

114TH CONGRESS
1ST SESSION

H. R. 3313

To amend the Homeland Security Act of 2002 to strengthen the ability of the Secretary of Homeland Security to detect and prevent intrusions against, and to use countermeasures to protect, agency information systems, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 29, 2015

Mr. McCAUL (for himself and Mr. RATCLIFFE) introduced the following bill; which was referred to the Committee on Oversight and Government Reform, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To amend the Homeland Security Act of 2002 to strengthen the ability of the Secretary of Homeland Security to detect and prevent intrusions against, and to use countermeasures to protect, agency information systems, and for other purposes.

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 “Cyber Defense of Fed-
5 eral Networks Act of 2015”.

1 **SEC. 2. CYBER DEFENSE OF FEDERAL NETWORKS.**

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 by adding at the end the following new sections:

5 **“SEC. 230. CYBERSECURITY PLANS.**

6 “(a) INTRUSION DETECTION AND RESPONSE
7 PLAN.—Not later than one year after the date of the en-
8 actment of this section, the Secretary, in coordination with
9 the Director of the Office of Management and Budget,
10 shall develop and implement an intrusion detection and
11 response plan to detect, identify, and remove intruders in
12 agency information systems. The Secretary, in coordina-
13 tion with the Director, shall update such plan as nec-
14 essary.

15 “(b) EXCEPTION.—The intrusion detection and re-
16 sponse plan required under subsection (a) shall not apply
17 to the Department of Defense or an element of the intel-
18 ligence community.

19 “(c) DEFINITIONS.—In this section and sections 231,
20 232, and 233:

21 “(1) AGENCY.—The term ‘agency’ has the
22 meaning given such term in section 3502 of title 44,
23 United States Code.

24 “(2) CYBERSECURITY RISK.—The term ‘cyber-
25 security risk’ has the meaning given such term in

1 the second section 226 (relating to the national cy-
2 bersecurity and communications integration center).

3 “(3) INFORMATION SYSTEM.—The term ‘infor-
4 mation system’ has the meaning given such term in
5 the second section 226 (relating to the national cy-
6 bersecurity and communications integration center).

7 “(4) INTELLIGENCE COMMUNITY.—The term
8 ‘intelligence community’ has the meaning given such
9 term in section 3(4) of the National Security Act of
10 1947 (50 U.S.C. 3003(4)).

11 **“SEC. 231. ADVANCED INTERNAL DEFENSES.**

12 “(a) ADVANCED NETWORK SECURITY TOOLS.—

13 “(1) IN GENERAL.—The Secretary shall include
14 in the Department’s efforts to continuously diagnose
15 and mitigate cybersecurity risks advanced network
16 security tools to improve visibility of network activ-
17 ity, including through the use of commercial and
18 free or open source tools, to detect and mitigate in-
19 trusions and anomalous activity in agencies’ infor-
20 mation systems.

21 “(2) DEVELOPMENT OF PLAN.—The Secretary,
22 in coordination with the Director of the Office of
23 Management and Budget, shall develop and imple-
24 ment a plan to ensure advanced network security
25 tools, including tools described in paragraph (1), to

1 detect and mitigate intrusions and anomalous activ-
2 ity are available for use by each agency.

3 “(b) PRIORITIZING ADVANCED SECURITY TOOLS.—

4 The Secretary, in coordination with the Director of the
5 Office of Management and Budget, and in consultation
6 with the heads of appropriate agencies, shall—

7 “(1) review and update operational capabilities
8 to ensure appropriate prioritization and use of net-
9 work security monitoring tools within such agency
10 networks; and

11 “(2) brief the Committee on Homeland Security
12 of the House of Representatives and the Committee
13 on Homeland Security and Governmental Affairs of
14 the Senate on such prioritization and use.

15 “(c) IMPROVED METRICS.—The Secretary, in coordi-
16 nation with the Director of the Office of Management and
17 Budget, shall review and update the metrics used to meas-
18 ure security under section 3554 of title 44, United States
19 Code, to include measures of intrusion and incident detec-
20 tion and response times.

21 “(d) TRANSPARENCY AND ACCOUNTABILITY.—The
22 Secretary, in coordination with the Director of the Office
23 of Management and Budget, shall increase transparency
24 to the public on agency cybersecurity postures, including
25 by increasing the number of metrics available on Federal

1 Government performance websites and, to the greatest ex-
2 tent practicable, displaying metrics for agencies.

3 “(e) MAINTENANCE OF TECHNOLOGIES.—Subpara-
4 graph (B) of section 3553(b)(6) of title 44, United States
5 Code, is amended by inserting ‘, operating, and maintain-
6 ing’ after ‘deploying’.

7 **“SEC. 232. FEDERAL CYBERSECURITY BEST PRACTICES.**

8 “The Secretary, in consultation with the Director of
9 the Office of Management and Budget, shall regularly as-
10 sess and require implementation of best practices for—

11 “(1) securing agency information systems
12 against intrusion; and

13 “(2) preventing data exfiltration from such sys-
14 tems in the event of an intrusion.

15 **“SEC. 233. ASSESSMENT; REPORTS.**

16 “(a) DEFINITIONS.—In this section:

17 “(1) APPROPRIATE CONGRESSIONAL COMMIT-
18 TEES.—The term ‘appropriate congressional com-
19 mittees’ means the Committee on Homeland Secu-
20 rity of the House of Representatives and the Com-
21 mittee on Homeland Security and Governmental Af-
22 fairs of the Senate.

23 “(2) INTRUSION ASSESSMENTS.—The term ‘in-
24 trusion assessments’ means actions taken under the
25 intrusion detection and response plan described in

1 section 230 to detect, identify, and remove intruders
2 in agency information systems.

3 “(3) INTRUSION DETECTION AND RESPONSE
4 PLAN.—The term ‘intrusion detection and response
5 plan’ means the intrusion detection and response
6 plan described in section 230.

7 “(b) GAO ASSESSMENT.—Not later than three years
8 after the date of the enactment of this section, the Comp-
9 troller General of the United States shall conduct a study
10 and publish a report on the effectiveness of the approach
11 and strategy of the Department’s capabilities and plans
12 in securing agency information systems, including in the
13 plans and assessments under sections 230, 231, and 232.

14 “(c) REPORT TO CONGRESS.—The Secretary, in co-
15 ordination with the Director of the Office of Management
16 and Budget, shall—

17 “(1) not later than six months after the date of
18 the enactment of this section and 30 days after any
19 update thereto, submit to the appropriate congres-
20 sional committees the intrusion detection and re-
21 sponse plan described in section 230; and

22 “(2) not later than one year after the date of
23 the enactment of this section and annually there-
24 after, submit to Congress—

1 “(A) a description of the implementation
2 of such intrusion detection and response plan;

3 “(B) the findings of the intrusion assess-
4 ments conducted pursuant to such intrusion de-
5 tection and response plan;

6 “(C) a description of the advanced network
7 security tools referred to in section 231;

8 “(D) information relating to the results of
9 the assessment of the Secretary of Federal cy-
10 bersecurity best practices under section 232;
11 and

12 “(E) the improved metrics referred to in
13 section 231.”.

14 (b) DEFINITIONS.—Paragraphs (1) and (2) of the
15 second section 226 of the Homeland Security Act of 2002
16 (6 U.S.C. 148; relating to the national cybersecurity and
17 communications integration center) are amended to read
18 as follows:

19 “(1)(A) except as provided in subparagraph
20 (B), the term ‘cybersecurity risk’ means threats to
21 and vulnerabilities of information or information sys-
22 tems and any related consequences caused by or re-
23 sulting from unauthorized access, use, disclosure,
24 degradation, disruption, modification, or destruction
25 of such information or information systems, includ-

1 ing such related consequences caused by an act of
 2 terrorism; and

3 “(B) such term does not include any action that
 4 solely involves a violation of a consumer term of
 5 service or a consumer licensing agreement;

6 “(2) the term ‘incident’ means an occurrence
 7 that actually or imminently jeopardizes, without law-
 8 ful authority, the integrity, confidentiality, or avail-
 9 ability of information on an information system, or
 10 actually or imminently jeopardizes, without lawful
 11 authority, an information system;”.

12 (c) CLERICAL AMENDMENTS.—The table of contents
 13 for subtitle C of title II of the Homeland Security Act
 14 of 2002 is amended by adding at the end the following
 15 new items:

“Sec. 230. Cybersecurity plans.

“Sec. 231. Advanced internal defenses.

“Sec. 232. Federal cybersecurity best practices.

“Sec. 233. Assessment; reports.”.

16 **SEC. 3. DUTIES OF THE SECRETARY OF HOMELAND SECU-**
 17 **RITY RELATED TO INFORMATION SECURITY.**

18 Section 3553(b)(6) of title 44, United States Code,
 19 is amended by striking subparagraphs (C) and (D) and
 20 inserting the following:

21 “(C) providing incident detection, analysis,
 22 mitigation, and response information, dissemi-
 23 nating related homeland security information,

1 and providing remote or onsite technical assist-
2 ance to the head of an agency;

3 “(D) compiling and analyzing data on
4 agency information security and disseminating
5 related homeland security information;

6 “(E) developing and conducting targeted
7 risk assessments, including assessments of the
8 risk of terrorism, and operational evaluations
9 for agency information and information systems
10 in consultation with the heads of other agencies
11 or governmental and private entities that own
12 and operate such systems, that may include
13 threat, vulnerability, and impact assessments;

14 “(F) in conjunction with other agencies
15 and the private sector, assessing and fostering
16 the development of information security tech-
17 nologies and capabilities for use across multiple
18 agencies; and

19 “(G) coordinating with appropriate agen-
20 cies and officials to ensure, to the maximum ex-
21 tent feasible, that policies and directives issued
22 under paragraph (2) are complementary with—

23 “(i) standards and guidelines devel-
24 oped for national security systems; and

1 “(ii) policies and directives issued by
2 the Secretary of Defense and the Director
3 of National Intelligence under subsection
4 (e)(1); and”.

5 **SEC. 4. DIRECTIVES AND IMMINENT THREATS.**

6 Section 3553 of title 44, United States Code, is
7 amended by adding at the end the following:

8 “(h) DIRECTION TO AGENCIES.—

9 “(1) AUTHORITY.—

10 “(A) IN GENERAL.—Notwithstanding sec-
11 tion 3554, and subject to subparagraph (B), in
12 response to a known or reasonably suspected in-
13 formation security threat, vulnerability, risk, or
14 incident, including an act of terrorism, that rep-
15 resents a substantial threat to the information
16 security of an agency, the Secretary may issue
17 a directive to the head of an agency to take any
18 lawful action with respect to the operation of
19 the information system, including such systems
20 owned or operated by another entity on behalf
21 of an agency, that collects, processes, stores,
22 transmits, disseminates, or otherwise maintains
23 agency information, for the purpose of pro-
24 tecting the information system from, or miti-

gating, an information security threat or an act of terrorism.

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

“(2) PROCEDURES FOR USE OF AUTHORITY.—
The Secretary shall—

“(A) in coordination with the Director and in consultation with Federal contractors, as appropriate, establish procedures under which a directive may be issued under this subsection, which shall include—

“(i) thresholds and other criteria;

“(ii) privacy and civil liberties protections; and

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

“(B) specify the reasons for the required action and the duration of the directive;

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

“(i) adopting the least intrusive means possible under the circumstances to

1 secure the agency information systems;
2 and

3 “(ii) limiting the directive to the
4 shortest period practicable; and

5 “(D) notify the Director and the head of
6 any affected agency immediately upon the
7 issuance of a directive under this subsection.

8 “(3) IMMINENT THREATS.—

9 “(A) IN GENERAL.—If the Secretary deter-
10 mines that there is an imminent threat, includ-
11 ing a threat of terrorism, to agency information
12 systems and a directive under this subsection is
13 not reasonably likely to result in a timely re-
14 sponse to the threat, the Secretary may author-
15 ize the use of protective capabilities under the
16 control of the Secretary for communications or
17 other system traffic transiting to or from or
18 stored on an agency information system without
19 prior consultation with the affected agency for
20 the purpose of ensuring the security of the in-
21 formation, information system, or other agency
22 information systems.

23 “(B) LIMITATION ON DELEGATION.—The
24 authority under this paragraph may not be del-
25 egated to an official in a position lower than an

1 Assistant Secretary of the Department of
2 Homeland Security.

3 “(C) NOTICE.—The Secretary shall imme-
4 diately notify the Director and the head and
5 chief information officer (or equivalent official)
6 of each affected agency of—

7 “(i) any action taken under this sub-
8 section; and

9 “(ii) the reasons for and duration and
10 nature of the action.

11 “(D) OTHER LAW.—Any action of the Sec-
12 retary under this paragraph shall be consistent
13 with applicable law.

14 “(4) LIMITATION.—The Secretary may direct
15 or authorize lawful action or protective capability
16 under this subsection only to—

17 “(A) protect agency information from un-
18 authorized access, use, disclosure, disruption,
19 modification, or destruction; or

20 “(B) require the remediation of or protect
21 against identified information security risks, in-
22 cluding acts of terrorism, with respect to—

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

1 “(ii) that portion of an information
2 system used or operated by an agency or
3 by a contractor of an agency or other orga-
4 nization on behalf of an agency.”.

5 **SEC. 5. REPORT TO CONGRESS REGARDING DHS FUNC-**
6 **TIONS.**

7 Section 3553 of title 44, United States Code, as
8 amended by section 3, is further amended by adding at
9 the end the following new subsection:

10 “(i) ANNUAL REPORT TO CONGRESS.—Not later
11 than February 1 of every year, the Secretary shall report
12 to the Committee on Homeland Security of the House of
13 Representatives and the Committee on Homeland Security
14 and Governmental Affairs of the Senate, regarding the
15 specific actions the Secretary has taken pursuant to sub-
16 sections (b) and (h).”.

○