Moira Bergin, of the Committee's minority staff, both of whom worked closely with Lillie Coney on my staff on the FRIENDS Act.

I also thank the staff of the Committee on Transportation and Infrastructure for their efforts to bring the bill before the full House for consideration.

I ask all Members to join me in voting to pass H.R. 58, the FRIENDS Act.

Mr. JOHNSON of Georgia. Mr. Speaker, I yield back the balance of my time.

Mr. BARLETTA. Mr. Speaker, I again urge my colleagues to vote ''yes'' on H.R. 58, as amended, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Pennsylvania (Mr. BARLETTA) that the House suspend the rules and pass the bill, H.R. 58, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

DEPARTMENT OF HOMELAND SECURITY INSIDER THREAT AND MITIGATION ACT OF 2017

Mr. KING of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 666) to amend the Homeland Security Act of 2002 to establish the Insider Threat Program, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 666

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Department of Homeland Security Insider Threat and Mitigation Act of 2017''.

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) 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) REPORTING.—

(1) IN GENERAL.—Not later than two years after the date of the enactment of section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) and the biennially thereafter for the next four years, the Secretary of Homeland Security 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 of Homeland Security and its components and offices have implemented the strategy developed pursuant to subsection (b)(2)(A) of such section 104, 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 (established pursuant to subsection (a) of such section 104), based on metrics developed, collected, and reported pursuant to subsection (b)(2)(H) of such section 104.

(2) DEFINITIONS.—In this subsection, the terms ''critical assets'', ''insider'', and ''insider threat'' have the meanings given such terms in section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section).

(c) 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.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. KING) and the gentleman from Mississippi (Mr. THOMPSON) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. KING of New York. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days within which to revise and extend their remarks and include any extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from New York?

There was no objection.

Mr. KING of New York. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in strong support of the legislation. Recent high-profile cases of government employees leaking classified information have caused drastic damage to U.S. national security and diplomacy. The names Snowden and Manning are now synonymous with the term ''insider threat.'' Unfortunately, Snowden, Manning, and others were able to conduct their traitorous work undetected because the government had at one time vetted and granted them access to secure facilities and information systems.

In response to these cases, it is vital that Congress ensure Federal agencies have the tools to detect and disrupt future insider threat situations before damage is done. H.R. 666, in contrast to its unholy numbering, has the important and respectable goal of authorizing and expanding insider threat detection and mitigation efforts at the Department of Homeland Security.

DHS has over 115,000 employees with access to classified information and many more with access to law enforcement sensitive data. Unauthorized disclosures of classified information, whether deliberate or unwitting, represent a significant threat to national security. The very nature of modern communication systems, as well as DHS' important information-sharing role with State and local partners, adds complexity to the challenge and requires thoughtful programs to educate employees and enhance DHS-wide detection capabilities.

The bill directs DHS to develop a strategy for the Department to identify, prevent, mitigate, and respond to insider threats and requires DHS to ensure that personnel understand what workplace behavior may be indicative of a potential insider threat and how their activity on DHS networks will be monitored. The bill codifies a comprehensive insider threat program at DHS that can be implemented through the Department and its component agencies and, most importantly, reinforces the importance of preventing future insider attacks.

I want to thank Homeland Security Chairman MCCAUL, Ranking Member THOMPSON, and Congressmen DAN DONOVAN and LOU BARLETTA for working with me to bring this bill to the floor.

The same bill passed the House floor in November 2015 by voice vote. Unfortunately, last-minute scheduling issues with the Senate prevented the bill from reaching the President's desk. I am pleased that the House is willing to take up this measure so quickly in the new Congress so we can move it through the process. I look forward to working with the Senate to move this measure forward.

I urge my colleagues to support this bill so we can establish a comprehensive, transparent, DHS-wide insider threat program. I urge support for the bill.

Mr. Speaker, I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 666, the Department of Homeland Security Insider Threat and Mitigation Act of 2017. H.R. 666, the Department of Homeland Security Insider Threat and Mitigation Act of 2017, authorizes the Department of Homeland Security to address the homeland and national security risk posed by trusted insiders.

Typically, trusted insiders are given unrestricted access to mission-critical assets such as personnel, facilities, and computer networks. While DHS, like other Federal agencies, conducts extensive vetting of prospective employees, there is a risk that someone with insider status exploits their position to damage the United States through espionage, terrorism, or the unauthorized disclosure of sensitive national security information.

As the ranking member of the Committee on Homeland Security, I am supportive of the Department of Homeland Security's current Insider Threat Program. It is targeted at preventing and detecting when a vetted DHS employee or contractor with access to U.S. Government resources, including personnel, facilities, information, equipment, networks, and systems, exploits such access for nefarious, terroristic, or criminal purposes.

□ 1430

Though I support the DHS program, I do have some concerns about DHS and other Federal agencies deploying continuous evaluation programs without transparency and congressional oversight. I am concerned that Federal agencies, with the understandable urge to protect their IT systems and facilities, are racing to acquire the capability before knowing whether such costly systems are even effective.

Therefore, I would like to reiterate to this Congress, as I did last Congress, that prior to establishing any such program, under which certain DHS employees would be subjected to ongoing automated credit, criminal, and social media monitoring, the Department engage Congress about not only the potential costs and benefits of such a program but what protections would be in place for workers subject to such a program.

Mr. Speaker, we live at a time when the threats to our Nation are complex. When this bill was considered last Congress, the prospect that a foreign intelligence agency would carry out an espionage campaign to influence the outcome of our Presidential election was material for the movies or for a good spy thriller. Today, in light of the Russian Government's actions in the 2016 elections, we have a greater appreciation for the importance of counterintelligence efforts. As such, this bill is particularly timely. None of us wants to see someone exploit their access to DHS networks to carry out cybercrimes or other criminal activity.

Even as DHS works to detect and prevent such threats, it is important that such activities be carried out in a transparent way so as not to compound the chronic morale challenges that exist within its workforce. Each time DHS considers making an adjustment to its insider threat program, thoughtful consideration must be paid to whether the operational drawbacks and costs for such an adjustment outweigh the benefits of such a change.

That said, I commend General TAYLOR, the previous Under Secretary for Intelligence and Analysis at DHS, for the attention he gave to the insider threat challenge. I look forward to continuing to work with the Department's successor to bolster security within the Department.

I would also like to give Mr. KING particular credit for his interest in this effort to make sure that problems don't come from the inside if we can help it.

With that, Mr. Speaker, I urge passage of H.R. 666.

I yield back the balance of my time.

Mr. KING of New York. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, at the outset, let me thank the ranking member for his support and for his kind words, and let me fully agree with him on the outstanding job General TAYLOR did during his time at DHS and throughout his career in public service.

Mr. Speaker, on a daily basis, adversaries are targeting DHS and other Federal agencies seeking to acquire sensitive information. U.S. citizens with trusted access to government facilities and electronic networks have been responsible for some of the most damaging attacks to the U.S. Government.

This bill provides the framework for DHS to implement an insider threat program that identifies and disrupts malicious insiders who seek to do the Department and its employees harm. It also seeks to protect the Department's workforce by conducting a transparent process to reinforce cyber hygiene, data security, and an awareness of malicious activity through a robust training program.

Mr. Speaker, I urge my colleagues to vote for this bill, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. KING) that the House suspend the rules and pass the bill, H.R. 666.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

DEPARTMENT OF HOMELAND SECURITY CLEARANCE MANAGEMENT AND ADMINISTRATION ACT

Mr. KING of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 697) to amend the Homeland Security Act of 2002 to improve the management and administration of the security clearance processes throughout the Department of Homeland Security, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 697

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Department of Homeland Security Clearance Management and Administration Act''.

SEC. 2. SECURITY CLEARANCE MANAGEMENT AND ADMINISTRATION.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 is amended—

(1) by inserting before section 701 (6 U.S.C. 341) the following:

''Subtitle A—Headquarters Activities'';

and