

Calendar No. 673114TH CONGRESS
2^D SESSION**S. 1869****[Report No. 114–378]**

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

JULY 27, 2015

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

NOVEMBER 17, 2016

Reported by Mr. JOHNSON, with amendments

[Omit the part struck through and insert the part printed in *italie*]

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “~~Federal Cybersecurity~~
3 ~~Enhancement Act of 2015~~” “*Federal Cybersecurity En-*
4 *hancement Act of 2016*”.

5 **SEC. 2. DEFINITIONS.**

6 In this Act—

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

10 (2) the term “agency information system” has
11 the meaning given the term in section 228 of the
12 Homeland Security Act of 2002, as added by section
13 3(a);

14 (3) the term “appropriate congressional com-
15 mittees” means—

16 (A) the Committee on Homeland Security
17 and Governmental Affairs of the Senate; and

18 (B) the Committee on Homeland Security
19 of the House of Representatives;

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

24 (5) the term “Director” means the Director of
25 the Office of Management and Budget;

1 (6) 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 and

5 (7) the term “Secretary” means the Secretary
6 of Homeland Security.

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

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

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

12 (2) by redesignating section 227 as subsection
13 (c) of section 228, as added by paragraph (4), and
14 adjusting the margins accordingly;

15 (3) by redesignating the second section des-
16 igned as section 226 (relating to the national cy-
17 bersecurity and communications integration center)
18 as section 227;

19 (4) by inserting after section 227, as so redesign-
20 ated, the following:

21 **“SEC. 228. CYBERSECURITY PLANS.**

22 “(a) DEFINITIONS.—In this section—

23 “(1) the term ‘agency information system’
24 means an information system used or operated by an

1 agency, by a contractor of an agency, or by another
2 entity on behalf of an agency;

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

6 ~~“(3) the term ‘information sharing and analysis
7 organization’ has the meaning given the term in sec-
8 tion 212(5); and~~

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

12 “(b) INTRUSION ASSESSMENT PLAN.—

13 “(1) REQUIREMENT.—The Secretary, in coordi-
14 nation with the Director of the Office of Manage-
15 ment and Budget, shall develop and implement an
16 intrusion assessment plan to identify and remove in-
17 truders in agency information systems.

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

22 (5) in section 228(c), as so redesignated, by
23 striking “section 226” and inserting “section 227”;
24 and

1 (6) by inserting after section 229, as so redesignated,
2 nated, the following:

3 **“SEC. 230. FEDERAL INTRUSION DETECTION AND PREVEN-**
4 **TION SYSTEM.**

5 “(a) DEFINITIONS.—In this section—

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

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

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

14 “(4) the terms ‘cybersecurity risk’ and ‘infor-
15 mation system’ have the meanings given those terms
16 in section 227.

17 “(b) REQUIREMENT.—

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

23 “(A) a capability to detect cybersecurity
24 risks in network traffic transiting or traveling
25 to or from an agency information system; and

1 “(B) a capability to prevent network traffic
2 associated with such cybersecurity risks from
3 transiting or traveling to or from an agency in-
4 formation system or modify such network traf-
5 fic to remove the cybersecurity risk.

6 “(2) REGULAR IMPROVEMENT.—The Secretary
7 shall regularly deploy new technologies and modify
8 existing technologies to the intrusion detection and
9 prevention capabilities described in paragraph (1) as
10 appropriate to improve the intrusion detection and
11 prevention capabilities.

12 “(c) ACTIVITIES.—In carrying out subsection (b), the
13 Secretary—

14 “(1) may access, and the head of an agency
15 may disclose to the Secretary or a private entity pro-
16 viding assistance to the Secretary under paragraph
17 (2), information transiting or traveling to or from an
18 agency information system, regardless of the location
19 from which the Secretary or a private entity pro-
20 viding assistance to the Secretary under paragraph
21 (2) accesses such information, notwithstanding any
22 other provision of law that would otherwise restrict
23 or prevent the head of an agency from disclosing
24 such information to the Secretary or a private entity

1 providing assistance to the Secretary under para-
2 graph (2);

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

7 “(3) may retain, use, and disclose information
8 obtained through the conduct of activities authorized
9 under this section only to protect information and
10 information systems from cybersecurity risks;

11 “(4) shall regularly assess through operational
12 test and evaluation in real world or simulated envi-
13 ronments available advanced protective technologies
14 to improve detection and prevention capabilities, in-
15 cluding commercial and non-commercial technologies
16 and detection technologies beyond signature-based
17 detection, and utilize such technologies when appro-
18 priate;

19 “(5) shall establish a pilot to acquire, test, and
20 deploy, as rapidly as possible, technologies described
21 in paragraph (4); ~~and~~

22 “(6) shall periodically update the privacy im-
23 pact assessment required under section 208(b) of
24 the E-Government Act of 2002 (44 U.S.C. 3501
25 note); *and*

1 “(7) shall ensure that—

2 “(A) activities carried out under this sec-
3 tion are reasonably necessary for the purpose of
4 protecting agency information and agency infor-
5 mation systems from a cybersecurity risk;

6 “(B) information accessed by the Secretary
7 will be retained no longer than reasonably nec-
8 essary for the purpose of protecting agency infor-
9 mation and agency information systems from a
10 cybersecurity risk;

11 “(C) notice has been provided to users of an
12 agency information system concerning access to
13 communications of users of the agency informa-
14 tion system for the purpose of protecting agency
15 information and the agency information system;
16 and

17 “(D) the activities are implemented pursu-
18 ant to policies and procedures governing the op-
19 eration of the intrusion detection and prevention
20 capabilities.

21 “(d) PRIVATE ENTITIES.—

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

24 “(A) disclose any network traffic transiting
25 or traveling to or from an agency information

1 system to any entity other than the Department
2 or the agency that disclosed the information
3 under subsection (c)(1); or

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

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

19 “(3) *RULE OF CONSTRUCTION.*—*Nothing in*
20 *paragraph (2) shall be construed to authorize an*
21 *Internet service provider to break a user agreement*
22 *with a customer.*

23 “(e) *ATTORNEY GENERAL REVIEW.*—*Not later than 1*
24 *year after the date of enactment of this section, the Attorney*
25 *General shall review the policies and guidelines for the pro-*

1 *gram carried out under this section to ensure that the poli-*
2 *cies and guidelines are consistent with applicable law gov-*
3 *erning the acquisition, interception, retention, use, and dis-*
4 *closure of communications.”.*

5 (b) **PRIORITIZING ADVANCED SECURITY TOOLS.—**

6 The Director and the Secretary, in consultation with ap-
7 propriate agencies, shall—

8 (1) review and update Governmentwide policies
9 and programs to ensure appropriate prioritization
10 and use of network security monitoring tools within
11 agency networks; and

12 (2) brief appropriate congressional committees
13 on such prioritization and use.

14 (c) **AGENCY RESPONSIBILITIES.—**

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

17 (A) not later than 1 year after the date of
18 enactment of this Act or 2 months after the
19 date on which the Secretary makes available the
20 intrusion detection and prevention capabilities
21 under section 230(b)(1) of the Homeland Secu-
22 rity Act of 2002, as added by subsection (a),
23 whichever is later, the head of each agency shall
24 apply and continue to utilize the capabilities to
25 all information traveling between an agency in-

1 formation system and any information system
2 other than an agency information system; and

3 (B) not later than 6 months after the date
4 on which the Secretary makes available im-
5 provements to the intrusion detection and pre-
6 vention capabilities pursuant to section
7 230(b)(2) of the Homeland Security Act of
8 2002, as added by subsection (a), the head of
9 each agency shall apply and continue to utilize
10 the improved intrusion detection and prevention
11 capabilities.

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

15 (d) TABLE OF CONTENTS AMENDMENT.—The table
16 of contents in section 1(b) of the Homeland Security Act
17 of 2002 (6 U.S.C. 101 note) is amended by striking the
18 items relating to the first section designated as section
19 226, the second section designated as section 226 (relating
20 to the national cybersecurity and communications integra-
21 tion center), section 227, and section 228 and inserting
22 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.”.

1 **SEC. 4. ADVANCED INTERNAL DEFENSES.**

2 (a) **ADVANCED NETWORK SECURITY TOOLS.**—

3 (1) **IN GENERAL.**—The Secretary shall include
4 in the Continuous Diagnostics and Mitigation Pro-
5 gram advanced network security tools to improve
6 visibility of network activity, including through the
7 use of commercial and free or open source tools, to
8 detect and mitigate intrusions and anomalous activ-
9 ity.

10 (2) **DEVELOPMENT OF PLAN.**—The Director
11 shall develop and implement a plan to ensure that
12 each agency utilizes advanced network security tools,
13 including those described in paragraph (1), to detect
14 and mitigate intrusions and anomalous activity.

15 (b) **IMPROVED METRICS.**—The Secretary, in collabo-
16 ration with the Director, shall review and update the
17 metrics used to measure security under section 3554 of
18 title 44, United States Code, to include measures of intru-
19 sion and incident detection and response times.

20 (c) **TRANSPARENCY AND ACCOUNTABILITY.**—The Di-
21 rector, in consultation with the Secretary, shall increase
22 transparency to the public on agency cybersecurity pos-
23 ture, including by increasing the number of metrics avail-
24 able on Federal Government performance websites and, to
25 the greatest extent practicable, displaying metrics for de-
26 partment components, small agencies, and micro agencies.

1 (d) MAINTENANCE OF TECHNOLOGIES.—Section
2 3553(b)(6)(B) of title 44, United States Code, is amended
3 by inserting “, operating, and maintaining” after “deploy-
4 ing”.

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

6 (a) ASSESSMENT OF BEST PRACTICES FOR FEDERAL
7 CYBERSECURITY.—The Secretary, in consultation with
8 the Director, shall regularly assess and require implemen-
9 tation of best practices for securing agency information
10 systems against intrusion and preventing data exfiltration
11 in the event of an intrusion.

12 (b) CYBERSECURITY REQUIREMENTS AT AGEN-
13 CIES.—

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

17 (A) identify sensitive and mission critical
18 data stored by the agency consistent with the
19 inventory required under the first subsection (c)
20 (relating to the inventory of major information
21 systems) and the second subsection (c) (relating
22 to the inventory of information systems) of sec-
23 tion 3505 of title 44, United States Code;

24 (B) assess access controls to the data de-
25 scribed in subparagraph (A), the need for read-

1 ily accessible storage of the data, and individ-
2 uals' need to access the data;

3 (C) encrypt the data described in subpara-
4 graph (A) that is stored on or transiting agency
5 information systems consistent with standards
6 and guidelines promulgated under section
7 11331 of title 40, United States Code;

8 (D) implement a single sign-on trusted
9 identity platform for individuals accessing each
10 public website of the agency that requires user
11 authentication, as developed by the Adminis-
12 trator of General Services in collaboration with
13 the Secretary; and

14 (E) implement multi-factor authentication
15 consistent with standards and guidelines pro-
16 mulgated under section 11331 of title 40,
17 United States Code, for—

18 (i) remote access to an agency infor-
19 mation system; and

20 (ii) each user account with elevated
21 privileges on an agency information sys-
22 tem.

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

2 (a) DEFINITIONS.—In this section—

3 (1) the term “intrusion assessments” means ac-
4 tions taken under the intrusion assessment plan to
5 identify and remove intruders in agency information
6 systems;

7 (2) the term “intrusion assessment plan”
8 means the plan required under section 228(b)(1) of
9 the Homeland Security Act of 2002, as added by
10 section 3(a) of this Act; and

11 (3) the term “intrusion detection and preven-
12 tion capabilities” means the capabilities required
13 under section 230(b) of the Homeland Security Act
14 of 2002, as added by section 3(a) of this Act.

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

22 (c) REPORTS TO CONGRESS.—

23 (1) INTRUSION DETECTION AND PREVENTION
24 CAPABILITIES.—

25 (A) SECRETARY OF HOMELAND SECURITY
26 REPORT.—Not later than 6 months after the

1 date of enactment of this Act, and annually
2 thereafter, the Secretary shall submit to the ap-
3 propriate congressional committees a report on
4 the status of implementation of the intrusion
5 detection and prevention capabilities, includ-
6 ing—

7 (i) a description of privacy controls;

8 (ii) a description of the technologies
9 and capabilities utilized to detect cyberse-
10 curity risks in network traffic, including
11 the extent to which those technologies and
12 capabilities include existing commercial
13 and non-commercial technologies;

14 (iii) a description of the technologies
15 and capabilities utilized to prevent network
16 traffic associated with cybersecurity risks
17 from transiting or traveling to or from
18 agency information systems, including the
19 extent to which those technologies and ca-
20 pabilities include existing commercial and
21 non-commercial technologies;

22 (iv) a list of the types of indicators or
23 other identifiers or techniques used to de-
24 tect cybersecurity risks in network traffic
25 transiting or traveling to or from agency

1 information systems on each iteration of
2 the intrusion detection and prevention ca-
3 pabilities and the number of each such
4 type of indicator, identifier, and technique;

5 (v) the number of instances in which
6 the intrusion detection and prevention ca-
7 pabilities detected a cybersecurity risk in
8 network traffic transiting or traveling to or
9 from agency information systems and the
10 number of times the intrusion detection
11 and prevention capabilities blocked net-
12 work traffic associated with cybersecurity
13 risk; and

14 *(vi) an explanation of whether any in-*
15 *formation on individuals, and to the great-*
16 *est extent practicable, on United States per-*
17 *sons, whose personally identifiable informa-*
18 *tion is not necessary to describe a cybersecu-*
19 *rity risk has been retained incidentally*
20 *under the intrusion detection and preven-*
21 *tion capabilities, and if such information*
22 *has been retained, for what purpose and for*
23 *what length of time; and*

24 ~~(vii)~~ a description of the pilot estab-
25 lished under section 230(e)(5) of the

1 Homeland Security Act of 2002, as added
2 by section 3(a) of this Act, including the
3 number of new technologies tested and the
4 number of participating agencies.

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

13 (i) a list of each agency and the de-
14 gree to which each agency has applied the
15 intrusion detection and prevention capabili-
16 ties to an agency information system; and

17 (ii) a list by agency of—

18 (I) the number of instances in
19 which the intrusion detection and pre-
20 vention capabilities detected a cyber-
21 security risk in network traffic
22 transiting or traveling to or from an
23 agency information system and the
24 types of indicators, identifiers, and

1 techniques used to detect such cyber-
2 security risks; and

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

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

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

22 (B) not later than 1 year after the date of
23 enactment of this Act, and annually thereafter,
24 submit to Congress, as part of the report re-

1 required under section 3553(c) of title 44, United
2 States Code—

3 (i) a description of the implementation
4 of the intrusion assessment plan;

5 (ii) the findings of the intrusion as-
6 sessments conducted pursuant to the intru-
7 sion assessment plan;

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

12 (iv) the results of the assessment of
13 the Secretary of best practices for Federal
14 cybersecurity pursuant to section 5(a); and

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

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

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

22 (ii) the improved metrics developed
23 pursuant to section 4(b).

1 **SEC. 7. TERMINATION.**

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

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

15 **SEC. 8. IDENTIFICATION OF UNCLASSIFIED INFORMATION**
 16 **SYSTEMS.**

17 (a) IN GENERAL.—*Except as provided in subsection*
 18 *(c), not later than 180 days after the date of enactment of*
 19 *this Act—*

20 (1) *the Director of National Intelligence, in co-*
 21 *ordination with the heads of other agencies, shall—*

22 (A) *identify all unclassified information*
 23 *systems that provide access to information that,*
 24 *when combined with other unclassified informa-*
 25 *tion, may comprise classified information;*

1 (B) assess the risks that would result from
2 the breach of each unclassified information sys-
3 tem identified in subparagraph (A); and

4 (C) assess the cost and impact on the mis-
5 sion carried out by each agency that owns an
6 unclassified information system identified in
7 subparagraph (A) if the system were to be subse-
8 quently classified; and

9 (2) the Director of National Intelligence shall
10 submit to the appropriate congressional committees a
11 report that includes the findings under paragraph
12 (1).

13 (b) *FORM.*—The report submitted under subsection
14 (a)(2) shall be in unclassified form, but may include a clas-
15 sified annex.

16 (c) *EXCEPTION.*—The requirements under subsection
17 (a)(1) shall not apply to the Department of Defense or an
18 element of the intelligence community.

19 **SEC. 9. OPM DATA BREACH DAMAGE ASSESSMENT.**

20 (a) *ASSESSMENT.*—The Secretary and the Director of
21 National Intelligence shall jointly, and in coordination
22 with the head of each appropriate agency, conduct an ongo-
23 ing damage and risk assessment relating to the data
24 breaches at the Office of Personnel Management (referred
25 to in this section as the “OPM data breach”).

1 **(b) REPORTS.**—

2 **(1) IN GENERAL.**—Not later than 180 days after
3 the date of enactment of this Act, and once not later
4 than 180 days thereafter, the Director of National In-
5 telligence shall submit to Congress a report on the as-
6 sessment conducted under subsection (a).

7 **(2) CONTENTS.**—Each report submitted under
8 this subsection shall include—

9 **(A)** updates on the extent to which Federal
10 data was compromised, exfiltrated, or manipu-
11 lated by the same entity that caused the OPM
12 data breach;

13 **(B)** analysis of the impact of the OPM data
14 breach on national security; and

15 **(C)** analysis of whether any information
16 accessed through the OPM data breach has been
17 released or deployed, whether publicly or pri-
18 vately.

19 **(3) UNCLASSIFIED FORM.**—Each report sub-
20 mitted under this subsection shall be in unclassified
21 form, but may include a classified annex.

22 **SEC. 10. DIRECTION TO AGENCIES.**

23 Section 3553 of title 44, United States Code, is amend-
24 ed by adding at the end the following:

25 “**(h) DIRECTION TO AGENCIES.**—

1 “(1) *AUTHORITY.*—

2 “(A) *IN GENERAL.*—*Notwithstanding sec-*
3 *tion 3554, and subject to subparagraph (B), in*
4 *response to a known or reasonably suspected in-*
5 *formation security threat, vulnerability, or inci-*
6 *dent that represents a substantial threat to the*
7 *information security of an agency, the Secretary*
8 *may issue a directive to the head of an agency*
9 *to take any lawful action with respect to the op-*
10 *eration of the information system, including such*
11 *systems owned or operated by another entity on*
12 *behalf of an agency, that collects, processes,*
13 *stores, transmits, disseminates, or otherwise*
14 *maintains agency information, for the purpose of*
15 *protecting the information system from, or miti-*
16 *gating, an information security threat.*

17 “(B) *EXCEPTION.*—*The authorities of the*
18 *Secretary under this subsection shall not apply*
19 *to a system described in paragraph (2) or (3) of*
20 *subsection (e).*

21 “(2) *PROCEDURES FOR USE OF AUTHORITY.*—

22 *The Secretary shall—*

23 “(A) *in coordination with the Director, es-*
24 *tablish procedures governing the circumstances*

1 *under which a directive may be issued under this*
2 *subsection, which shall include—*

3 *“(i) thresholds and other criteria;*

4 *“(ii) privacy and civil liberties protec-*
5 *tions; and*

6 *“(iii) providing notice to potentially*
7 *affected third parties;*

8 *“(B) specify the reasons for the required ac-*
9 *tion and the duration of the directive;*

10 *“(C) minimize the impact of a directive*
11 *under this subsection by—*

12 *“(i) adopting the least intrusive means*
13 *possible under the circumstances to secure*
14 *the agency information systems; and*

15 *“(ii) limiting directives to the shortest*
16 *period practicable;*

17 *“(D) notify the Director and the head of*
18 *any affected agency immediately upon the*
19 *issuance of a directive under this subsection; and*

20 *“(E) not later than February 1 of each*
21 *year, submit to the appropriate congressional*
22 *committees a report regarding the specific ac-*
23 *tions the Secretary has taken pursuant to para-*
24 *graph (1)(A).*

25 *“(3) IMMINENT THREATS.—*

1 “(A) *IN GENERAL.*—*If the Secretary deter-*
2 *mines that there is an imminent threat to agen-*
3 *cy information systems and a directive under*
4 *this subsection is not reasonably likely to result*
5 *in a timely response to the threat, the Secretary*
6 *may authorize the use of protective capabilities*
7 *under the control of the Secretary for commu-*
8 *nications or other system traffic transiting to or*
9 *from or stored on an agency information system*
10 *without prior consultation with the affected*
11 *agency for the purpose of ensuring the security*
12 *of the information or information system or*
13 *other agency information systems.*

14 “(B) *NOTICE.*—*The Secretary shall imme-*
15 *diately notify the Director, the head and chief*
16 *information officer (or equivalent official) of*
17 *each agency to which specific actions were taken*
18 *pursuant to subparagraph (A), and the appro-*
19 *priate congressional committees and authorizing*
20 *committees of each such agencies of—*

21 “(i) *any action taken under subpara-*
22 *graph (A); and*

23 “(ii) *the reasons for and duration and*
24 *nature of the action.*

1 “(C) *OTHER LAW.*—Any action of the Sec-
2 retary under this paragraph shall be consistent
3 with applicable law.

4 “(D) *LIMITATION ON DELEGATION.*—The
5 authority under this paragraph may not be dele-
6 gated to an official in a position lower than an
7 Under Secretary of the Department of Homeland
8 Security.

9 “(4) *LIMITATION.*—The Secretary may direct or
10 authorize lawful action or protective capability under
11 this subsection only to—

12 “(A) protect agency information from unau-
13 thorized access, use, disclosure, disruption, modi-
14 fication, or destruction; or

15 “(B) require the remediation of or protect
16 against identified information security risks
17 with respect to—

18 “(i) information collected or main-
19 tained by or on behalf of an agency; or

20 “(ii) that portion of an information
21 system used or operated by an agency or by
22 a contractor of an agency or other organiza-
23 tion on behalf of an agency.

24 “(i) *ANNUAL REPORT TO CONGRESS.*—Not later than
25 February 1 of each year, the Director shall submit to the

1 *appropriate congressional committees a report regarding*
2 *the specific actions the Director has taken pursuant to sub-*
3 *section (a)(5), including any actions taken pursuant to sec-*
4 *tion 11303(b)(5) of title 40.*

5 “(j) *APPROPRIATE CONGRESSIONAL COMMITTEES.—In*
6 *this section, the term ‘appropriate congressional commit-*
7 *tees’ means—*

8 “(1) *the Committee on Appropriations and the*
9 *Committee on Homeland Security and Governmental*
10 *Affairs of the Senate; and*

11 “(2) *the Committee on Appropriations and the*
12 *Committee on Homeland Security of the House of*
13 *Representatives.”.*

Calendar No. 673

114TH CONGRESS
2^D SESSION

S. 1869

[Report No. 114-378]

A BILL

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

NOVEMBER 17, 2016

Reported with amendments