114TH CONGRESS, 1st Session | HOUSE OF REPRESENTATIVES | REPORT 114–321

DEPARTMENT OF HOMELAND SECURITY INSIDER THREAT AND MITIGATION ACT OF 2015

NOVEMBER 2, 2015.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Committee on Homeland Security, submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 3361]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (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, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

59–006

The amendment is as follows:

Strike out all after the enacting clause and insert the following:

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 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) REPORT.—Not later than two years after the date of the enactment of this section and the biennially thereafter for the next four 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 imple-

mented 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 inserting after the item relating to section 103 the following new item:

"Sec. 104. Insider Threat Program.".

PURPOSE AND SUMMARY

The purpose of H.R. 3361, the "Department of Homeland Security Insider Threat and Mitigation Act" is to amend the Homeland Security Act of 2002 to establish an Insider Threat program at the Department of Homeland Security (DHS). The bill mandates employee education and training programs, and establishes an internal DHS Steering Committee to manage and coordinate DHS activities related to insider threat issues.

BACKGROUND AND NEED FOR LEGISLATION

Over the last six years several acts of espionage and workplace violence committed by U.S. government employees have caused grave damage to U.S. national security and taken American lives. U.S. Army PFC Bradley Manning provided thousands of classified government documents to WikiLeaks, which were subsequently published. Edward Snowden continues to hide from prosecution in Russia for stealing and later releasing classified information related to sensitive national security programs. Aaron Alexis, who held a Secret security clearance while working as a contractor at the Washington Navy Yard, killed 12 people during a rampage in 2013.

All three of these individuals were vetted, trusted U.S. security professionals who abused that trust and committed heinous acts. Furthermore, these events underscore the importance of identifying potential insider threats that could put Department and its employees at risk.

An official from the Office of Director of National Intelligence (ODNI) testified before this Subcommittee in 2013 that, "damage assessments regarding individuals involved in unauthorized disclosures of classified information or acts of workplace violence have uncovered information that was not discovered during the existing

security clearance process. Timely knowledge of such information might have prompted a security review or increased monitoring of the individual."[1] A recent survey of 150 Federal information technology managers, including those from the defense and intelligence communities, showed that 29 percent of the agencies had suffered a loss of data due to an insider over the last year.[2]

The Department of Homeland Security Insider Threat and Mitigation Act of 2015 establishes an Insider Threat program at DHS to provide a foundation for the Secretary to secure DHS facilities and its workforce. It creates a multidisciplinary steering committee to coordinate insider threat efforts across the Department by developing a holistic strategy for the Department to identify, prevent, mitigate and respond to insider threats to its critical assets.

In order for DHS to protect itself against two common threats—malicious insiders and external cybercriminals—it is important that the Department complete the process to identify and secure those critical assets and related infrastructure components that it depends on to fulfill its responsibility of ensuring homeland security and public safety, as well as the security of its workforce. This bill directs the Department to conduct a risk assessment of its critical assets which includes the Department's information, networks, facilities, and its workforce.

Insider threats are very difficult to discover through technology alone, and many leaks are unintentional in nature, therefore a key element of any insider threat program is training and employee awareness. Research at Carnegie Mellon University's Computer Emergency Response Teams has shown that most insider threats are first detected by other users who note and report something suspicious. Users need training and awareness to know what to look out for and to report it in the appropriate manner.[3] The bill requires both to ensure that personnel understand how their use of DHS networks will be monitored, as well as what workplace behavior may be indicative of a potential insider threat.

The bill ensures that insider threat best practices are standardized and implemented across the DHS enterprise, and that all relevant stakeholders who possess information pertinent to insider threat, have a seat at the table and contribute to the program's effectiveness.

Additionally, this bill provides the authorities and direction DHS needs to develop a robust, holistic insider threat program. The legislation focuses on: Building a proper governance structure; assessing the Department's critical assets so it can prioritize appropriately; and training the Department's workforce—three pillars of a successful insider threat program that seeks to protect the Department's workforce, its information, and its physical assets.

---

[1] Brian Prioletti, Assistant Director, Special Security Directorate, Office of National Counterintelligence Executive, Office of the Director for National Intelligence, Testimony before the Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, November 13, 2013.

[2] Aaron Boyd, "Survey: Insider threats target nearly half of agencies", C4ISR Networks, September 14, 2015, available at: *http://www.c4isrnet.com/story/military-tech/it/2015/09/14/us-government-insider-threats-survey/72254846/*.

[3] Jon Ramsey, "Empower Workers to Take Ownership of Cybersecurity", Dell.com, October 2, 2015, available at: *https://powermore.dell.com/technology/empower-workers-to-take-ownership-of-cybersecurity/*.

HEARINGS

The Committee did not hold any hearing specifically on H.R. 3361, however, the Committee did hold the following oversight hearing in the 113th Congress:

On November 13, 2013, the Subcommittee on Counterterrorism and Intelligence held a hearing entitled, "The Insider Threat to Homeland Security: Examining Our Nation's Security Clearances Processes." The Subcommittee received testimony from Mr. Merton W. Miller, Associate Director of Investigations, Federal Investigative Services, U.S. Office of Personnel Management; Mr. Gregory Marshall, Chief Security Officer, U.S. Department of Homeland Security; Mr. Brian Prioletti, Assistant Director, Special Security Directorate, National Counterintelligence Executive, Office of the Director of National Intelligence; Ms. Brenda Farrell, Director, Military and DOD Civilian Personnel Issues, U.S. Government Accountability Office.

COMMITTEE CONSIDERATION

The Committee met on September 30, 2015, to consider H.R. 3361, and ordered the measure to be reported to the House with a favorable recommendation, as amended, by voice vote. The Committee took the following actions:

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. KATKO listed on the roster as by MR. KING of New York (#1); was AGREED TO by voice vote.

The Subcommittee on Counterterrorism and Intelligence met on September 17, 2015, to consider H.R. 3361 and reported the measure to the Full Committee with a favorable recommendation, as amended, by voice vote.

The following amendment was offered:

An Amendment in the Nature of a Substitute offered by MR. KING of New York (#1); was AGREED TO by voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during the Committee consideration of H.R. 3361.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 3361, the Department of Homeland Security Insider Threat and Mitigation

Act of 2015, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 23, 2015.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security,
House of Representatives, 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 2015.

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 2015

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 bill, and 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 H.R. 3361 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2026.

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.

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

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3361 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

The goal of H.R. 3361 is to establish a Department-wide Insider Threat program at DHS that reports to the Secretary, and is managed by the Undersecretary for Intelligence and Analysis and the Chief Security Officer. H.R. 3361 ensures that a robust, standardized program is implemented across the Department and its Com-

ponent organizations by establishing a Steering Committee that consists of Department principals, who coordinate insider threat efforts across the Department and review insider threat cases and issues related to the Department's critical assets. The bill assigns a number of tasks to the Steering Committee including developing a comprehensive strategy to identify, prevent, mitigate, and respond to insider threat to the Department and its employees, and conducting a risk assessment of the Department's critical assets.

H.R. 3361 also requires the Secretary to report to Congress on the Department's insider threat strategy, the status of the Department's risk assessment of critical assets, training of Department employees and contractors, and information on the effectiveness of the program.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3361 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3361 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 3361 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or

accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that bill may be cited as the "Department of Homeland Security Insider Threat and Mitigation Act of 2015".

Sec. 2. Establishment of Insider Threat Program

This section amends Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) by adding the following new section:

"SEC. 104. INSIDER THREAT PROGRAM.

Section 104 directs the Secretary of Homeland Security to establish an insider threat program at the Department. The purpose of the program is to provide training and education to Department personnel regarding insider threats to the Department's critical assets, which include its people, facilities, and sensitive data; provide support to insider threat investigations that may pose a risk to the Department's critical assets; and conduct risk mitigation for potential insider threats.

The Committee believes that an insider threat program is necessary to standardize efforts Department-wide. The Committee is concerned that progress across the Department's component agencies has been uneven and requires more centralized coordination to ensure that all offices within the Department reach a baseline standard of effectiveness.

The Committee strongly believes that while insiders with malicious intent have caused the most serious damage to national security and American lives, most gaps that allow insiders to conduct their nefarious work are often caused by unwitting employees who are not properly trained. The purpose of this program is not only to identify and prevent insiders from damaging the United States, but also to spot individuals who may demonstrate tendencies of an insider threat, and intervene through contact with an investigator to mitigate the activity through education and increased awareness.

This section also creates a Steering Committee within the Department to coordinate insider threat efforts across the Department, and review insider threat cases and issues related to the Department's critical assets. The Steering Committee is chaired by the Under Secretary for Intelligence and Analysis, and the Chief Security Officer serves as the Vice-Chair. The Steering Committee's membership includes relevant stakeholders from across the Department and its component organizations that hold pertinent information to insider threats.

The Committee believes that a designated Steering Committee, chaired by the Under Secretary for Intelligence and Analysis, and the Chief Security Officer, with a mandate to develop, execute and manage the daily operations of the Department's Insider Threat program, will ensure that a comprehensive strategy is developed, and a thorough assessment of the Department's critical assets is conducted. The Committee also believes that the Steering Committee should be responsible for issuing guidance and training re-

lated to insider threats Department-wide to ensure that all employees and contractors achieve a consistent-level of understanding and awareness about the program.

It is the Committee's intention that the membership of the Steering Committee includes all relevant stakeholders within the Department that possess information pertinent to operating an effective insider threat program. The Committee believes that adding members to the Steering Committee should be at the discretion of the Secretary as the Department's needs and resources evolve.

Additionally, this section defines the responsibilities for the Steering Committee, including to: (A) Develop a holistic strategy for the Department to identify, prevent, mitigate and respond to insider threats to its critical assets; (B) develop a plan to implement the strategy across the component organizations and offices of the Department; (C) document insider threat policies; (D) conduct a baseline risk assessment of insider threats posed to the Department's critical assets; (E) leverage best practices and technology from across the Federal Government, industry, and the research community to implement insider threat solutions that are validated and cost-effective; (F) develop a timeline for deploying workplace monitoring technologies, awareness campaigns, and insider threat training; (G) consult with the Under Secretary of Science and Technology to stay current on insider threats, best practices and technology related to insider threats; and (H) develop and report on metrics that indicate the effectiveness of the program.

In addition to the Department's networks, information and technology, the Committee believes that the Department's critical assets include its workforce and physical assets. It is important that the Department consider all its assets when conducting its risk assessment so that it can prioritize and allocate resources accordingly.

As part of leveraging best practices and technology, the Committee notes that according to a survey of Federal IT managers, more than 40 percent of Federal agencies don't track data assets on their networks, and therefore they cannot be sure when and how specific documents are shared or otherwise exfiltrated.[4] The Committee remains concerned that DHS' inability to track sensitive documents could allow it to be victimized by a malicious insider and suffer damage similar in scale to WikiLeaks or the Snowden crime. The Committee strongly recommends that DHS develop a plan to secure its proprietary content and documents so that it can monitor the Department's most sensitive digital content, personally identifiable information (PII) and classified information at all times while in transit on a network, and in storage.

Furthermore, this section requires the Secretary to submit a report to Congress no later than two years after the date of enactment that describes how the Department and its components have implemented the insider threat strategy, the status of the Department's risk assessment of critical assets, training that has been provided to Department employees, and information on the effectiveness of the program.

---

[4] Aaron Boyd, "Survey: Insider threats target nearly half of agencies", C4ISR Networks, September 14, 2015, available at: *http://www.c4isrnet.com/story/military-tech/it/2015/09/14/us-government-insider-threats-survey/72254846/*.

The Committee believes that the required report in this subsection will assist the Department in articulating its insider threat strategy, how it intends to increase awareness of the problem and train employees on how to identify and report signs of an insider threat, and collect data that will help it evaluate the effectiveness of the program as a whole.

Finally, this section provides for definitions used in this section including: "critical assets," "insider," and "insider threat."

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

Sec. 104. Insider Threat Program.

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

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) REPORT.—Not later than two years after the date of the enactment of this section and the biennially thereafter for the next four 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.

* * * * * * *

DISSENTING VIEWS

Though I am supportive of the insider threat program that is currently in operation at the Department of Homeland Security (DHS), I reluctantly voted "no" when H.R. 3361 was considered on September 30th by the Full Committee. At the time, I expressed disappointment that the Majority would not agree to clarify that H.R. 3361 authorizes the current DHS insider threat program and does not authorize the establishment of a continuous evaluation program that subjects certain personnel to ongoing automated credit, criminal, and social media monitoring.

DHS' current insider threat program is properly targeted at preventing and detecting when a person with authorized access to U.S. Government resources, to include personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States. In response to high profile incidents involving the misappropriation of classified and sensitive material by Edward Snowden and Bradley Manning, Federal agencies have, increasingly, sought to establish continuous evaluation programs to monitor personnel with security clearances or in positions of trust on an ongoing basis through automated systems. The Department of Defense, in particular, has pursued this capability and is currently gathering credit, financial, travel information as well as criminal records from both public and private databases, including social media, for more than 100,000 individuals who are eligible for access to classified information. While I appreciate that the standard periods for recurrent checks may need to be adjusted to enhance detection of potential issues, it is incumbent upon Congress to ensure that any adjustments to the longstanding security clearance system be transparent and effective, with minimum disruption to the important work undertaking by the Federal workforce.

I strongly believe that, as authorizers, we have a responsibility, to have an open conversation with the Department about the potential costs, both financial and to the stability of the security-cleared workforce, as well as the potential benefits of erecting such a system prior to authorizing DHS to move forward with it.

Unfortunately, without clarifying language, H.R. 3361 could be interpreted to authorize DHS to move forward with a continuous evaluation program without our Committee setting forth our expectations are for such a system.

For these reasons, I reluctantly oppose H.R. 3361.

BENNIE G. THOMPSON.

○