

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: In the nature of a substitute.

**IN THE SENATE OF THE UNITED STATES—114th Cong., 2d Sess.**

**H. R. 3361**

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

Referred to the Committee on \_\_\_\_\_ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mr. JOHNSON

Viz:

1 Strike all after the enacting clause and insert the fol-  
2 lowing:

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:

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

2 “(a) ESTABLISHMENT.—The Secretary shall estab-  
3 lish an Insider Threat Program within the Department,  
4 which shall—

5 “(1) provide training and education for employ-  
6 ees of the Department to identify, prevent, mitigate,  
7 and respond to insider threat risks to the Depart-  
8 ment’s critical assets;

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

12 “(3) conduct risk mitigation activities for in-  
13 sider threats.

14 “(b) STEERING COMMITTEE.—

15 “(1) IN GENERAL.—

16 “(A) ESTABLISHMENT.—The Secretary  
17 shall establish a Steering Committee within the  
18 Department.

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

21 “(i) The Under Secretary for Intel-  
22 ligence and Analysis shall serve as the  
23 Chairperson of the Steering Committee.

24 “(ii) The Chief Security Officer shall  
25 serve as the Vice Chairperson of the Steer-  
26 ing Committee.

1                   “(iii) The other members of the Steer-  
2                   ing Committee shall be comprised of rep-  
3                   resentatives of the Office of Intelligence  
4                   and Analysis, the Office of the Chief Infor-  
5                   mation Officer, the Office of the General  
6                   Counsel, the Office for Civil Rights and  
7                   Civil Liberties, the Privacy Office, the Of-  
8                   fice of the Chief Human Capital Officer,  
9                   the Office of the Chief Financial Officer,  
10                  the Federal Protective Service, the Office  
11                  of the Chief Procurement Officer, the  
12                  Science and Technology Directorate, and  
13                  other components or offices of the Depart-  
14                  ment, as appropriate.

15                  “(C) MEETINGS.—The members of the  
16                  Steering Committee shall meet on a regular  
17                  basis to discuss cases and issues related to in-  
18                  sider threats to the Department’s critical as-  
19                  sets, in accordance with subsection (a).

20                  “(2) RESPONSIBILITIES.—Not later than 1 year  
21                  after the date of enactment of this section, the  
22                  Under Secretary for Intelligence and Analysis and  
23                  the Chief Security Officer, in coordination with the  
24                  Steering Committee, shall—

1           “(A) develop a holistic strategy for Depart-  
2           ment-wide efforts to identify, prevent, mitigate,  
3           and respond to insider threats to the Depart-  
4           ment’s critical assets;

5           “(B) develop a plan to implement the in-  
6           sider threat measures identified in the strategy  
7           developed under subparagraph (A) across the  
8           components and offices of the Department;

9           “(C) document insider threat policies and  
10          controls;

11          “(D) conduct a baseline risk assessment of  
12          insider threats posed to the Department’s crit-  
13          ical assets;

14          “(E) examine programmatic and tech-  
15          nology best practices adopted by the Federal  
16          Government, industry, and research institutions  
17          to implement solutions that are validated and  
18          cost-effective;

19          “(F) develop a timeline for deploying work-  
20          place monitoring technologies, employee aware-  
21          ness campaigns, and education and training  
22          programs related to identifying, preventing,  
23          mitigating, and responding to potential insider  
24          threats to the Department’s critical assets;

1           “(G) consult with the Under Secretary for  
2 Science and Technology and other appropriate  
3 stakeholders to ensure the Insider Threat Pro-  
4 gram is informed, on an ongoing basis, by cur-  
5 rent information regarding threats, beset prac-  
6 tices, and available technology; and

7           “(H) develop, collect, and report metrics  
8 on the effectiveness of the Department’s insider  
9 threat mitigation efforts.

10       “(c) DISCIPLINE OF EMPLOYEES ENGAGED IN IN-  
11 SIDER MISCONDUCT.—

12           “(1) IN GENERAL.—In accordance with para-  
13 graph (2), the head of an agency employing an in-  
14 sider employee shall propose—

15           “(A) for an insider employee whom an ad-  
16 judicatory authority determines knowingly or  
17 recklessly engaged in insider misconduct, re-  
18 moval; and

19           “(B) for an insider employee whom an ad-  
20 judicatory authority determines negligently en-  
21 gaged in insider misconduct—

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

1                   “(ii) removal, for any subsequent in-  
2                   stance.

3                   “(2) PROCEDURES.—

4                   “(A) NOTICE.—An insider employee  
5                   against whom an adverse action under para-  
6                   graph (1) is proposed is entitled to written no-  
7                   tice.

8                   “(B) ANSWER AND EVIDENCE.—

9                   “(i) IN GENERAL.—An insider em-  
10                  ployee who is notified under subparagraph  
11                  (A) that the insider employee is the subject  
12                  of a proposed adverse action under para-  
13                  graph (1) is entitled to 14 days following  
14                  such notification to answer and furnish  
15                  evidence in support of the answer.

16                  “(ii) NO EVIDENCE.—After the end of  
17                  the 14-day period described in clause (i), if  
18                  an insider employee does not furnish evi-  
19                  dence as described in clause (i) or if the  
20                  head of the agency employing the insider  
21                  employee determines that such evidence is  
22                  not sufficient to reverse the proposed ad-  
23                  verse action, the head of the agency shall  
24                  carry out the adverse action.

1           “(C) SCOPE OF PROCEDURES.—Para-  
2           graphs (1) and (2) of subsection (b) and sub-  
3           subsection (c) of section 7513 of title 5, United  
4           States Code, and paragraphs (1) and (2) of  
5           subsection (b) and subsection (c) of 7543 of  
6           title 5, United States Code, shall not apply with  
7           respect to an adverse action carried out under  
8           this subsection.

9           “(3) LIMITATION ON OTHER ADVERSE AC-  
10          TIONS.—With respect to insider misconduct, if the  
11          head of the agency employing an insider employee  
12          carries out an adverse action against the insider em-  
13          ployee under another provision of law, the head of  
14          the agency may carry out an additional adverse ac-  
15          tion under this section based on the same insider  
16          misconduct.

17          “(d) REPORT.—Not later than 2 years after the date  
18          of the enactment of this section, and every 2 years there-  
19          after for the next 4 years, the Secretary shall submit to  
20          the Committee on Homeland Security and the Permanent  
21          Select Committee on Intelligence of the House of Rep-  
22          resentatives and the Committee on Homeland Security  
23          and Governmental Affairs and the Select Committee on  
24          Intelligence of the Senate a report on—

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

4           “(2) the status of the Department’s risk assess-  
5           ment of critical assets;

6           “(3) the types of insider threat training con-  
7           ducted by the Department;

8           “(4) the number of employees of the Depart-  
9           ment who have received such training; and

10          “(5) information on the effectiveness of the In-  
11          sider Threat Program, based on metrics under sub-  
12          section (b)(2)(H).

13          “(e) DEFINITIONS.—In this section:

14                 “(1) ADJUDICATORY AUTHORITY.—The term  
15                 ‘adjudicatory authority’ means—

16                         “(A) a person with the rank of Assistant  
17                         Secretary or higher at the Department;

18                         “(B) an administrative law judge;

19                         “(C) the Merit Systems Protection Board;

20                         “(D) the Office of Special Counsel;

21                         “(E) an adjudicating body provided under  
22                         a union contract;

23                         “(F) a Federal judge; and

24                         “(G) the Inspector General of the Depart-  
25                         ment.



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

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

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

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

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

23           “(5) INSIDER EMPLOYEE.—The term ‘insider  
24           employee’ means an insider who is an employee.

1           “(6) INSIDER MISCONDUCT.—The term ‘insider  
2           misconduct’ means harm to the security of the  
3           United States, including damage to the United  
4           States through espionage, terrorism, the unauthor-  
5           ized disclosure of classified national security infor-  
6           mation, or through the loss or degradation of de-  
7           partmental resources or capabilities, through use of  
8           authorized access by an insider employee.

9           “(7) INSIDER THREAT.—The term ‘insider  
10          threat’ means the threat that an insider will use the  
11          authorized access of the insider, wittingly or unwit-  
12          tingly, to do harm to the security of the United  
13          States, including damage to the United States  
14          through espionage, terrorism, the unauthorized dis-  
15          closure of classified national security information, or  
16          through the loss or degradation of departmental re-  
17          sources or capabilities.

18          “(8) STEERING COMMITTEE.—The term ‘Steer-  
19          ing Committee’ means the Steering Committee es-  
20          tablished under subsection (b)(1)(A).”.

21          (b) CLERICAL AMENDMENT.—The table of contents  
22          for the Homeland Security Act of 2002 is amended by  
23          inserting after the item relating to section 103 the fol-  
24          lowing:

“Sec. 104. Insider Threat Program.”.