I

114TH CONGRESS
1ST SESSION

H. R. 3305

To help enhance American network security and mitigate cybersecurity risks, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 29, 2015

Mr. HURD of Texas (for himself, Mr. MCCAUL, 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 help enhance American network security and mitigate cybersecurity risks, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "EINSTEIN Act of 2015".

SEC. 2. PROTECTION OF FEDERAL CIVILIAN INFORMATION SYSTEMS.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

"SEC. 230. AVAILABLE PROTECTION OF FEDERAL CIVILIAN INFORMATION SYSTEMS.

''(a) IN GENERAL.—The Secretary shall deploy, operate, and maintain, to make available for use by any Federal agency, with or without reimbursement, capabilities to protect Federal agency information and Federal civilian information systems, including technologies to diagnose, detect, prevent, and mitigate against cybersecurity risks involving Federal agency information or Federal civilian information systems.

''(b) ACTIVITIES.—In carrying out this section, the Secretary may—

''(1) access, and Federal agency heads may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information traveling to or from or stored on a Federal civilian information system, regardless of from where the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or pre-

vent Federal agency heads from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

''(2) enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (a); and

''(3) retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect Federal agency information and Federal civilian information systems from cybersecurity risks or in furtherance of the national cybersecurity and communications integration center's authority under the second section 226, or, with the approval of the Attorney General and if disclosure of such information is not otherwise prohibited by law, to law enforcement only to investigate, prosecute, disrupt, or otherwise respond to—

''(A) a violation of section 1030 of title 18, United States Code;

''(B) an imminent threat of death or serious bodily harm;

"(C) a serious threat to a minor, including sexual exploitation or threats to physical safety; or

"(D) an attempt, or conspiracy, to commit an offense described in any of subparagraphs (A) through (C).

"(c) CONDITIONS.—Contracts or other agreements under subsection (b)(2) shall include appropriate provisions barring—

"(1) the disclosure of information to any entity other than the Department or a Federal agency disclosing information in accordance with subsection (b)(1) that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk; and

"(2) the use of any information to which such private entity gains access in accordance with this section for any purpose other than to protect Federal agency information and Federal civilian information systems against cybersecurity risks or to administer any such contract or other agreement.

"(d) LIMITATION.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and a contract or agreement under subsection (b)(2).

''(e) DEFINITION.—The term 'cybersecurity risk' has the meaning given such term in the second section 226 (relating to the national cybersecurity and communications integration center).''.

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

''(1)(A) except as provided in subparagraph (B), the term 'cybersecurity risk' means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

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

''(2) the term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or

actually or imminently jeopardizes, without lawful authority, an information system;''.

(c) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by adding at the end the following new item:

''Sec. 230. Available protection of Federal civilian information systems.''.

○