SEC. 11. 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 a interagency working group consisting of appropriate personnel of the Federal 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 un-
classified form.

(c) COMPREHENSIVE PLAN TO ADDRESS CYBER AT-
TACKS.—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 defi-
nitions apply:

(1) APPROPRIATE CONGRESSIONAL COMMIT-
TEES.—The term “appropriate congressional com-
mittes” means—

(A) the Committee on Armed Services, the
Committee on the Judiciary, the Permanent Se-
lect Committee on Intelligence, and the Com-
mittee on Homeland Security of the House of
Representatives; and

(B) the Committee on Armed Services, the
Committee on the Judiciary, the Select Com-
mittee on Intelligence, and the Committee on
Homeland Security and Government 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.