I

115TH CONGRESS
1ST SESSION

H. R. 666

To amend the Homeland Security Act of 2002 to establish the Insider Threat Program, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 24, 2017

Mr. KING of New York (for himself, Mr. BARLETTA, Mr. MCCAUL, and Mr. DONOVAN) introduced the following bill; which was referred to the Committee on Homeland Security

---

A BILL

To amend the Homeland Security Act of 2002 to establish the Insider Threat Program, 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 ''Department of Homeland Security Insider Threat and Mitigation Act of 2017''.

SEC. 2. ESTABLISHMENT OF INSIDER THREAT PROGRAM.

(a) IN GENERAL.—Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding at the end the following new section:

"SEC. 104. INSIDER THREAT PROGRAM.

''(a) ESTABLISHMENT.—The Secretary shall establish an Insider Threat Program within the Department. Such Program shall—

''(1) provide training and education for Department personnel to identify, prevent, mitigate, and respond to insider threat risks to the Department's critical assets;

''(2) provide investigative support regarding potential insider threats that may pose a risk to the Department's critical assets; and

''(3) conduct risk mitigation activities for insider threats.

''(b) STEERING COMMITTEE.—

''(1) IN GENERAL.—The Secretary shall establish a Steering Committee within the Department. The Under Secretary for Intelligence and Analysis shall serve as the Chair of the Steering Committee. The Chief Security Officer shall serve as the Vice Chair. The Steering Committee shall be comprised of representatives of the Office of Intelligence and Analysis, the Office of the Chief Information Officer, the Office of the General Counsel, the Office for Civil Rights and Civil Liberties, the Privacy Office, the Office of the Chief Human Capital Officer, the Office of the Chief Financial Officer, the Federal

Protective Service, the Office of the Chief Procurement Officer, the Science and Technology Directorate, and other components or offices of the Department as appropriate. Such representatives shall meet on a regular basis to discuss cases and issues related to insider threats to the Department's critical assets, in accordance with subsection (a).

''(2) RESPONSIBILITIES.—Not later than one year after the date of the enactment of this section, the Under Secretary for Intelligence and Analysis and the Chief Security Officer, in coordination with the Steering Committee established pursuant to paragraph (1), shall—

''(A) develop a holistic strategy for Department-wide efforts to identify, prevent, mitigate, and respond to insider threats to the Department's critical assets;

''(B) develop a plan to implement the insider threat measures identified in the strategy developed under subparagraph (A) across the components and offices of the Department;

''(C) document insider threat policies and controls;

''(D) conduct a baseline risk assessment of insider threats posed to the Department's critical assets;

''(E) examine existing programmatic and technology best practices adopted by the Federal Government, industry, and research institutions to implement solutions that are validated and cost-effective;

''(F) develop a timeline for deploying workplace monitoring technologies, employee awareness campaigns, and education and training programs related to identifying, preventing, mitigating, and responding to potential insider threats to the Department's critical assets;

''(G) require the Chair and Vice Chair of the Steering Committee to consult with the Under Secretary for Science and Technology and other appropriate stakeholders to ensure the Insider Threat Program is informed, on an ongoing basis, by current information regarding threats, beset practices, and available technology; and

''(H) develop, collect, and report metrics on the effectiveness of the Department's insider threat mitigation efforts.

''(c) DEFINITIONS.—In this section:

''(1) CRITICAL ASSETS.—The term 'critical assets' means the people, facilities, information, and technology required for the Department to fulfill its mission.

''(2) INSIDER.—The term 'insider' means—

''(A) any person who has access to classified national security information and is employed by, detailed to, or assigned to the Department, including members of the Armed Forces, experts or consultants to the Department, industrial or commercial contractors, licensees, certificate holders, or grantees of the Department, including all subcontractors, personal services contractors, or any other category of person who acts for or on behalf of the Department, as determined by the Secretary; or

''(B) State, local, tribal, territorial, and private sector personnel who possess security clearances granted by the Department.

''(3) INSIDER THREAT.—The term 'insider threat' means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States, including damage to the United States through espionage,

terrorism, the unauthorized disclosure of classified national security information, or through the loss or degradation of departmental resources or capabilities.''.

(b) REPORTING.—

(1) IN GENERAL.—Not later than two years after the date of the enactment of section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) and the biennially thereafter for the next four years, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate a report on how the Department of Homeland Security and its components and offices have implemented the strategy developed pursuant to subsection (b)(2)(A) of such section 104, the status of the Department's risk assessment of critical assets, the types of insider threat training conducted, the number of Department employees who have received such training, and information on the effectiveness of the Insider Threat Program (established pursuant to subsection (a) of such section

104), based on metrics developed, collected, and reported pursuant to subsection (b)(2)(H) of such section 104.

(2) DEFINITIONS.—In this subsection, the terms ''critical assets'', ''insider'', and ''insider threat'' have the meanings given such terms in section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section).

(c) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 103 the following new item:

''Sec. 104. Insider Threat Program.''.

○