

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Department of Home-
5 land Security Insider Threat and Mitigation Act of 2015”.

1 **SEC. 2. ESTABLISHMENT OF INSIDER THREAT PROGRAM.**

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

5 **“SEC. 104. INSIDER THREAT PROGRAM.**

6 “(a) ESTABLISHMENT.—The Secretary shall estab-
7 lish an Insider Threat Program within the Department.
8 Such Program shall—

9 “(1) provide training and education for Depart-
10 ment personnel to identify, prevent, mitigate, and re-
11 spond to insider threat risks to the Department’s
12 critical assets;

13 “(2) provide investigative support regarding po-
14 tential insider threats that may pose a risk to the
15 Department’s critical assets; and

16 “(3) conduct risk mitigation activities for in-
17 sider threats.

18 “(b) STEERING COMMITTEE.—

19 “(1) IN GENERAL.—The Secretary shall estab-
20 lish a Steering Committee within the Department.
21 The Under Secretary for Intelligence and Analysis
22 shall serve as the Chair of the Steering Committee.
23 The Chief Security Officer shall serve as the Vice
24 Chair. The Steering Committee shall be comprised
25 of representatives of the Office of Intelligence and
26 Analysis, the Office of the Chief Information Officer,

1 the Office of the General Counsel, the Office for
2 Civil Rights and Civil Liberties, the Privacy Office,
3 the Office of the Chief Human Capital Officer, the
4 Office of the Chief Financial Officer, the Federal
5 Protective Service, the Office of the Chief Procure-
6 ment Officer, the Science and Technology Direc-
7 torate, and other components or offices of the De-
8 partment as appropriate. Such representatives shall
9 meet on a regular basis to discuss cases and issues
10 related to insider threats to the Department's crit-
11 ical assets, in accordance with subsection (a).

12 “(2) RESPONSIBILITIES.—Not later than 1 year
13 after the date of the enactment of this section, the
14 Under Secretary for Intelligence and Analysis and
15 the Chief Security Officer, in coordination with the
16 Steering Committee established pursuant to para-
17 graph (1), shall—

18 “(A) develop a holistic strategy for Depart-
19 ment-wide efforts to identify, prevent, mitigate,
20 and respond to insider threats to the Depart-
21 ment's critical assets;

22 “(B) develop a plan to implement the in-
23 sider threat measures identified in the strategy
24 developed under subparagraph (A) across the
25 components and offices of the Department;

1 “(C) document insider threat policies and
2 controls;

3 “(D) conduct a baseline risk assessment of
4 insider threats posed to the Department’s crit-
5 ical assets;

6 “(E) examine existing programmatic and
7 technology best practices adopted by the Fed-
8 eral Government, industry, and research insti-
9 tutions to implement solutions that are vali-
10 dated and cost-effective;

11 “(F) develop a timeline for deploying work-
12 place monitoring technologies, employee aware-
13 ness campaigns, and education and training
14 programs related to identifying, preventing,
15 mitigating, and responding to potential insider
16 threats to the Department’s critical assets;

17 “(G) require the Chair and Vice Chair of
18 the Steering Committee to consult with the
19 Under Secretary for Science and Technology
20 and other appropriate stakeholders to ensure
21 the Insider Threat Program is informed, on an
22 ongoing basis, by current information regarding
23 threats, beset practices, and available tech-
24 nology; and

1 “(H) develop, collect, and report metrics
 2 on the effectiveness of the Department’s insider
 3 threat mitigation efforts.

4 “(c) REPORT.—Not later than 2 years after the date
 5 of the enactment of this section and the biennially there-
 6 after for the next 4 years, the Secretary shall submit to
 7 the Committee on Homeland Security and the Permanent
 8 Select Committee on Intelligence of the House of Rep-
 9 resentatives and the Committee on Homeland Security
 10 and Governmental Affairs and the Select Committee on
 11 Intelligence of the Senate a report on how the Department
 12 and its components and offices have implemented the
 13 strategy developed under subsection (b)(2)(A), the status
 14 of the Department’s risk assessment of critical assets, the
 15 types of insider threat training conducted, the number of
 16 Department employees who have received such training,
 17 and information on the effectiveness of the Insider Threat
 18 Program, based on metrics under subsection (b)(2)(H).

19 “(d) DEFINITIONS.—In this section:

20 “(1) CRITICAL ASSETS.—The term ‘critical as-
 21 sets’ means the people, facilities, information, and
 22 technology required for the Department to fulfill its
 23 mission.

24 “(2) INSIDER.—The term ‘insider’ means—

1 “(A) any person who has access to classi-
2 fied national security information and is em-
3 ployed by, detailed to, or assigned to the De-
4 partment, including members of the Armed
5 Forces, experts or consultants to the Depart-
6 ment, industrial or commercial contractors, li-
7 censees, certificate holders, or grantees of the
8 Department, including all subcontractors, per-
9 sonal services contractors, or any other category
10 of person who acts for or on behalf of the De-
11 partment, as determined by the Secretary; or

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

15 “(3) ~~INSIDER THREAT.~~—The term ‘insider
16 threat’ means the threat that an insider will use his
17 or her authorized access, wittingly or unwittingly, to
18 do harm to the security of the United States, includ-
19 ing damage to the United States through espionage,
20 terrorism, the unauthorized disclosure of classified
21 national security information, or through the loss or
22 degradation of departmental resources or capabili-
23 ties.”.

24 (b) ~~CLERICAL AMENDMENT.~~—The table of contents
25 of the Homeland Security Act of 2002 is amended by in-

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

~~“Sec. 104. Insider Threat Program.”.~~

3 **SECTION 1. SHORT TITLE.**

4 *This Act may be cited as the “Department of Home-*
 5 *land Security Insider Threat and Mitigation Act of 2016”.*

6 **SEC. 2. ESTABLISHMENT OF INSIDER THREAT PROGRAM.**

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

10 **“SEC. 104. INSIDER THREAT PROGRAM.**

11 *“(a) ESTABLISHMENT.—The Secretary shall establish*
 12 *an Insider Threat Program within the Department, which*
 13 *shall—*

14 *“(1) provide training and education for employ-*
 15 *ees of the Department to identify, prevent, mitigate,*
 16 *and respond to insider threat risks to the Depart-*
 17 *ment’s critical assets;*

18 *“(2) provide investigative support regarding po-*
 19 *tential insider threats that may pose a risk to the De-*
 20 *partment’s critical assets; and*

21 *“(3) conduct risk mitigation activities for in-*
 22 *sider threats.*

23 *“(b) STEERING COMMITTEE.—*

24 *“(1) IN GENERAL.—*

1 “(A) *ESTABLISHMENT.*—*The Secretary shall*
2 *establish a Steering Committee within the De-*
3 *partment.*

4 “(B) *MEMBERSHIP.*—*The membership of*
5 *the Steering Committee shall be as follows:*

6 “(i) *The Under Secretary for Intel-*
7 *ligence and Analysis shall serve as the*
8 *Chairperson of the Steering Committee.*

9 “(ii) *The Chief Security Officer shall*
10 *serve as the Vice Chairperson of the Steer-*
11 *ing Committee.*

12 “(iii) *The other members of the Steer-*
13 *ing Committee shall be comprised of rep-*
14 *resentatives of the Office of Intelligence and*
15 *Analysis, the Office of the Chief Information*
16 *Officer, the Office of the General Counsel,*
17 *the Office for Civil Rights and Civil Lib-*
18 *erties, the Privacy Office, the Office of the*
19 *Chief Human Capital Officer, the Office of*
20 *the Chief Financial Officer, the Federal*
21 *Protective Service, the Office of the Chief*
22 *Procurement Officer, the Science and Tech-*
23 *nology Directorate, and other components or*
24 *offices of the Department, as appropriate.*

1 “(C) *MEETINGS.*—*The members of the*
2 *Steering Committee shall meet on a regular basis*
3 *to discuss cases and issues related to insider*
4 *threats to the Department’s critical assets, in ac-*
5 *cordance with subsection (a).*

6 “(2) *RESPONSIBILITIES.*—*Not later than 1 year*
7 *after the date of enactment of this section, the Under*
8 *Secretary for Intelligence and Analysis and the Chief*
9 *Security Officer, in coordination with the Steering*
10 *Committee, shall—*

11 “(A) *develop a holistic strategy for Depart-*
12 *ment-wide efforts to identify, prevent, mitigate,*
13 *and respond to insider threats to the Depart-*
14 *ment’s critical assets;*

15 “(B) *develop a plan to implement the in-*
16 *sider threat measures identified in the strategy*
17 *developed under subparagraph (A) across the*
18 *components and offices of the Department;*

19 “(C) *document insider threat policies and*
20 *controls;*

21 “(D) *conduct a baseline risk assessment of*
22 *insider threats posed to the Department’s critical*
23 *assets;*

24 “(E) *examine programmatic and technology*
25 *best practices adopted by the Federal Govern-*

1 *ment, industry, and research institutions to im-*
2 *plement solutions that are validated and cost-ef-*
3 *fective;*

4 “(F) *develop a timeline for deploying work-*
5 *place monitoring technologies, employee aware-*
6 *ness campaigns, and education and training*
7 *programs related to identifying, preventing,*
8 *mitigating, and responding to potential insider*
9 *threats to the Department’s critical assets;*

10 “(G) *consult with the Under Secretary for*
11 *Science and Technology and other appropriate*
12 *stakeholders to ensure the Insider Threat Pro-*
13 *gram is informed, on an ongoing basis, by cur-*
14 *rent information regarding threats, best prac-*
15 *tices, and available technology; and*

16 “(H) *develop, collect, and report metrics on*
17 *the effectiveness of the Department’s insider*
18 *threat mitigation efforts.*

19 “(c) *DISCIPLINE OF EMPLOYEES ENGAGED IN INSIDER*
20 *MISCONDUCT.—*

21 “(1) *IN GENERAL.—In accordance with para-*
22 *graph (2), the head of an agency or a component of*
23 *an agency employing an insider employee shall pro-*
24 *pose—*

1 “(A) for an insider employee whom an ap-
2 propriate entity determines knowingly or reck-
3 lessly engaged in insider misconduct, removal;
4 and

5 “(B) for an insider employee whom an ap-
6 propriate entity determines negligently engaged
7 in insider misconduct—

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

11 “(ii) removal, for any subsequent in-
12 stance.

13 “(2) PROCEDURES.—

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

17 “(B) ANSWER AND EVIDENCE.—

18 “(i) IN GENERAL.—An insider em-
19 ployee who is notified under subparagraph
20 (A) that the insider employee is the subject
21 of a proposed adverse action under para-
22 graph (1) is entitled to 14 days following
23 such notification to answer and furnish evi-
24 dence in support of the answer.

1 “(ii) *NO EVIDENCE.*—After the end of
2 the 14-day period described in clause (i), if
3 an insider employee does not furnish evi-
4 dence as described in clause (i) or if the
5 head of the agency or component of the
6 agency employing the insider employee de-
7 termines that such evidence is not sufficient
8 to reverse the proposed adverse action, the
9 head of the agency or component of the
10 agency shall carry out the adverse action.

11 “(C) *SCOPE OF PROCEDURES.*—Paragraphs
12 (1) and (2) of subsection (b) and subsection (c)
13 of section 7513 of title 5, United States Code,
14 and paragraphs (1) and (2) of subsection (b)
15 and subsection (c) of 7543 of title 5, United
16 States Code, shall not apply with respect to an
17 adverse action carried out under this subsection.

18 “(3) *LIMITATION ON OTHER ADVERSE AC-*
19 *TIONS.*—With respect to insider misconduct, if the
20 head of the agency or component of the agency em-
21 ploying an insider employee carries out an adverse
22 action against the insider employee under another
23 provision of law, the head of the agency or component
24 of the agency may carry out an additional adverse

1 *action under this subsection based on the same insider*
 2 *misconduct.*

3 “(d) *REPORT.—Not later than 2 years after the date*
 4 *of the enactment of this section, and every 2 years thereafter*
 5 *for the next 4 years, the Secretary shall submit to the Com-*
 6 *mittee on Homeland Security and the Permanent Select*
 7 *Committee on Intelligence of the House of Representatives*
 8 *and the Committee on Homeland Security and Govern-*
 9 *mental Affairs and the Select Committee on Intelligence of*
 10 *the Senate a report on—*

11 “(1) *how the Department and its components*
 12 *and offices have implemented the strategy developed*
 13 *under subsection (b)(2)(A);*

14 “(2) *the status of the Department’s risk assess-*
 15 *ment of critical assets;*

16 “(3) *the types of insider threat training con-*
 17 *ducted by the Department;*

18 “(4) *the number of employees of the Department*
 19 *who have received such training; and*

20 “(5) *information on the effectiveness of the In-*
 21 *sider Threat Program, based on metrics under sub-*
 22 *section (b)(2)(H).*

23 “(e) *PRESERVATION OF MERIT SYSTEM RIGHTS.—*

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

1 *this section shall not be used to, deter, detect, or miti-*
2 *gate disclosures of information by Government em-*
3 *ployees or contractors that are lawful under and pro-*
4 *ected by section 17(d)(5) of the Central Intelligence*
5 *Agency Act of 1949 (50 U.S.C. 3517(d)(5)) (com-*
6 *monly known as the ‘Intelligence Community Whistle-*
7 *blower Protection Act of 1998’), chapter 12 or 23 of*
8 *title 5, United States Code, the Inspector General Act*
9 *of 1978 (5 U.S.C. App.), or any other whistleblower*
10 *statute, regulation, or policy.*

11 “(2) *IMPLEMENTATION.—*

12 “(A) *IN GENERAL.—Any activity carried*
13 *out under this section shall be subject to section*
14 *115 of the Whistleblower Protection Enhance-*
15 *ment Act of 2012 (5 U.S.C. 2302 note).*

16 “(B) *REQUIRED STATEMENT.—Any activity*
17 *to implement or enforce any insider threat activ-*
18 *ity or authority under this section or Executive*
19 *Order 13587 (50 U.S.C. 3161 note) shall include*
20 *the statement required by section 115 of the*
21 *Whistleblower Protection Enhancement Act of*
22 *2012 (5 U.S.C. 2302 note) that preserves rights*
23 *under whistleblower laws and section 7211 of*
24 *title 5, United States Code, protecting commu-*
25 *nications with Congress.*

1 “(f) *DEFINITIONS.—In this section:*

2 “(1) *APPROPRIATE ENTITY.—The term ‘appropriate*
3 *entity’ means—*

4 “(A) *the head of an agency or a component*
5 *of an agency;*

6 “(B) *an administrative law judge;*

7 “(C) *the Merit Systems Protection Board;*

8 “(D) *the Office of Special Counsel;*

9 “(E) *an adjudicating body provided under*
10 *a union contract;*

11 “(F) *a Federal judge; and*

12 “(G) *the Inspector General of the Depart-*
13 *ment.*

14 “(2) *CRITICAL ASSETS.—The term ‘critical as-*
15 *sets’ means the people, facilities, information, and*
16 *technology required for the Department to fulfill its*
17 *mission.*

18 “(3) *EMPLOYEE.—The term ‘employee’ means an*
19 *employee, as defined under section 7103(a) of title 5,*
20 *United States Code.*

21 “(4) *INSIDER.—The term ‘insider’ means—*

22 “(A) *any person who has access to classified*
23 *national security information and is employed*
24 *by, detailed to, or assigned to the Department,*
25 *including members of the Armed Forces, experts*

1 *or consultants to the Department, industrial or*
2 *commercial contractors, licensees, certificate*
3 *holders, or grantees of the Department, including*
4 *all subcontractors, personal services contractors,*
5 *or any other category of person who acts for or*
6 *on behalf of the Department, as determined by*
7 *the Secretary; or*

8 *“(B) State, local, tribal, territorial, and*
9 *private sector personnel who possess security*
10 *clearances granted by the Department.*

11 *“(5) INSIDER EMPLOYEE.—The term ‘insider em-*
12 *ployee’ means an insider who is an employee.*

13 *“(6) INSIDER MISCONDUCT.—The term ‘insider*
14 *misconduct’ means harm to the security of the United*
15 *States, including damage to the United States*
16 *through espionage, terrorism, or the unauthorized dis-*
17 *closure of classified national security information, or*
18 *through the loss or degradation of departmental re-*
19 *sources or capabilities, through use of authorized ac-*
20 *cess by an insider employee.*

21 *“(7) INSIDER THREAT.—The term ‘insider*
22 *threat’ means the threat that an insider will use the*
23 *authorized access of the insider, wittingly or unwit-*
24 *tingly, to do harm to the security of the United*
25 *States, including damage to the United States*

1 *through espionage, terrorism, or the unauthorized dis-*
2 *closure of classified national security information, or*
3 *through the loss or degradation of departmental re-*
4 *sources or capabilities.*

5 “(8) *STEERING COMMITTEE.*—*The term ‘Steering*
6 *Committee’ means the Steering Committee established*
7 *under subsection (b)(1)(A).’.*”

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

 “*Sec. 104. Insider Threat Program.*”.

Calendar No. 553

114TH CONGRESS
2^D 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