

116TH CONGRESS
1ST SESSION

H. R. 5394

To amend the Homeland Security Act of 2002 to require certain coordination between the Department of Homeland Security and Federal and non-Federal entities relating to cybersecurity risks and incidents, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 11, 2019

Mr. TAYLOR (for himself, Mr. ROGERS of Alabama, Mr. HURD of Texas, Mr. PANETTA, Mr. GREEN of Texas, Mr. GUEST, and Ms. SLOTKIN) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Oversight and Reform, 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 require certain coordination between the Department of Homeland Security and Federal and non-Federal entities relating to cybersecurity risks and incidents, 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 “Strengthening State
5 and Local Cybersecurity Defenses Act”.

1 **SEC. 2. COOPERATION RELATING TO CYBERSECURITY**
2 **RISKS AND INCIDENTS.**

3 Subtitle A of title XXII of the Homeland Security
4 Act of 2002 (6 U.S.C. 652 et seq.) is amended—

5 (1) in section 2201 (6 U.S.C. 651)—

6 (A) by redesignating paragraphs (4), (5),
7 and (6) as paragraphs (5), (6), and (7), respec-
8 tively; and

9 (B) by inserting after paragraph (3) the
10 following new paragraph:

11 “(4) ENTITY.—The term ‘entity’ includes—

12 “(A) an association, corporation, whether
13 for-profit or nonprofit, partnership, proprietor-
14 ship, organization, institution, establishment, or
15 individual, whether domestic or foreign;

16 “(B) a government agency or other govern-
17 mental entity, whether domestic or foreign, in-
18 cluding State, local, Tribal, and territorial gov-
19 ernment entities; and

20 “(C) the general public.”;

21 (2) in section 2209 of the Homeland Security
22 Act of 2002 (6 U.S.C. 659), by adding at the end
23 the following new subsection:

24 “(n) COORDINATION.—The Director shall, to the ex-
25 tent practicable, and in coordination as appropriate with

1 Federal and non-Federal entities, such as the Multi-State
2 Information Sharing and Analysis Center—

3 “(1) conduct exercises with Federal and non-
4 Federal entities;

5 “(2) provide operational and technical cyberse-
6 curity training related to cyber threat indicators, de-
7 fensive measures, cybersecurity risks, and incidents
8 to Federal and non-Federal entities to address cy-
9 bersecurity risks or incidents, with or without reim-
10 bursement;

11 “(3) assist Federal and non-Federal entities,
12 upon request, in sharing cyber threat indicators, de-
13 fensive measures, cybersecurity risks, and incidents
14 from and to the Federal Government as well as
15 among Federal and non-Federal entities, in order to
16 increase situational awareness and help prevent inci-
17 dents;

18 “(4) provide Federal and non-Federal entities
19 timely notifications containing specific incident and
20 malware information that may affect such entities or
21 individuals with respect to whom such entities have
22 a relationship;

23 “(5) provide and periodically update via a web
24 portal and other means tools, products, resources,
25 policies, guidelines, controls, procedures, and other

1 cybersecurity standards and best practices and pro-
2 cedures related to information security;

3 “(6) work with senior Federal and non-Federal
4 officials, including State and local Chief Information
5 Officers, senior election officials, and through na-
6 tional associations, to coordinate a nationwide effort
7 to ensure effective implementation of tools, products,
8 resources, policies, guidelines, controls, procedures,
9 and other cybersecurity standards and best practices
10 and procedures related to information security to se-
11 cure and ensure the resiliency of Federal and non-
12 Federal information systems, including election sys-
13 tems;

14 “(7) provide, upon request, operational and
15 technical assistance to Federal and non-Federal enti-
16 ties to implement tools, products, resources, policies,
17 guidelines, controls, procedures, and other cyberse-
18 curity standards and best practices and procedures
19 related to information security, including by, as ap-
20 propriate, deploying and sustaining cybersecurity
21 technologies, such as an intrusion detection capa-
22 bility, to assist such Federal and non-Federal enti-
23 ties in detecting cybersecurity risks and incidents;

24 “(8) assist Federal and non-Federal entities in
25 developing policies and procedures for coordinating

1 vulnerability disclosures, to the extent practicable,
2 consistent with international and national standards
3 in the information technology industry;

4 “(9) ensure that Federal and non-Federal enti-
5 ties, as appropriate, are made aware of the tools,
6 products, resources, policies, guidelines, controls,
7 procedures, and other cybersecurity standards and
8 best practices and procedures related to information
9 security developed by the Department and other ap-
10 propriate Federal entities for ensuring the security
11 and resiliency of civilian information systems; and

12 “(10) promote cybersecurity education and
13 awareness through engagements with Federal and
14 non-Federal entities.”.

○