Calendar No. 553

114TH CONGRESS *2d Session*	SENATE	REPORT 114–297

DEPARTMENT OF HOMELAND SECURITY INSIDER THREAT AND MITIGATION ACT OF 2015

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

H.R. 3361

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO ESTABLISH THE INSIDER THREAT PROGRAM, AND FOR OTHER PURPOSES

JULY 12, 2016.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
59–010 WASHINGTON : 2016

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire
JONI ERNST, Iowa
BEN SASSE, Nebraska

THOMAS R. CARPER, Delaware
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota
CORY A. BOOKER, New Jersey
GARY C. PETERS, Michigan

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
ELIZABETH MCWHORTER, *Senior Professional Staff Member*
GABRIELLE A. BATKIN, *Minority Staff Director*
JOHN P. KILVINGTON, *Minority Deputy Staff Director*
MARY BETH SCHULTZ, *Minority Chief Counsel*
MATTHEW R. GROTE, *Minority Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 553

114TH CONGRESS *2d Session* | SENATE | REPORT 114–297

HOMELAND SECURITY ACT OF 2002

JULY 12, 2016.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany H.R. 3361]

The Committee on Homeland Security and Governmental Affairs, to which was referred the act (H.R. 3361), to amend the Homeland Security Act of 2002 to establish the Insider Threat Program, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The purpose of H.R. 3361, the Department of Homeland Security Insider Threat and Mitigation Act of 2016, is to establish an Insider Threat Program (ITP) within the Department of Homeland Security (DHS or "the Department"). The act mandates an ITP structure that improves employee identification, prevention, and mitigation of risks to the Department's critical assets. It also establishes an internal DHS Steering Committee to manage and coordinate DHS activities related to insider threat issues, includes employee education and training, and strengthens the Department's ability to discipline employees found to be insider threats. The act

requires the Secretary to report to Congress on implementation progress and the metrics-based effectiveness of the ITP.

II. Background and the Need for Legislation

As evolving computer technology becomes an increasingly pervasive part of everyday life, both government and private entities have grown dependent on information technology (IT) systems to process, maintain, and transmit sensitive information.[1] This reliance on IT drives a persistent and evolving insider threat to Federal IT systems that manage national security critical assets.[2]

It has been "insiders" with trusted access within the United States Government who have conducted some of the most egregious releases of classified information and espionage in recent years. In 2010, United States Army PFC Manning used access to classified databases to leak classified information that would ultimately be published online.[3] Edward Snowden continues to evade criminal prosecution after he used his access to classified databases to steal and publish classified information related to sensitive national security programs.[4]

Publicized security leaks inspired the 2011 Executive Order 13587 "Structural Reforms to Improve Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."[5] This Executive Order requires that "the heads of agencies that operate or access classified computer networks" shall "implement an insider threat detection and prevention program."[6]

Although according to the Department, current efforts align with the requirements of these policies, H.R. 3361 ensures the Department will maintain a management structure for the ITP that is the most effective for the purposes of national security. This structure involves a multidisciplinary steering committee that coordinates Department-wide activities related to insider threats to its critical assets, including the identification of potential threats. The act also directs the Department to conduct a risk assessment of its critical assets, including its networks, facilities, workforce, and information.

However, the 2011 Executive Order 13587 and a 2012 Presidential memorandum on ITPs only require the Department ITP to

---

[1] GOV'T Accountability Office, GAO–13–187, Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented 1 (2013), *available at* http://www.gao.gov/assets/660/652170.pdf.

[2] *Id.*

[3] *See id.; see also* Ellen Nakashima & Julie Tate, *Prosecutors Say Manning and Assange Collaborated in Stealing Secret Documents*, Wash. Post (Dec. 22, 2011), https://www.washingtonpost.com/national/national-security/prosecutors-say-manning-and-assange-collaborated-in-stealing-secret-documents/2011/12/22/gIQARwAXCP_story.html.

[4] *See generally* Jordan Fabian, *White House Stands Firm on Snowden Prosecution*, The Hill (June 1, 2015), http://thehill.com/homenews/administration/243643-amid-nsa-furor-white-house-standing-firm-on-snowden-prosecution; *Safeguarding Our Nation's Secrets: Examining the Security Clearance Process: Joint Hearing Before the S. Subcomm. on Efficiency and Effectiveness of Fed. Programs and the Fed. Workforce and the S. Subcomm. on Fin. and Contracting Oversight of the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. (2013); *Open Hearing: Current and Projected National Security Threats Against the United States: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. (2014) (statement of James R. Clapper, Director of National Intelligence).

[5] Gov't Accountability Office, GAO–15–544, Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems 6 (2015), *available at* http://gao.gov/assets/680/670570.pdf.

[6] Exec. Order No. 13,587, 3 C.F.R. 63811 (2011), *available at* http://www.archives.gov/isoo/policy-documents/eo-13587.pdf.

cover classified systems.[7] Insider threats can affect both classified and unclassified systems, as the Department of Defense learned in 2008 when malicious software on an infected flash drive spread through both system types at a military base in the Middle East.[8] The intelligence and security communities recommended and strongly urged that the DHS ITP should cover the Department's unclassified systems as well.[9] H.R. 3361 will expand the ITP to cover both the Department's classified and unclassified critical assets.

In the event an employee is found to be an insider threat, the substitute amendment empowers the Secretary of DHS to further prevent and mitigate insider threats by requiring certain disciplinary actions against that employee. Overall, this act establishes an effective ITP structure to secure Department facilities, its workforce, and its critical assets—both classified and unclassified.

The extreme cases of intentional insider threats mentioned above highlight the need for a strong ITP within departments and agencies with national security responsibilities. Intentional attacks aside, unwitting employee data breaches also pose a significant risk to the security of Federal systems. Of the 200 Federal IT decision makers surveyed under a study published in 2015 to identify critical cybersecurity challenges, more than half (53 percent) "identified careless and untrained insiders as the greatest source of IT security threats at their agencies." [10] This represented a 42 percent increase from the previous year.[11]

While the number of respondents that indicated careless and untrained insiders as the foremost cybersecurity issue dropped to 48 percent in 2016, it is still tied for the top security threat.[12] This means that for the third survey in as many years, over 40 percent of Federal IT professionals highlighted employee security training and education as a necessary investment for threat prevention.

In 2015, a different survey of 150 Federal IT managers, as well as a Government Accountability Office (GAO) report, identified the vulnerability of Federal systems to insider threats. Results of that survey revealed that nearly half of Federal agencies were targets of insider threats and nearly one in three (29 percent) suffered a loss of data due to an insider.[13]

Meanwhile, GAO reported steadily increasing information security incidents affecting Federal systems from fiscal year (FY) 2006

---

[7] Exec. Order No. 13,587, 3 C.F.R. 63811 (2011), *available at* http://www.archives.gov/isoo/policy-documents/eo-13587.pdf; National Insider Threat Task Force, *National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs*, National Counterintelligence and Security Center (Nov. 2012), https://www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf.

[8] GAO–13–187, *supra note* 1 at 10.

[9] Communications between Dept. of Homeland Sec. staff and S. Homeland Sec. & Governmental Affairs Comm. staff (Feb. 1, 2016).

[10] Press Release, SolarWinds Survey Investigates Insider Threats to Federal Cybersecurity, SolarWinds Worldwide, LLC (Jan. 26, 2015), *available at* http://www.solarwinds.com/company/newsroom/press_releases/threats_to_federal_cybersecurity.aspx.

[11] *Id.*

[12] Press Release, Consolidation and Modernization Chief Among Federal IT Security Concerns, SolarWinds Survey Discovers, SolarWinds Worldwide, LLC (Mar. 1, 2016), *available at* http://www.solarwinds.com/company/newsroom/press_releases/consolidation-and-modernization-chief-among-federal-it-security.aspx.

[13] *Id.*

(5,503 incidents) to FY 2014 (67,168 incidents): an overall increase of 1,121 percent.[14]

Unfortunately, technology alone is often incapable of detecting insider threats. Patricia Larsen, co-director of the National Insider Threat Task Force, recently attested to this stating, "[t]raining is a huge piece of this. No technology tool in the world is going to be your silver bullet."[15] In addition to requiring department-wide coordination on addressing insider threats, H.R. 3361 mandates employee education and training.

Through employee education and training, this act seeks to create a Federal workforce that is aware of the risks posed by insider threats, and qualified to detect and report suspicious activity among colleagues.

III. Legislative History

Representative Peter King, along with Representatives Lou Barletta, Daniel M. Donovan Jr., Brian Higgins, and John Katko, introduced H.R. 3361 on July 29, 2015, which was referred to the House Committee on Homeland Security. The House Committee on Homeland Security considered H.R. 3361 at a business meeting on November 2, 2015. On the same day, the bill passed the House by voice vote and under suspension of the rules.

The act was received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs on November 3, 2015. The Committee considered H.R. 3361 at a business meeting on February 10, 2016.

Chairman Ron Johnson offered a substitute amendment that required certain discipline of employees found to be insider threats as well as a modified technical amendment. The technical amendment replaced the term "adjudicatory authority" with "appropriate entity." Senator Claire McCaskill offered an amendment to clarify that nothing in this act would change existing whistleblower protections for Federal employees that are accused of being insider threats.

The Committee adopted both the Johnson amendments and the McCaskill amendment, and ordered the act, as amended, reported favorably, *en bloc* by voice vote. Senators present for the vote on the amendments and the vote on the amended act were: Johnson, McCain, Portman, Paul, Lankford, Ayotte, Ernst, Sasse, Carper, McCaskill, Tester, Baldwin, Heitkamp, Booker, and Peters.

IV. Section-by-Section Analysis of the Act, as Reported

Section 1. Short title

This section provides the act's short title, the "Department of Homeland Security Insider Threat and Mitigation Act of 2016."

Section 2. Establishment of the Insider Threat Program

This section establishes DHS's Insider Threat Program.

---

[14] *Is the OPM Data Breach the Tip of the Iceberg?: Joint Hearing Before the H. Subcomm. on Research and Tech. and the H. Subcomm. on Oversight of the H. Comm. on Science, Space, and Tech.*, 114th Cong. 7 (2015) (statement of Gregory Wilshusen, Director, Information Security Issues, U.S. Gov't Accountability Office).

[15] Calvin Hennick, *Commerce, State Departments Take Steps to Combat Insider Security Threats*, FEDTECH MAGAZINE (Apr. 25, 2016), *available at* http://www.fedtechmagazine.com/article/2016/04/commerce-state-departments-take-steps-combat-insider-security-threats.

Subsection (a) requires the Secretary of DHS to establish a robust, centralized ITP within the Department. The ITP shall provide Department employee training and education related to insider threats to the Department's critical assets, allow the Department to investigate such threats, and standardize risk mitigation of such threats.

Subsection (b) creates a Steering Committee to manage Department-wide activities related to insider threats to the Department's critical assets. This subsection further identifies the Steering Committee's membership, frequency of meetings, and responsibilities. Due to the multidisciplinary aspect of Department-wide assets, a successful DHS ITP must be led by professionals with not only counterintelligence but also law enforcement and investigation authorities. For this reason, the DHS Under Secretary for Intelligence and Analysis and Chief Security Officer shall serve as Chairperson and Vice Chairperson of the Steering Committee, respectively. This allows for longer retention of records against which system flags can be checked. The remaining members of the Steering Committee shall be comprised of representatives from other components or offices of the Department identified by the risk assessment as appropriate stakeholders. This ensures that components or offices with information, networks, or facilities at risk of insider threat activities participate in the program.

The Steering Committee shall meet on a regular basis to discuss cases and issues related to insider threats to the Department's critical assets. This subsection also identifies the Steering Committee's responsibilities.

Subsection (c) details the procedure to be followed when an insider threat is discovered. The head of an agency exploited by an insider threat is required to propose an adverse action against an employee engaged in insider misconduct that is not less than a 12-day suspension, with respect to the first instance; and removal, for any subsequent instance. That employee receives written notice and an opportunity to refute the accusation.

An employee can face multiple adverse actions for the same incident of insider misconduct if another provision of law applies.

Subsection (d) requires the Secretary of DHS to report to Congress on the status of Department-wide insider threat strategy implementation; the status of the Department's critical asset insider threat risk assessment; the types of training the Department conducts as part of the ITP; the number of Department employees trained through the ITP; and analysis determining whether the program effectively protects the Department's critical assets from insider threats.

Subsection (e) clarifies that the act does not change existing whistleblower protections for Federal employees that are accused of being insider threats.

Subsection (f) provides definitions for the following terms: "appropriate entity," "critical assets," "employee," "insider," "insider employee," "insider misconduct," "insider threat," and "steering committee."

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered

the regulatory impact of this act and determined that the act will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that H.R. 3361 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

MARCH 21, 2016.

Hon. RON JOHNSON,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3361, the Department of Homeland Security Insider Threat and Mitigation Act of 2016.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

KEITH HALL.

Enclosure.

H.R. 3361—Department of Homeland Security Insider Threat and Mitigation Act of 2016

H.R. 3361 would direct the Department of Homeland Security (DHS) to establish a program to protect the department's critical assets from insider threats (that is, harmful activities by department employees and certain other persons with access to classified information). DHS is currently carrying out activities similar to those required by the act; thus, CBO estimates that implementing H.R. 3361 would not significantly affect spending by DHS. Because enacting the legislation would not affect direct spending or revenues, pay-as-you-go procedures do not apply.

CBO estimates that enacting the legislation would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

H.R. 3361 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

On October 23, 2015, CBO transmitted a cost estimate for H.R. 3361, the Department of Homeland Security Insider Threat and Mitigation Act of 2015, as ordered reported by the House Committee on Homeland Security on September 30, 2015. The two versions of the act are similar and CBO's estimates of the budgetary effects are the same.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE ACT, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by H.R. 3361 as reported, are shown as follows (existing law proposed to be omitted

is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

Sec. 104. Insider Threat Program

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 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) 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).

* * * * * * *

○