

113TH CONGRESS
2^D SESSION

S. 2519

AN ACT

To codify an existing operations center for cybersecurity.

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 “National Cybersecurity
3 Protection Act of 2014”.

4 **SEC. 2. DEFINITIONS.**

5 In this Act—

6 (1) the term “Center” means the national cy-
7 bersecurity and communications integration center
8 under section 226 of the Homeland Security Act of
9 2002, as added by section 3;

10 (2) the term “critical infrastructure” has the
11 meaning given that term in section 2 of the Home-
12 land Security Act of 2002 (6 U.S.C. 101);

13 (3) the term “cybersecurity risk” has the mean-
14 ing given that term in section 226 of the Homeland
15 Security Act of 2002, as added by section 3;

16 (4) the term “information sharing and analysis
17 organization” has the meaning given that term in
18 section 212(5) of the Homeland Security Act of
19 2002 (6 U.S.C. 131(5));

20 (5) the term “information system” has the
21 meaning given that term in section 3502(8) of title
22 44, United States Code; and

23 (6) the term “Secretary” means the Secretary
24 of Homeland Security.

1 **SEC. 3. NATIONAL CYBERSECURITY AND COMMUNICA-**
2 **TIONS INTEGRATION CENTER.**

3 (a) IN GENERAL.—Subtitle C of title II of the Home-
4 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-
5 ed by adding at the end the following:

6 **“SEC. 226. NATIONAL CYBERSECURITY AND COMMUNICA-**
7 **TIONS INTEGRATION CENTER.**

8 “(a) DEFINITIONS.—In this section—

9 “(1) the term ‘cybersecurity risk’ means threats
10 to and vulnerabilities of information or information
11 systems and any related consequences caused by or
12 resulting from unauthorized access, use, disclosure,
13 degradation, disruption, modification, or destruction
14 of information or information systems, including
15 such related consequences caused by an act of ter-
16 rorism;

17 “(2) the term ‘incident’ means an occurrence
18 that—

19 “(A) actually or imminently jeopardizes,
20 without lawful authority, the integrity, con-
21 fidentiality, or availability of information on an
22 information system; or

23 “(B) constitutes a violation or imminent
24 threat of violation of law, security policies, secu-
25 rity procedures, or acceptable use policies;

1 “(3) the term ‘information sharing and analysis
2 organization’ has the meaning given that term in
3 section 212(5); and

4 “(4) the term ‘information system’ has the
5 meaning given that term in section 3502(8) of title
6 44, United States Code.

7 “(b) CENTER.—There is in the Department a na-
8 tional cybersecurity and communications integration cen-
9 ter (referred to in this section as the ‘Center’) to carry
10 out certain responsibilities of the Under Secretary ap-
11 pointed under section 103(a)(1)(H).

12 “(c) FUNCTIONS.—The cybersecurity functions of the
13 Center shall include—

14 “(1) being a Federal civilian interface for the
15 multi-directional and cross-sector sharing of infor-
16 mation related to cybersecurity risks, incidents, anal-
17 ysis, and warnings for Federal and non-Federal enti-
18 ties;

19 “(2) providing shared situational awareness to
20 enable real-time, integrated, and operational actions
21 across the Federal Government and non-Federal en-
22 tities to address cybersecurity risks and incidents to
23 Federal and non-Federal entities;

1 “(3) coordinating the sharing of information re-
2 lated to cybersecurity risks and incidents across the
3 Federal Government;

4 “(4) facilitating cross-sector coordination to ad-
5 dress cybersecurity risks and incidents, including cy-
6 bersecurity risks and incidents that may be related
7 or could have consequential impacts across multiple
8 sectors;

9 “(5)(A) conducting integration and analysis, in-
10 cluding cross-sector integration and analysis, of cy-
11 bersecurity risks and incidents; and

12 “(B) sharing the analysis conducted under sub-
13 paragraph (A) with Federal and non-Federal enti-
14 ties;

15 “(6) upon request, providing timely technical
16 assistance, risk management support, and incident
17 response capabilities to Federal and non-Federal en-
18 tities with respect to cybersecurity risks and inci-
19 dents, which may include attribution, mitigation,
20 and remediation; and

21 “(7) providing information and recommenda-
22 tions on security and resilience measures to Federal
23 and non-Federal entities, including information and
24 recommendations to—

25 “(A) facilitate information security; and

1 “(B) strengthen information systems
2 against cybersecurity risks and incidents.

3 “(d) COMPOSITION.—

4 “(1) IN GENERAL.—The Center shall be com-
5 posed of—

6 “(A) appropriate representatives of Fed-
7 eral entities, such as—

8 “(i) sector-specific agencies;

9 “(ii) civilian and law enforcement
10 agencies; and

11 “(iii) elements of the intelligence com-
12 munity, as that term is defined under sec-
13 tion 3(4) of the National Security Act of
14 1947 (50 U.S.C. 3003(4));

15 “(B) appropriate representatives of non-
16 Federal entities, such as—

17 “(i) State and local governments;

18 “(ii) information sharing and analysis
19 organizations; and

20 “(iii) owners and operators of critical
21 information systems;

22 “(C) components within the Center that
23 carry out cybersecurity and communications ac-
24 tivities;

1 “(D) a designated Federal official for oper-
2 ational coordination with and across each sec-
3 tor; and

4 “(E) other appropriate representatives or
5 entities, as determined by the Secretary.

6 “(2) INCIDENTS.—In the event of an incident,
7 during exigent circumstances the Secretary may
8 grant a Federal or non-Federal entity immediate
9 temporary access to the Center.

10 “(e) PRINCIPLES.—In carrying out the functions
11 under subsection (c), the Center shall ensure—

12 “(1) to the extent practicable, that—

13 “(A) timely, actionable, and relevant infor-
14 mation related to cybersecurity risks, incidents,
15 and analysis is shared;

16 “(B) when appropriate, information related
17 to cybersecurity risks, incidents, and analysis is
18 integrated with other relevant information and
19 tailored to the specific characteristics of a sec-
20 tor;

21 “(C) activities are prioritized and con-
22 ducted based on the level of risk;

23 “(D) industry sector-specific, academic,
24 and national laboratory expertise is sought and
25 receives appropriate consideration;

1 “(E) continuous, collaborative, and inclu-
2 sive coordination occurs—

3 “(i) across sectors; and

4 “(ii) with—

5 “(I) sector coordinating councils;

6 “(II) information sharing and
7 analysis organizations; and

8 “(III) other appropriate non-Fed-
9 eral partners;

10 “(F) as appropriate, the Center works to
11 develop and use mechanisms for sharing infor-
12 mation related to cybersecurity risks and inci-
13 dents that are technology-neutral, interoperable,
14 real-time, cost-effective, and resilient; and

15 “(G) the Center works with other agencies
16 to reduce unnecessarily duplicative sharing of
17 information related to cybersecurity risks and
18 incidents;

19 “(2) that information related to cybersecurity
20 risks and incidents is appropriately safeguarded
21 against unauthorized access; and

22 “(3) that activities conducted by the Center
23 comply with all policies, regulations, and laws that
24 protect the privacy and civil liberties of United
25 States persons.

1 “(f) NO RIGHT OR BENEFIT.—

2 “(1) IN GENERAL.—The provision of assistance
3 or information to, and inclusion in the Center of,
4 governmental or private entities under this section
5 shall be at the sole and unreviewable discretion of
6 the Under Secretary appointed under section
7 103(a)(1)(H).

8 “(2) CERTAIN ASSISTANCE OR INFORMATION.—
9 The provision of certain assistance or information
10 to, or inclusion in the Center of, one governmental
11 or private entity pursuant to this section shall not
12 create a right or benefit, substantive or procedural,
13 to similar assistance or information for any other
14 governmental or private entity.”.

15 (b) TECHNICAL AND CONFORMING AMENDMENT.—
16 The table of contents in section 1(b) of the Homeland Se-
17 curity Act of 2002 (6 U.S.C. 101 note) is amended by
18 inserting after the item relating to section 225 the fol-
19 lowing:

“Sec. 226. National cybersecurity and communications integration center.”.

20 **SEC. 4. RECOMMENDATIONS REGARDING NEW AGREE-**
21 **MENTS.**

22 (a) IN GENERAL.—Not later than 180 days after the
23 date of enactment of this Act, the Secretary shall submit
24 recommendations on how to expedite the implementation
25 of information-sharing agreements for cybersecurity pur-

1 poses between the Center and non-Federal entities (re-
2 ferred to in this section as “cybersecurity information-
3 sharing agreements”) to—

4 (1) the Committee on Homeland Security and
5 Governmental Affairs and the Committee on the Ju-
6 diciary of the Senate; and

7 (2) the Committee on Homeland Security and
8 the Committee on the Judiciary of the House of
9 Representatives.

10 (b) CONTENTS.—In submitting recommendations
11 under subsection (a), the Secretary shall—

12 (1) address the development and utilization of
13 a scalable form that retains all privacy and other
14 protections in cybersecurity information-sharing
15 agreements that are in effect as of the date on which
16 the Secretary submits the recommendations, includ-
17 ing Cooperative Research and Development Agree-
18 ments; and

19 (2) include in the recommendations any addi-
20 tional authorities or resources that may be needed to
21 carry out the implementation of any new cybersecu-
22 rity information-sharing agreements.

23 **SEC. 5. ANNUAL REPORT.**

24 Not later than 1 year after the date of enactment
25 of this Act, and every year thereafter for 3 years, the Sec-

1 retary shall submit to the Committee on Homeland Secu-
2 rity and Governmental Affairs and the Committee on the
3 Judiciary of the Senate, the Committee on Homeland Se-
4 curity and the Committee on the Judiciary of the House
5 of Representatives, and the Comptroller General of the
6 United States a report on the Center, which shall in-
7 clude—

8 (a) information on the Center, including—

9 (1) an assessment of the capability and capacity
10 of the Center to carry out its cybersecurity mission
11 under this Act;

12 (2) the number of representatives from non-
13 Federal entities that are participating in the Center,
14 including the number of representatives from States,
15 nonprofit organizations, and private sector entities,
16 respectively;

17 (3) the number of requests from non-Federal
18 entities to participate in the Center and the response
19 to such requests;

20 (4) the average length of time taken to resolve
21 requests described in paragraph (3);

22 (5) the identification of—

23 (A) any delay in resolving requests de-
24 scribed in paragraph (3) involving security
25 clearance processing; and

1 (B) the agency involved with a delay de-
2 scribed in subparagraph (A);

3 (6) a description of any other obstacles or chal-
4 lenges to resolving requests described in paragraph
5 (3) and a summary of the reasons for denials of any
6 such requests;

7 (7) the extent to which the Department is en-
8 gaged in information sharing with each critical in-
9 frastructure sector, including—

10 (A) the extent to which each sector has
11 representatives at the Center;

12 (B) the extent to which owners and opera-
13 tors of critical infrastructure in each critical in-
14 frastructure sector participate in information
15 sharing at the Center; and

16 (C) the volume and range of activities with
17 respect to which the Secretary has collaborated
18 with the sector coordinating councils and the
19 sector-specific agencies to promote greater en-
20 gagement with the Center; and

21 (8) the policies and procedures established by
22 the Center to safeguard privacy and civil liberties.

23 **SEC. 6. GAO REPORT.**

24 Not later than 2 years after the date of enactment
25 of this Act, the Comptroller General of the United States

1 shall submit to the Committee on Homeland Security and
2 Governmental Affairs of the Senate and the Committee
3 on Homeland Security of the House of Representatives a
4 report on the effectiveness of the Center in carrying out
5 its cybersecurity mission.

6 **SEC. 7. CYBER INCIDENT RESPONSE PLAN; CLEARANCES;**
7 **BREACHES.**

8 (a) CYBER INCIDENT RESPONSE PLAN; CLEAR-
9 ANCES.—Subtitle C of title II of the Homeland Security
10 Act of 2002 (6 U.S.C. 141 et seq.), as amended by section
11 3, is amended by adding at the end the following:

12 **“SEC. 227. CYBER INCIDENT RESPONSE PLAN.**

13 “The Under Secretary appointed under section
14 103(a)(1)(H) shall, in coordination with appropriate Fed-
15 eral departments and agencies, State and local govern-
16 ments, sector coordinating councils, information sharing
17 and analysis organizations (as defined in section 212(5)),
18 owners and operators of critical infrastructure, and other
19 appropriate entities and individuals, develop, regularly up-
20 date, maintain, and exercise adaptable cyber incident re-
21 sponse plans to address cybersecurity risks (as defined in
22 section 226) to critical infrastructure.

23 **“SEC. 228. CLEARANCES.**

24 “The Secretary shall make available the process of
25 application for security clearances under Executive Order

1 13549 (75 Fed. Reg. 162; relating to a classified national
2 security information program) or any successor Executive
3 Order to appropriate representatives of sector coordi-
4 nating councils, sector information sharing and analysis
5 organizations (as defined in section 212(5)), owners and
6 operators of critical infrastructure, and any other person
7 that the Secretary determines appropriate.”.

8 (b) BREACHES.—

9 (1) REQUIREMENTS.—The Director of the Of-
10 fice of Management and Budget shall ensure that
11 data breach notification policies and guidelines are
12 updated periodically and require—

13 (A) except as provided in paragraph (4),
14 notice by the affected agency to each committee
15 of Congress described in section 3544(c)(1) of
16 title 44, United States Code, the Committee on
17 the Judiciary of the Senate, and the Committee
18 on Homeland Security and the Committee on
19 the Judiciary of the House of Representatives,
20 which shall—

21 (i) be provided expeditiously and not
22 later than 30 days after the date on which
23 the agency discovered the unauthorized ac-
24 quisition or access; and

25 (ii) include—

1 (I) information about the breach,
2 including a summary of any informa-
3 tion that the agency knows on the
4 date on which notification is provided
5 about how the breach occurred;

6 (II) an estimate of the number of
7 individuals affected by the breach,
8 based on information that the agency
9 knows on the date on which notifica-
10 tion is provided, including an assess-
11 ment of the risk of harm to affected
12 individuals;

13 (III) a description of any cir-
14 cumstances necessitating a delay in
15 providing notice to affected individ-
16 uals; and

17 (IV) an estimate of whether and
18 when the agency will provide notice to
19 affected individuals; and

20 (B) notice by the affected agency to af-
21 fected individuals, pursuant to data breach noti-
22 fication policies and guidelines, which shall be
23 provided as expeditiously as practicable and
24 without unreasonable delay after the agency

1 discovers the unauthorized acquisition or ac-
2 cess.

3 (2) NATIONAL SECURITY; LAW ENFORCEMENT;
4 REMEDICATION.—The Attorney General, the head of
5 an element of the intelligence community (as such
6 term is defined under section 3(4) of the National
7 Security Act of 1947 (50 U.S.C. 3003(4)), or the
8 Secretary may delay the notice to affected individ-
9 uals under paragraph (1)(B) if the notice would dis-
10 rupt a law enforcement investigation, endanger na-
11 tional security, or hamper security remediation ac-
12 tions.

13 (3) OMB REPORT.—During the first 2 years
14 beginning after the date of enactment of this Act,
15 the Director of the Office of Management and Budget
16 shall, on an annual basis—

17 (A) assess agency implementation of data
18 breach notification policies and guidelines in ag-
19 gregate; and

20 (B) include the assessment described in
21 clause (i) in the report required under section
22 3543(a)(8) of title 44, United States Code.

23 (4) EXCEPTION.—Any element of the intel-
24 ligence community (as such term is defined under
25 section 3(4) of the National Security Act of 1947

1 (50 U.S.C. 3003(4)) that is required to provide no-
2 tice under paragraph (1)(A) shall only provide such
3 notice to appropriate committees of Congress.

4 (c) **RULE OF CONSTRUCTION.**—Nothing in the
5 amendment made by subsection (a) or in subsection (b)(1)
6 shall be construed to alter any authority of a Federal
7 agency or department.

8 (d) **TECHNICAL AND CONFORMING AMENDMENT.**—
9 The table of contents in section 1(b) of the Homeland Se-
10 curity Act of 2002 (6 U.S.C. 101 note), as amended by
11 section 3, is amended by inserting after the item relating
12 to section 226 the following:

“Sec. 227. Cyber incident response plan.
“Sec. 228. Clearances.”.

13 **SEC. 8. RULES OF CONSTRUCTION.**

14 (a) **PROHIBITION ON NEW REGULATORY AUTHOR-**
15 **ITY.**—Nothing in this Act or the amendments made by
16 this Act shall be construed to grant the Secretary any au-
17 thority to promulgate regulations or set standards relating
18 to the cybersecurity of private sector critical infrastructure
19 that was not in effect on the day before the date of enact-
20 ment of this Act.

21 (b) **PRIVATE ENTITIES.**—Nothing in this Act or the
22 amendments made by this Act shall be construed to re-
23 quire any private entity—

24 (1) to request assistance from the Secretary; or

1 (2) that requested such assistance from the
2 Secretary to implement any measure or rec-
3 ommendation suggested by the Secretary.

Passed the Senate December 10, 2014.

Attest:

Secretary.

113TH CONGRESS
2^D SESSION

S. 2519

AN ACT

To codify an existing operations center for
cybersecurity.