.—

10 “(1) IN GENERAL.—Not later than 1 year after
11 the date of enactment of this section, the Secretary
12 shall deploy, operate, and maintain, to make avail-
13 able for use by any agency, with or without reim-
14 bursement—

15 “(A) a capability to detect cybersecurity
16 risks in network traffic transiting or traveling
17 to or from an agency information system; and

18 “(B) a capability to prevent network traffic
19 associated with such cybersecurity risks from
20 transiting or traveling to or from an agency in-
21 formation system or modify such network traf-
22 fic to remove the cybersecurity risk.

23 “(2) REGULAR IMPROVEMENT.—The Secretary
24 shall regularly deploy new technologies and modify
25 existing technologies to the intrusion detection and

1 prevention capabilities described in paragraph (1) as
2 appropriate to improve the intrusion detection and
3 prevention capabilities.

4 “(c) ACTIVITIES.—In carrying out subsection (b), the
5 Secretary—

6 “(1) may access, and the head of an agency
7 may disclose to the Secretary or a private entity pro-
8 viding assistance to the Secretary under paragraph
9 (2), information transiting or traveling to or from an
10 agency information system, regardless of the location
11 from which the Secretary or a private entity pro-
12 viding assistance to the Secretary under paragraph
13 (2) accesses such information, notwithstanding any
14 other provision of law that would otherwise restrict
15 or prevent the head of an agency from disclosing
16 such information to the Secretary or a private entity
17 providing assistance to the Secretary under para-
18 graph (2);

19 “(2) may enter into contracts or other agree-
20 ments with, or otherwise request and obtain the as-
21 sistance of, private entities to deploy and operate
22 technologies in accordance with subsection (b);

23 “(3) may retain, use, and disclose information
24 obtained through the conduct of activities authorized

1 under this section only to protect information and
2 information systems from cybersecurity risks;

3 “(4) shall regularly assess through operational
4 test and evaluation in real world or simulated envi-
5 ronments available advanced protective technologies
6 to improve detection and prevention capabilities, in-
7 cluding commercial and non-commercial technologies
8 and detection technologies beyond signature-based
9 detection, and utilize such technologies when appro-
10 priate;

11 “(5) shall establish a pilot to acquire, test, and
12 deploy, as rapidly as possible, technologies described
13 in paragraph (4); and

14 “(6) shall periodically update the privacy im-
15 pact assessment required under section 208(b) of
16 the E-Government Act of 2002 (44 U.S.C. 3501
17 note).

18 “(d) PRIVATE ENTITIES.—

19 “(1) CONDITIONS.—A private entity described
20 in subsection (c)(2) may not—

21 “(A) disclose any network traffic transiting
22 or traveling to or from an agency information
23 system to any entity other than the Department
24 or the agency that disclosed the information
25 under subsection (c)(1); or

1 “(B) use any network traffic transiting or
2 traveling to or from an agency information sys-
3 tem to which the private entity gains access in
4 accordance with this section for any purpose
5 other than to protect agency information and
6 agency information systems against cybersecu-
7 rity risks or to administer a contract or other
8 agreement entered into pursuant to subsection
9 (c)(2) or as part of another contract with the
10 Secretary.

11 “(2) LIMITATION ON LIABILITY.—No cause of
12 action shall lie in any court against a private entity
13 for assistance provided to the Secretary in accord-
14 ance with this section and any contract or agree-
15 ment entered into pursuant to subsection (c)(2).”.

16 (b) PRIORITIZING ADVANCED SECURITY TOOLS.—
17 The Director and the Secretary, in consultation with ap-
18 propriate agencies, shall—

19 (1) review and update governmentwide policies
20 and programs to ensure appropriate prioritization
21 and use of network security monitoring tools within
22 agency networks; and

23 (2) brief appropriate congressional committees
24 on such prioritization and use.

25 (c) AGENCY RESPONSIBILITIES.—

1 (1) IN GENERAL.—Except as provided in para-
2 graph (2)—

3 (A) not later than 1 year after the date of
4 enactment of this Act or 2 months after the
5 date on which the Secretary makes available the
6 intrusion detection and prevention capabilities
7 under section 230(b)(1) of the Homeland Secu-
8 rity Act of 2002, as added by subsection (a),
9 whichever is later, the head of each agency shall
10 apply and continue to utilize the capabilities to
11 all information traveling between an agency in-
12 formation system and any information system
13 other than an agency information system; and

14 (B) not later than 6 months after the date
15 on which the Secretary makes available im-
16 provements to the intrusion detection and pre-
17 vention capabilities pursuant to section
18 230(b)(2) of the Homeland Security Act of
19 2002, as added by subsection (a), the head of
20 each agency shall apply and continue to utilize
21 the improved intrusion detection and prevention
22 capabilities.

23 (2) EXCEPTION.—The requirements under
24 paragraph (1) shall not apply to the Department of
25 Defense or an element of the intelligence community.

1 (d) TABLE OF CONTENTS AMENDMENT.—The table
2 of contents in section 1(b) of the Homeland Security Act
3 of 2002 (6 U.S.C. 101 note) is amended by striking the
4 items relating to the first section designated as section
5 226, the second section designated as section 226 (relating
6 to the national cybersecurity and communications integra-
7 tion center), section 227, and section 228 and inserting
8 the following:

“Sec. 226. Cybersecurity recruitment and retention.

“Sec. 227. National cybersecurity and communications integration center.

“Sec. 228. Cybersecurity plans.

“Sec. 229. Clearances.

“Sec. 230. Federal intrusion detection and prevention system.”.

9 **SEC. 4. ADVANCED INTERNAL DEFENSES.**

10 (a) ADVANCED NETWORK SECURITY TOOLS.—

11 (1) IN GENERAL.—The Secretary shall include
12 in the Continuous Diagnostics and Mitigation Pro-
13 gram advanced network security tools to improve
14 visibility of network activity, including through the
15 use of commercial and free or open source tools, to
16 detect and mitigate intrusions and anomalous activ-
17 ity.

18 (2) DEVELOPMENT OF PLAN.—The Director
19 shall develop and implement a plan to ensure that
20 each agency utilizes advanced network security tools,
21 including those described in paragraph (1), to detect
22 and mitigate intrusions and anomalous activity.

1 (b) IMPROVED METRICS.—The Secretary, in collabo-
2 ration with the Director, shall review and update the
3 metrics used to measure security under section 3554 of
4 title 44, United States Code, to include measures of intru-
5 sion and incident detection and response times.

6 (c) TRANSPARENCY AND ACCOUNTABILITY.—The Di-
7 rector, in consultation with the Secretary, shall increase
8 transparency to the public on agency cybersecurity pos-
9 ture, including by increasing the number of metrics avail-
10 able on Federal Government performance websites and, to
11 the greatest extent practicable, displaying metrics for de-
12 partment components, small agencies, and micro agencies.

13 (d) MAINTENANCE OF TECHNOLOGIES.—Section
14 3553(b)(6)(B) of title 44, United States Code, is amended
15 by inserting “, operating, and maintaining” after “deploy-
16 ing”.

17 **SEC. 5. FEDERAL CYBERSECURITY BEST PRACTICES.**

18 (a) ASSESSMENT OF BEST PRACTICES FOR FEDERAL
19 CYBERSECURITY.—The Secretary, in consultation with
20 the Director, shall regularly assess and require implemen-
21 tation of best practices for securing agency information
22 systems against intrusion and preventing data exfiltration
23 in the event of an intrusion.

24 (b) CYBERSECURITY REQUIREMENTS AT AGEN-
25 CIES.—

1 (1) IN GENERAL.—Except as provided in para-
2 graph (2), not later than 1 year after the date of en-
3 actment of this Act, the head of each agency shall—

4 (A) identify sensitive and mission critical
5 data stored by the agency consistent with the
6 inventory required under the first subsection (c)
7 (relating to the inventory of major information
8 systems) and the second subsection (c) (relating
9 to the inventory of information systems) of sec-
10 tion 3505 of title 44, United States Code;

11 (B) assess access controls to the data de-
12 scribed in subparagraph (A), the need for read-
13 ily accessible storage of the data, and individ-
14 uals' need to access the data;

15 (C) encrypt the data described in subpara-
16 graph (A) that is stored on or transiting agency
17 information systems consistent with standards
18 and guidelines promulgated under section
19 11331 of title 40, United States Code;

20 (D) implement a single sign-on trusted
21 identity platform for individuals accessing each
22 public website of the agency that requires user
23 authentication, as developed by the Adminis-
24 trator of General Services in collaboration with
25 the Secretary; and

1 (E) implement multi-factor authentication
2 consistent with standards and guidelines pro-
3 mulgated under section 11331 of title 40,
4 United States Code, for—

5 (i) remote access to an agency infor-
6 mation system; and

7 (ii) each user account with elevated
8 privileges on an agency information sys-
9 tem.

10 (2) EXCEPTION.—The requirements under
11 paragraph (1) shall not apply to the Department of
12 Defense or an element of the intelligence community.

13 **SEC. 6. ASSESSMENT; REPORTS.**

14 (a) DEFINITIONS.—In this section—

15 (1) the term “intrusion assessments” means ac-
16 tions taken under the intrusion assessment plan to
17 identify and remove intruders in agency information
18 systems;

19 (2) the term “intrusion assessment plan”
20 means the plan required under section 228(b)(1) of
21 the Homeland Security Act of 2002, as added by
22 section 3(a) of this Act; and

23 (3) the term “intrusion detection and preven-
24 tion capabilities” means the capabilities required

1 under section 230(b) of the Homeland Security Act
2 of 2002, as added by section 3(a) of this Act.

3 (b) THIRD PARTY ASSESSMENT.—Not later than 3
4 years after the date of enactment of this Act, the Govern-
5 ment Accountability Office shall conduct a study and pub-
6 lish a report on the effectiveness of the approach and
7 strategy of the Federal Government to securing agency in-
8 formation systems, including the intrusion detection and
9 prevention capabilities and the intrusion assessment plan.

10 (c) REPORTS TO CONGRESS.—

11 (1) INTRUSION DETECTION AND PREVENTION
12 CAPABILITIES.—

13 (A) SECRETARY OF HOMELAND SECURITY
14 REPORT.—Not later than 6 months after the
15 date of enactment of this Act, and annually
16 thereafter, the Secretary shall submit to the ap-
17 propriate congressional committees a report on
18 the status of implementation of the intrusion
19 detection and prevention capabilities, includ-
20 ing—

21 (i) a description of privacy controls;

22 (ii) a description of the technologies
23 and capabilities utilized to detect cyberse-
24 curity risks in network traffic, including
25 the extent to which those technologies and

1 capabilities include existing commercial
2 and non-commercial technologies;

3 (iii) a description of the technologies
4 and capabilities utilized to prevent network
5 traffic associated with cybersecurity risks
6 from transiting or traveling to or from
7 agency information systems, including the
8 extent to which those technologies and ca-
9 pabilities include existing commercial and
10 non-commercial technologies;

11 (iv) a list of the types of indicators or
12 other identifiers or techniques used to de-
13 tect cybersecurity risks in network traffic
14 transiting or traveling to or from agency
15 information systems on each iteration of
16 the intrusion detection and prevention ca-
17 pabilities and the number of each such
18 type of indicator, identifier, and technique;

19 (v) the number of instances in which
20 the intrusion detection and prevention ca-
21 pabilities detected a cybersecurity risk in
22 network traffic transiting or traveling to or
23 from agency information systems and the
24 number of times the intrusion detection
25 and prevention capabilities blocked net-

1 work traffic associated with cybersecurity
2 risk; and

3 (vi) a description of the pilot estab-
4 lished under section 230(e)(5) of the
5 Homeland Security Act of 2002, as added
6 by section 3(a) of this Act, including the
7 number of new technologies tested and the
8 number of participating agencies.

9 (B) OMB REPORT.—Not later than 18
10 months after the date of enactment of this Act,
11 and annually thereafter, the Director shall sub-
12 mit to Congress, as part of the report required
13 under section 3553(c) of title 44, United States
14 Code, an analysis of agency application of the
15 intrusion detection and prevention capabilities,
16 including—

17 (i) a list of each agency and the de-
18 gree to which each agency has applied the
19 intrusion detection and prevention capabili-
20 ties to an agency information system; and

21 (ii) a list by agency of—

22 (I) the number of instances in
23 which the intrusion detection and pre-
24 vention capabilities detected a cyber-
25 security risk in network traffic

1 transiting or traveling to or from an
2 agency information system and the
3 types of indicators, identifiers, and
4 techniques used to detect such cyber-
5 security risks; and

6 (II) the number of instances in
7 which the intrusion detection and pre-
8 vention capabilities prevented network
9 traffic associated with a cybersecurity
10 risk from transiting or traveling to or
11 from an agency information system
12 and the types of indicators, identi-
13 fiers, and techniques used to detect
14 such agency information systems.

15 (2) OMB REPORT ON DEVELOPMENT AND IM-
16 PLEMENTATION OF INTRUSION ASSESSMENT PLAN,
17 ADVANCED INTERNAL DEFENSES, AND FEDERAL CY-
18 BERSECURITY BEST PRACTICES.—The Director
19 shall—

20 (A) not later than 6 months after the date
21 of enactment of this Act, and 30 days after any
22 update thereto, submit the intrusion assessment
23 plan to the appropriate congressional commit-
24 tees;

1 (B) not later than 1 year after the date of
2 enactment of this Act, and annually thereafter,
3 submit to Congress, as part of the report re-
4 quired under section 3553(c) of title 44, United
5 States Code—

6 (i) a description of the implementation
7 of the intrusion assessment plan;

8 (ii) the findings of the intrusion as-
9 sessments conducted pursuant to the intru-
10 sion assessment plan;

11 (iii) advanced network security tools
12 included in the Continuous Diagnostics
13 and Mitigation Program pursuant to sec-
14 tion 4(a)(1);

15 (iv) the results of the assessment of
16 the Secretary of best practices for Federal
17 cybersecurity pursuant to section 5(a); and

18 (v) a list by agency of compliance with
19 the requirements of section 5(b); and

20 (C) not later than 1 year after the date of
21 enactment of this Act, submit to the appro-
22 priate congressional committees—

23 (i) a copy of the plan developed pursu-
24 ant to section 4(a)(2); and

1 (ii) the improved metrics developed
2 pursuant to section 4(b).

3 **SEC. 7. TERMINATION.**

4 (a) IN GENERAL.—The authority provided under sec-
5 tion 230 of the Homeland Security Act of 2002, as added
6 by section 3(a) of this Act, and the reporting requirements
7 under section 6(c) shall terminate on the date that is 7
8 years after the date of enactment of this Act.

9 (b) RULE OF CONSTRUCTION.—Nothing in sub-
10 section (a) shall be construed to affect the limitation of
11 liability of a private entity for assistance provided to the
12 Secretary under section 230(d)(2) of the Homeland Secu-
13 rity Act of 2002, as added by section 3(a) of this Act,
14 if such assistance was rendered before the termination
15 date under subsection (a) or otherwise during a period in
16 which the assistance was authorized.