NOTIFICATION OF INTENT TO TERMINATE THE DESIGNATION OF THE REPUBLIC OF BURUNDI AS A BENEFICIARY SUB-SAHARAN AFRICAN COUNTRY UNDER AGOA—MESSAGE FROM THE PRESIDENT OF THE UNITED STATES (H. DOC. NO. 114–72)

The SPEAKER pro tempore laid before the House the following message from the President of the United States; which was read and referred to the Committee on Ways and Means and ordered to be printed:

To the Congress of the United States:

In accordance with section 506A(a)(3)(B) of the African Growth and Opportunity Act, as amended (AGOA) (19 U.S.C. 2466a(a)(3)(B)), I am providing notification of my intent to terminate the designation of the Republic of Burundi (Burundi) as a beneficiary sub-Saharan African country under AGOA.

I am taking this step because I have determined that the Government of Burundi has not established or is not making continual progress toward establishing the rule of law and political pluralism, as required by the AGOA eligibility requirements outlined in section 104 of the AGOA (19 U.S.C. 3703). In particular, the continuing crackdown on opposition members, which has included assassinations, extra-judicial killings, arbitrary arrests, and torture, have worsened significantly during the election campaign that returned President Nkurunziza to power earlier this year. In addition, the Government of Burundi has blocked opposing parties from holding organizational meetings and campaigning throughout the electoral process. Police and armed youth militias with links to the ruling party have intimidated the opposition, contributing to nearly 200,000 refugees fleeing the country since April 2015. Accordingly, I intend to terminate the designation of Burundi as a beneficiary sub-Saharan African country under AGOA as of January 1, 2016.

BARACK OBAMA.

THE WHITE HOUSE, *October 30, 2015.*

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 4 of rule I, the following enrolled bills were signed by Speaker pro tempore MESSER on Monday, November 2, 2015:

H.R. 623, to amend the Homeland Security Act of 2002 to authorize the Department of Homeland Security to establish a social media working group, and for other purposes;

H.R. 1314, to amend the Internal Revenue Code of 1986 to provide for a right to an administrative appeal relating to adverse determinations of tax-exempt status of certain organizations.

RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair declares the House in recess until approximately 4 p.m. today.

Accordingly (at 2 o'clock and 11 minutes p.m.), the House stood in recess.

□ 1607

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. HOLDING) at 4 o'clock and 7 minutes p.m.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which a recorded vote or the yeas and nays are ordered, or on which the vote incurs objection under clause 6 of rule XX.

Record votes on postponed questions will be taken later.

DEPARTMENT OF HOMELAND SECURITY INSIDER THREAT AND MITIGATION ACT OF 2015

Mr. KING of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3361) to amend the Homeland Security Act of 2002 to establish the Insider Threat Program, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3361

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 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 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.''.

(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.''.

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 support of this legislation. The bill under consideration ensures that the Department of Homeland Security has the authority and congressional mandate to create a robust Insider Threat Program.

In the Manning and Snowden espionage scandals, two trusted insiders abused their access to classified information. When Aaron Alexis attacked the Washington Navy Yard, 12 Americans lost their lives. In the face of these insider threat scenarios, it is vital that government agencies have the tools to detect and disrupt future insider threat situations before damage is done. Unfortunately, all three 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.

H.R. 3361 reinforces the message that a security clearance is a privilege granted to individuals who have pledged to protect the American people from threats domestically and abroad. Had investigators more thoroughly scrutinized Edward Snowden's background, they might have identified disturbing trends that made him unfit to hold a clearance of any kind and a potential insider threat to U.S. national security. Had Federal adjudicators had access to criminal history records from the Seattle Police Department, they would have been aware of Aaron Alexis' arrest in 2004 on firearms charges and potentially conducted a more rigorous screening of his background prior to authorizing him access to the Washington Navy Yard.

Trusted insiders, going back to Aldrich Ames and Robert Hanssen, not only severely damaged national security, their traitorous actions led to the loss of life. In each case, the post-breach review highlighted that the previously trusted individual exhibited suspicious behavior, but it was not reported due to a lack of understanding by colleagues or failures in the reinvestigation process.

In describing the new type of insider threat represented by Snowden and WikiLeaks, Michael Hayden correctly concluded that, ''in this new, modern, connected era, the trusted insider who betrays us is far more empowered to do damage far greater than these kinds of people were able to do in the past. And therefore we have to be even more vigilant.''

The Department of Homeland Security has over 280,000 employees, including tens of thousands with access to classified or sensitive information. The Department has an existing Insider Threat Program and is moving forward to increase security controls on internal systems, but much more remains to be done.

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 throughout 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, Ranking Member HIGGINS, and Congressmen KATKO, DONOVAN, and BARLETTA for working with me to bring this bill to the floor. The bill went through regular order and received bipartisan support during subcommittee and full committee consideration.

I urge my colleagues to support this bill so we can establish a comprehensive, transparent DHS-wide Insider Threat Program that is a model for the public and private sectors.

I reserve the balance of my time.

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

I rise in support of H.R. 3361, the Department of Homeland Security Insider Threat and Mitigation Act of 2015.

Mr. Speaker, H.R. 3361, the Department of Homeland Security Insider Threat and Mitigation Act of 2015, 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 remains a risk that someone who gains ''insider status'' exploits their position to damage the United States through espionage, terrorism, or even 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 authorized access to U.S. Government resources, including personnel, facilities, information, equipment, networks, and systems, exploits such access for nefarious, terroristic, or criminal purposes.

While I support the DHS program, I could not support this legislation when it was considered by the full committee because it did not include language to prevent the somewhat broad authority granted under this bill for being used by DHS to deploy ''continuous evaluation.'' Continuous evaluation is an automated system that constantly monitors public and private databases for information regarding the credit, criminal, and social media activities of certain individuals. The Defense Department has an extensive pilot underway, and I am concerned that Federal agencies, with the understandable urge to protect their IT systems and facilities, are racing to acquire this capability before knowing whether such costly systems are even effective.

At this time, I would like to engage in a colloquy with the gentleman from New York (Mr. KING) about some concerns I have with the prospect that the Department will use the authority under this act to establish a continuous evaluation program.

□ 1615

Would the gentleman agree that it is important that, prior to establishing any such program under which certain DHS employees would be subjected to ongoing automated credit, criminal, or social media monitoring, the Department engages 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 program?

I yield to the gentleman from New York (Mr. KING).

Mr. KING of New York. I thank the gentleman for yielding.

Yes, I agree with the gentleman from Mississippi. The implementation of the Insider Threat Program, including a possible continuous evaluation component, needs congressional oversight and must be transparent.

I look forward to working with the gentleman from Mississippi on this issue as we go forward.

Mr. THOMPSON of Mississippi. I thank the gentleman.

Mr. Speaker, we live at a time when the threats to our Nation are complex. None of us want 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 the 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 of such an adjustment outweigh the benefit of such change.

That said, I commend General Taylor, the Under Secretary for Intelligence and Analysis at DHS, for the attention he has given to the insider threat challenge and look forward to continuing to work with him to bolster security within the Department.

I appreciate the gentleman from New York's cooperation and colloquy. I look forward to the successful passage and approval of this bill.

Mr. Speaker, 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, let me also at the outset thank the distinguished ranking member for his support and his cooperation as this bill has gone forward. I am sure the two of us will be able to continue to work and cooperate as, again, this will be monitored in the future.

The Department of Homeland Security and all Federal agencies are targeted by adversaries on a daily basis. Some of the most damaging attacks to the U.S. Government have been committed by U.S. citizens who have been granted access to government facilities and electronic networks.

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 awareness of malicious activity through a robust training program.

I want to thank the committee staff, especially John Neal and Tyler Lowe.

I urge my colleagues to vote for H.R. 3361.

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

Ms. JACKSON LEE. Mr. Speaker, as a senior member of the Homeland Security Committee, I rise in support of H.R. 3361, the ''Department of Homeland Security Insider Threat and Mitigation Act.''

I am in support of this bill because it amends the Homeland Security Act of 2002 to direct the Department of Homeland Security (DHS) to establish an Insider Threat Program, which shall: provide training and education for DHS personnel to identify, prevent, mitigate, and respond to insider threat risks to DHS's critical assets; provide investigative support regarding such threats; and conduct risk mitigation activities for such threats.

The Department of Homeland Security will establish a Steering Committee headed by the Under Secretary for Intelligence and Analysis who will serve as the Chair; and the Chief Security Officer of the office as the Vice Chair of the Committee.

The Under Secretary and the Chief Security Officer, in coordination with the Steering Committee, shall: develop a holistic strategy for DHS-wide efforts to identify, prevent, mitigate, and respond to insider threats to DHS's critical assets; develop a plan to implement the strategy across DHS components and offices; document insider threat policies and controls; conduct a baseline risk assessment of such threats; examine existing programmatic and technology best practices adopted by the federal government, industry, and research institutions; develop a timeline for deploying workplace monitoring technologies, employee awareness campaigns, and education and training programs related to potential insider threats; consult with the Under Secretary for Science and Technology and other stakeholders to ensure that the Insider Threat Program is informed by current information regarding threats, best practices, and available technology; and develop, collect, and report metrics on the effectiveness of DHS's insider threat mitigation efforts.

Threat mitigation is focused on blunting the effectiveness of threats posed by terrorists seeking to carry out attacks in the United States.

This is a core mission of the Department of Homeland Security and this bill will support that mission.

I ask my colleagues to join me in support of this bill.

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. 3361, 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 CLEARANCE MANAGEMENT AND ADMINISTRATION ACT

Mr. KING of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3505) 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. 3505

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

(2) by adding at the end the following new subtitle:

''Subtitle B—Security Clearances

''SEC. 711. DESIGNATION OF NATIONAL SECURITY SENSITIVE AND PUBLIC TRUST POSITIONS.

''(a) IN GENERAL.—The Secretary shall require the designation of the sensitivity level of national security positions (pursuant to part 1400 of title 5, Code of Federal Regulations, or similar successor regulation) be conducted in a consistent manner with respect to all components and offices of the Department, and consistent with Federal guidelines.

''(b) IMPLEMENTATION.—In carrying out subsection (a), the Secretary shall require the utilization of uniform designation tools throughout the Department and provide training to appropriate staff of the Department on such utilization. Such training shall include guidance on factors for determining eligibility for access to classified information and eligibility to hold a national security position.

''SEC. 712. REVIEW OF POSITION DESIGNATIONS.

''(a) IN GENERAL.—Not later than July 6, 2017, and every five years thereafter, the Secretary shall review all sensitivity level designations of national security positions (pursuant to part 1400 of title 5, Code of Federal Regulations, or similar successor regulation) at the Department.

''(b) DETERMINATION.—If during the course of a review required under subsection (a), the Secretary determines that a change in the sensitivity level of a position that affects the need for an individual to obtain access to classified information is warranted, such access shall be administratively adjusted and an appropriate level periodic reinvestigation completed, as necessary.

''(c) CONGRESSIONAL REPORTING.—Upon completion of each review required under subsection (a), the Secretary shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the findings of each such review, including the number of positions by classification level and by component and office of the Department in which the Secretary made a determination in accordance with subsection (b) to—

''(1) require access to classified information;

''(2) no longer require access to classified information; or

''(3) otherwise require a different level of access to classified information.

''SEC. 713. AUDITS.

''Beginning not later than 180 days after the date of the enactment of this section, the Inspector General of the Department shall conduct regular audits of compliance of the Department with part 1400 of title 5, Code of Federal Regulations, or similar successor regulation.

''SEC. 714. REPORTING.

''(a) IN GENERAL.—The Secretary shall annually through fiscal year 2021 submit to the