Calendar No. 553

114TH CONGRESS
2D SESSION

H. R. 3361

[Report No. 114–297]

IN THE SENATE OF THE UNITED STATES

NOVEMBER 3, 2015

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

JULY 12, 2016

Reported by Mr. JOHNSON, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

AN ACT

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 2015".~~

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 1 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) REPORT.—Not later than 2 years after the date of the enactment of this section and the biennially thereafter for the next 4 years, the Secretary 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 and its components and offices have implemented the strategy developed under subsection (b)(2)(A), 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, based on metrics under subsection (b)(2)(H).

"(d) 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) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by in-

~~serting after the item relating to section 103 the following new item:~~

~~"Sec. 104. Insider Threat Program.".~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "Department of Homeland Security Insider Threat and Mitigation Act of 2016".

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:

"SEC. 104. INSIDER THREAT PROGRAM.

"(a) ESTABLISHMENT.—The Secretary shall establish an Insider Threat Program within the Department, which shall—

"(1) provide training and education for employees of the Department 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.—

"(A) ESTABLISHMENT.—The Secretary shall establish a Steering Committee within the Department.

"(B) MEMBERSHIP.—The membership of the Steering Committee shall be as follows:

"(i) The Under Secretary for Intelligence and Analysis shall serve as the Chairperson of the Steering Committee.

"(ii) The Chief Security Officer shall serve as the Vice Chairperson of the Steering Committee.

"(iii) The other members of 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.

"(C) MEETINGS.—The members of the Steering Committee 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 1 year after the date of enactment of this section, the Under Secretary for Intelligence and Analysis and the Chief Security Officer, in coordination with the Steering Committee, 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 programmatic and technology best practices adopted by the Federal Govern-

ment, 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) 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, best practices, and available technology; and

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

"(c) DISCIPLINE OF EMPLOYEES ENGAGED IN INSIDER MISCONDUCT.—

"(1) IN GENERAL.—In accordance with paragraph (2), the head of an agency or a component of an agency employing an insider employee shall propose—

"(A) for an insider employee whom an appropriate entity determines knowingly or recklessly engaged in insider misconduct, removal; and

"(B) for an insider employee whom an appropriate entity determines negligently engaged in insider misconduct—

"(i) an adverse action that is not less than a 12-day suspension, with respect to the first instance; and

"(ii) removal, for any subsequent instance.

"(2) PROCEDURES.—

"(A) NOTICE.—An insider employee against whom an adverse action under paragraph (1) is proposed is entitled to written notice.

"(B) ANSWER AND EVIDENCE.—

"(i) IN GENERAL.—An insider employee who is notified under subparagraph (A) that the insider employee is the subject of a proposed adverse action under paragraph (1) is entitled to 14 days following such notification to answer and furnish evidence in support of the answer.

"(ii) NO EVIDENCE.—After the end of the 14-day period described in clause (i), if an insider employee does not furnish evidence as described in clause (i) or if the head of the agency or component of the agency employing the insider employee determines that such evidence is not sufficient to reverse the proposed adverse action, the head of the agency or component of the agency shall carry out the adverse action.

"(C) SCOPE OF PROCEDURES.—Paragraphs (1) and (2) of subsection (b) and subsection (c) of section 7513 of title 5, United States Code, and paragraphs (1) and (2) of subsection (b) and subsection (c) of 7543 of title 5, United States Code, shall not apply with respect to an adverse action carried out under this subsection.

"(3) LIMITATION ON OTHER ADVERSE ACTIONS.—With respect to insider misconduct, if the head of the agency or component of the agency employing an insider employee carries out an adverse action against the insider employee under another provision of law, the head of the agency or component of the agency may carry out an additional adverse

action under this subsection based on the same insider misconduct.

"(d) REPORT.—Not later than 2 years after the date of the enactment of this section, and every 2 years thereafter for the next 4 years, the Secretary 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—

"(1) how the Department and its components and offices have implemented the strategy developed under subsection (b)(2)(A);

"(2) the status of the Department's risk assessment of critical assets;

"(3) the types of insider threat training conducted by the Department;

"(4) the number of employees of the Department who have received such training; and

"(5) information on the effectiveness of the Insider Threat Program, based on metrics under subsection (b)(2)(H).

"(e) PRESERVATION OF MERIT SYSTEM RIGHTS.—

"(1) IN GENERAL.—The Steering Committee shall not seek to, and the authorities provided under

this section shall not be used to, deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)) (commonly known as the 'Intelligence Community Whistleblower Protection Act of 1998'), chapter 12 or 23 of title 5, United States Code, the Inspector General Act of 1978 (5 U.S.C. App.), or any other whistleblower statute, regulation, or policy.

"(2) IMPLEMENTATION.—

"(A) IN GENERAL.—Any activity carried out under this section shall be subject to section 115 of the Whistleblower Protection Enhancement Act of 2012 (5 U.S.C. 2302 note).

"(B) REQUIRED STATEMENT.—Any activity to implement or enforce any insider threat activity or authority under this section or Executive Order 13587 (50 U.S.C. 3161 note) shall include the statement required by section 115 of the Whistleblower Protection Enhancement Act of 2012 (5 U.S.C. 2302 note) that preserves rights under whistleblower laws and section 7211 of title 5, United States Code, protecting communications with Congress.

"(f) DEFINITIONS.—In this section:

"(1) APPROPRIATE ENTITY.—The term 'appropriate entity' means—

"(A) the head of an agency or a component of an agency;

"(B) an administrative law judge;

"(C) the Merit Systems Protection Board;

"(D) the Office of Special Counsel;

"(E) an adjudicating body provided under a union contract;

"(F) a Federal judge; and

"(G) the Inspector General of the Department.

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

"(3) EMPLOYEE.—The term 'employee' means an employee, as defined under section 7103(a) of title 5, United States Code.

"(4) 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.

"(5) INSIDER EMPLOYEE.—The term 'insider employee' means an insider who is an employee.

"(6) INSIDER MISCONDUCT.—The term 'insider misconduct' means harm to the security of the United States, including damage to the United States through espionage, terrorism, or the unauthorized disclosure of classified national security information, or through the loss or degradation of departmental resources or capabilities, through use of authorized access by an insider employee.

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

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

"(8) STEERING COMMITTEE.—The term 'Steering Committee' means the Steering Committee established under subsection (b)(1)(A).".

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

"Sec. 104. Insider Threat Program.".

Calendar No. 553

114TH CONGRESS
2D SESSION

H. R. 3361

[Report No. 114–297]

AN ACT

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

JULY 12, 2016

Reported with an amendment