

.....  
(Original Signature of Member)

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

Mr. MCCAUL introduced the following bill; which was referred to the Committee on \_\_\_\_\_

---

**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  
25 ‘cybersecurity risk’ has the meaning given such term  
26 in the second section 226 (relating to the national

1       cybersecurity and communications integration cen-  
2       ter).

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  
6       cybersecurity and communications integration cen-  
7       ter).

8           “(4) INTELLIGENCE COMMUNITY.—The term  
9       ‘intelligence community’ has the meaning given such  
10      term in section 3(4) of the National Security Act of  
11      1947 (50 U.S.C. 3003(4)).

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

13      “(a) ADVANCED NETWORK SECURITY TOOLS.—

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

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

1 tools, including tools described in paragraph (1), to  
2 detect and mitigate intrusions and anomalous activ-  
3 ity are available for use by each agency.

4 “(b) **PRIORITIZING ADVANCED SECURITY TOOLS.**—  
5 The Secretary, in coordination with the Director of the  
6 Office of Management and Budget, and in consultation  
7 with the heads of appropriate agencies, shall—

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

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

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

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

1 by increasing the number of metrics available on Federal  
2 Government performance websites and, to the greatest ex-  
3 tent practicable, displaying metrics for agencies.

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

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

8 “(1) securing agency information systems  
9 against intrusion; and

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

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

13 “(a) DEFINITIONS.—In this section:

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

20 “(2) INTRUSION ASSESSMENTS.—The term ‘in-  
21 trusion assessments’ means actions taken under the  
22 intrusion detection and response plan described in  
23 section 230 to detect, identify, and remove intruders  
24 in agency information systems.

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

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

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

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

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

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

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

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

6           “(D) information relating to the results of  
7           the assessment of the Secretary of Federal  
8           cybersecurity best practices under section 232;  
9           and

10           “(E) the improved metrics referred to in  
11           section 231.”.

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

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



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

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

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

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

21                  “(i) standards and guidelines devel-  
22                  oped for national security systems; and

23                  “(ii) policies and directives issued by  
24                  the Secretary of Defense and the Director

1 of National Intelligence under subsection  
2 (e)(1); and”.

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

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

6 “(h) DIRECTION TO AGENCIES.—

7 “(1) AUTHORITY.—

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

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

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

7                   “(A) in coordination with the Director and  
8                   in consultation with Federal contractors, as ap-  
9                   propriate, establish procedures under which a  
10                   directive may be issued under this subsection,  
11                   which shall include—

12                           “(i) thresholds and other criteria;

13                           “(ii) privacy and civil liberties protec-  
14                           tions; and

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

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

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

21                           “(i) adopting the least intrusive  
22                           means possible under the circumstances to  
23                           secure the agency information systems;  
24                           and

1                   “(ii) limiting the directive to the  
2                   shortest period practicable; and

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

6                   “(3) IMMINENT THREATS.—

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

21                  “(B) LIMITATION ON DELEGATION.—The  
22                  authority under this paragraph may not be del-  
23                  egated to an official in a position lower than an  
24                  Assistant Secretary of the Department of  
25                  Homeland Security.

1           “(C) NOTICE.—The Secretary shall immediately notify the Director and the head and  
2           chief information officer (or equivalent official)  
3           of each affected agency of—

4                   “(i) any action taken under this subsection; and  
5                   “(ii) the reasons for and duration and  
6                   nature of the action.

7           “(D) OTHER LAW.—Any action of the Secretary under this paragraph shall be consistent  
8           with applicable law.  
9           “(4) LIMITATION.—The Secretary may direct  
10           or authorize lawful action or protective capability  
11           under this subsection only to—

12                   “(A) protect agency information from unauthorized access, use, disclosure, disruption,  
13                   modification, or destruction; or  
14                   “(B) require the remediation of or protect  
15                   against identified information security risks, including acts of terrorism, with respect to—  
16                   “(i) information collected or main-  
17                   tained by or on behalf of an agency; or  
18                   “(ii) that portion of an information  
19                   system used or operated by an agency or  
20                   “(i) information collected or main-  
21                   tained by or on behalf of an agency; or  
22                   “(ii) that portion of an information  
23                   system used or operated by an agency or  
24                   “(i) information collected or main-  
25                   tained by or on behalf of an agency; or  
26                   “(ii) that portion of an information  
27                   system used or operated by an agency or

1                   by a contractor of an agency or other orga-  
2                   nization on behalf of an agency.”.

3 **SEC. 5. MAINTENANCE OF TECHNOLOGIES.**

4           Subparagraph (B) of section 3553(b)(6) of title 44,  
5 United States Code, is amended by inserting “, operating,  
6 and maintaining” after “deploying”.

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

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

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