I

115TH CONGRESS
1ST SESSION

H. R. 3403

To provide for an interagency cyber victim coordinator to respond to data breaches and other cyber attacks on Federal employees.

IN THE HOUSE OF REPRESENTATIVES

JULY 26, 2017

Mr. BROWN of Maryland (for himself, Mr. RUPPERSBERGER, and Mr. WITTMAN) introduced the following bill; which was referred to the Committee on Oversight and Government Reform

---

A BILL

To provide for an interagency cyber victim coordinator to respond to data breaches and other cyber attacks on Federal employees.

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 ''Cyber Valuing Individual Cybersecurity Through Interagency Measures Act'' or the ''Cyber VICTIM Act''.

SEC. 2. INTERAGENCY CYBER VICTIM RESPONSE.

(a) INTERAGENCY CYBER VICTIM COORDINATOR.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the President shall designate a Federal official to coordinate efforts to respond to data breaches and other cyber attacks on Federal employees. Such official shall have the title of interagency cyber victim response coordinator.

(2) DUTIES.—The coordinator designated under paragraph (1) shall have the following duties:

(A) Coordinate activities of the Federal Government relating to incidents of data breaches in which the data of Federal employees, including Social Security numbers, personal financial information, addresses, and other private identifying information, has been compromised, to—

(i) ensure victims receive appropriate response and assistance from the Federal Government; and

(ii) ensure synchronization of intelligence and responses among Federal law enforcement agencies to incidents of cyber attacks against Federal employees.

(B) Chair an interagency working group consisting of appropriate personnel of the Fed-

eral Government with purview over response to cyber attacks against Federal employees.

(C) Ensure sufficient representation of each Federal agency and department at any interagency working group established under subparagraph (B).

(D) Develop processes and procedures to keep victims informed of efforts to—

(i) mitigate damage from data breaches; and

(ii) prosecute perpetrators.

(b) ANNUAL REPORT.—

(1) IN GENERAL.—On an annual basis, the Coordinator shall submit to the appropriate congressional committees a report that includes a summary of each data breach described in subsection (a)(1) that occurred during the year for which the report is submitted.

(2) FORM OF REPORT.—Each report under paragraph (1) may be submitted in classified or unclassified form.

(c) COMPREHENSIVE PLAN TO ADDRESS CYBER ATTACKS.—Not later than 180 days after the date of the enactment of this Act, the President shall develop a com-

prehensive plan for the United States response to data breaches of personal information of Federal employees.

(d) DEFINITIONS.—In this section, the following definitions apply:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, and the Committee on Homeland Security of the House of Representatives; and

(B) the Committee on Armed Services, the Committee on the Judiciary, the Select Committee on Intelligence, and the Committee on Homeland Security and Governmental Affairs of the Senate.

(2) DATA BREACH.—The term ''data breach'' means an unauthorized intrusion of a Federal database resulting in a breach of personal information of a Federal employee, including—

(A) the 2015 breaches of the Office of Personnel Management databases relating to background security checks and Federal employee background information; and

(B) the November 2014 breach of the United States Postal Service employee database system.

○