Pope Francis charged with those listening to his remarks of the important responsibility of safeguarding religious freedom. He stated at the White House that that freedom remains one of America's most precious possessions. Of course, that freedom is not only an American possession, and it is not only enjoyed by certain religions. That freedom flows from the inherent dignity of every human person and should be protected wherever it is threatened.

The United States Commission on International Religious Freedom remains a strong, independent, and authoritative voice on behalf of religious believers everywhere. This measure will ensure that it continues to pursue the Commission's nonpartisan mission of promoting around the world the right of religious liberty that we hold so dear as a nation. It deserves our unanimous support.

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

Mr. HULTGREN. Mr. Speaker, I rise today to support a commission which embodies the highest of our democratic principles: independence, bipartisanship, transparency and the defense of our fundamental freedoms.

The United States Commission on International Religious Freedom was created from a landmark piece of legislation, the 1998 International Religious Freedom Act (IRFA).

How that bill came about is a story in its own right, and a demonstration of how a diverse set of our nation's leaders can come together to protect a foundational freedom.

One of the best ways to expose attacks on religious freedom is meticulous chronicling of such abuses and then proclaiming them loud and clear to a watching world.

The importance of USCIRF's mission of monitoring, recording and publishing attacks on religious belief—or any belief at all—cannot be overestimated.

Their annual report is an invaluable reference for my colleagues and me and our staffs.

Like the TIP report which monitors countries' records on human trafficking, the USCIRF annual report exposes lawbreakers and violators of human rights—and recommends what actions should be taken.

And we have seen how across the world religious minorities are under attack.

Christians made up 20 percent of the Middle East population at the start of the 20th century.

Given a sustained attack in recent years on Christian belief and practice, that number is now around 5 percent and declining.

In fact, less than 1 percent of the world's more than 2 billion Christians live in the Middle East—the birthplace of the religion.

Other religions and belief systems have suffered under sustained persecution.

Yazidis in Iraq and Syria have been systematically targeted by ISIS for slavery and execution.

Just this week, news reports have revealed Yazidi women have taken their own lives out of despair after repeated rapes and assaults.

USCIRF has documented ethnic cleansing of Muslims and sectarian violence in the Central African Republic, and urged the State Department designate it as a Country of Particular Concern.

In Russia, "serious violations of freedom of religion or belief continue."

China has taken further steps to "consolidate" its "authoritarian monopoly" over the lives of its citizens.

This has led to "unprecedented violence" against Uigher Muslims, Tibetan Buddhists, Catholics, Protestants, and Falun Gong practitioners.

And the list goes on and on.

An attack on the religious belief of one is an attack on all of us.

USCIRF is a unique, independent voice calling the world to pay attention and act, especially when this freedom can take a backseat in foreign affairs.

The world forgets that the chilling of religious belief is the first step toward totalitarian control over all areas of life.

All other freedoms flow from religious liberty.

Without the freedom to believe what your conscience tells you, and live that belief out without fear of violence or other persecution, all other freedoms are meaningless.

USCIRF recognizes this reality, and acts in defense of all peoples everywhere.

I urge the House and reauthorize this important commission, and continue to defend and promote our First Amendment freedoms around the world.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. ROYCE) that the House suspend the rules and pass the bill, S. 2078.

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.

AIRPORT ACCESS CONTROL SECURITY IMPROVEMENT ACT OF 2015

Mr. KATKO. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3102) to amend the Homeland Security Act of 2002 to reform programs of the Transportation Security Administration, streamline transportation security regulations, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3102

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 "Airport Access Control Security Improvement Act of 2015".

SEC. 2. AVIATION SECURITY.

(a) IN GENERAL.—Subtitle A of title XVI of the Homeland Security Act of 2002 is amended by adding at the end the following new section:

"SEC. 1602. RISK-BASED SCREENING OF EMPLOYEES AT AIRPORTS.

"(a) SCREENING MODEL.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Administrator shall establish a risk-based, intelligence-driven model for the screening of employees at airports based on level of access and employment positions at domestic airports. Such screening model shall—

"(A) ensure that only those individuals authorized to have access to the secure areas of a domestic airport are permitted such access;

"(B) ensure that an individual is immediately denied entry to a secure area when such individual's access authorization for such secure area is withdrawn; and

"(C) provide a means to differentiate between individuals authorized to have access to an entire secure area and individuals authorized access to only a particular portion of a secure area.

"(2) FACTORS.—The Administrator shall consider the following factors when establishing the screening model described in paragraph (1):

"(A) Whether and how often employees at airports require employment-related access to Secure Identification Display Areas, Airport Operations Areas, or secure areas.

"(B) The ability of each airport operator to reduce employee entry and exit points to a mutually agreed upon minimum number of such entry and exit points necessary to maintain airport operations.

"(C) In consultation with airport operators, the ability of the Administration to create a randomization plan for screening at the defined operational minimum entry and exit points at airports which maximizes the deterrent effect of screening efforts.

"(b) DISQUALIFYING OFFENSES.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Administrator, in consultation with the Director of the Federal Bureau of Investigation, labor organizations representing aviation, ground, and cabin crew workers, and the Aviation Security Advisory Committee, shall conduct an aviation security risk-based review of the disqualifying criminal offenses codified in sections 1542.209 and 1544.229 of title 49, Code of Federal Regulations, to determine the appropriateness of such offenses as a basis for denying to an employee a credential that allows unescorted access to Secure Identification Display Areas of airports. Such review shall consider the following:

"(A) The adequacy of codified disqualifying offenses to address the current aviation security threat environment, particularly the terrorism insider threat.

"(B) If such codified disqualifying offenses should be tailored to address the current aviation security threat environment, particularly the terrorism insider threat, by excluding or including other offenses.

"(C) The potential security benefits, drawbacks, and challenges associated with identifying patterns of misdemeanors or of other non-disqualifying offenses that could jeopardize aviation security.

"(D) The feasibility of integrating similar departmental eligibility requirements for access to Secure Identification Display Areas of airports.

"(E) If the ten year look-back period for disqualifying offenses is appropriate, in light of the current aviation security threat environment, particularly the terrorism insider threat.

"(2) WAIVER.—Not later than 180 days after the date of the enactment of this section, the Administrator shall provide an adequate redress process for an employee who is subject to an adverse employment decision, including removal or suspension of such employee, due to a disqualifying offense referred to in paragraph (1), that is consistent with the appeals and waiver process established for applicants for commercial motor vehicle hazardous materials endorsements and transportation workers at ports under section 70105(c) of title 46, United States Code.

"(3) NOTICE.—Any changes to the Secure Identification Display area badge program,

such as changes considered pursuant to subparagraphs (B), (C), (D), and (E) of paragraph (1) shall be subject to notice of proposed rulemaking.

''(4) BRIEFING TO CONGRESS.—Upon completion of the aviation security risk-based review required under paragraph (1), the Administrator shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on the results of such review.

''(c) CREDENTIALING.—Not later than 120 days after the date of the enactment of this section, the Administrator, in consultation with the Aviation Security Advisory Committee, shall review the auditing procedures for all airport-issued identification media. Such review shall determine the following:

''(1) The efficacy of the auditing program requirements at domestic airports to ensure the integrity, accountability, and control of airport-issued identification media.

''(2) The feasibility of including biometrics standards for all airport-issued identification media used for identity verification and badge verification.

''(3) The feasibility of integrating other departmental programs' eligibility requirements for access to secure areas of airports.

''(d) VETTING.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Administrator shall—

''(A) establish a program to allow airport badging offices to utilize the employment eligibility confirmation system established under section 404 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1324a note; commonly referred to as 'E-Verify') to determine the eligibility to work in the United States of all applicants seeking access to secure areas of airports;

''(B) establish a process to transmit applicants' biometric fingerprint data to the Office of Biometric Identity Management's (OBIM's) Automated Biometrics Identification System (IDENT) for vetting; and

''(C) conduct a data quality assessment to ensure that credential application data elements received by the Administration are complete and match the data submitted by the airport operators.

''(2) BRIEFING TO CONGRESS.—Upon completion of the responsibilities specified in paragraph (1), the Administrator shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on the results of such completion.

''(e) REPORTING OF VIOLATIONS.—Not later than 180 days after the date of the enactment of this section, the Administrator shall establish a nationwide program for the anonymous reporting of violations of airport security.

''(f) CENTRALIZED DATABASE.—Not later than 180 days after the date of the enactment of this section, the Administrator, in consultation with the Aviation Security Advisory Committee, shall—

''(1) establish a national database of employees who have had either their airport or aircraft operator-issued badge revoked for failure to comply with aviation security requirements;

''(2) determine the appropriate reporting mechanisms for airports and airlines to submit data regarding employees described in paragraph (1) and to access the database established pursuant to such paragraph; and

''(3) establish a process that allows individuals whose names were mistakenly entered into such database to have their names removed and have their credentialing restored.

''(g) UPDATED REVIEW.—Not later than April 8, 2016, the Administrator, in consultation with the Aviation Security Advisory Committee, shall conduct an updated and thorough review of airport access controls.

''(h) EMPLOYEE SCREENING STUDY.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Administrator, in consultation with the Aviation Security Advisory Committee, shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, and the Comptroller General of the United States a cost and feasibility study of a statistically significant number of Category I, II, and X airports, that ensures that all employee entry and exit points that lead to secure areas of such airports are comprised of the following:

''(A) A secure door utilizing card and pin entry or biometric technology.

''(B) Surveillance video recording, capable of storing video data for at least 30 days.

''(C) Advanced screening technologies, including at least one of the following:

''(i) Magnetometer (walk-through or handheld).

''(ii) Explosives detection canines.

''(iii) Explosives trace detection swabbing.

''(iv) Advanced imaging technology.

''(v) X-ray bag screening technology.

''(2) CONTENTS.—The study required under paragraph (1) shall include information related to the employee screening costs of those airports which have already implemented practices of screening one-hundred percent of employees entering secure areas of airports, including the following:

''(A) Costs associated with establishing an operational minimum number of employee entry and exit points.

''(B) A comparison of costs associated with implementing the requirements specified in paragraph (1), based on whether such implementation was carried out by the Administration or airports.

''(3) COMPTROLLER GENERAL ASSESSMENT.—

''(A) IN GENERAL.—Upon completion of the study required under paragraph (1), the Comptroller General of the United States shall review such study to assess the quality and reliability of such study.

''(B) ASSESSMENT.—Not later than 60 days after the receipt of the study required under paragraph (1), the Comptroller General of the United States shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on the results of the review required under subparagraph (A).''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 1601 the following new item:

''Sec. 1602. Risk-based screening of employees at airports.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. KATKO) and the gentleman from Louisiana (Mr. RICHMOND) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

□ 1715

GENERAL LEAVE

Mr. KATKO. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and to include 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. KATKO. Mr. Speaker, I yield myself such time as I may consume.

H.R. 3102 is a critically important, bipartisan piece of legislation, which serves as a culmination of months of intense oversight on the issue of airport access controls and the insider threat to aviation security.

The gaps in airport employee access control made headlines after an investigation revealed that aviation employees were trafficking weapons and ammunitions between Atlanta and New York. More than 170 guns were trafficked in such a manner.

Furthermore, a recent inspector general report found that TSA failed to identify 73 aviation workers with possible links to terrorism. Lastly, at airports such as Dallas/Fort Worth, Los Angeles International, and Oakland, many major drug-trafficking rings have been uncovered involving employees using their insider ability to access the airports.

It is the responsibility of this committee to act to prevent similar stories from continuing to emerge.

Specifically, H.R. 3102 requires TSA to consult with Federal and private sector partners to review existing employee screening protocols and work comprehensively to improve the effectiveness of controls at airports across the United States.

Moreover, the bill improves standards of vetting for the credentials granted to individuals with access to secure areas of airports and takes a robust approach to bolstering the oversight of the access given to these employees.

H.R. 3102 codifies a number of recommendations put forward by the Aviation Security Advisory Committee, which examined the issue of airport access controls earlier this year at our urging.

This legislation reflects rigorous oversight, including a number of hearings, site visits, and briefings from Homeland Security, TSA, the FBI, and aviation stakeholders.

Furthermore, I am very proud of the cooperation among our private sector stakeholders, Federal partners, and the labor community that has helped to bring this bill to the floor today.

Throughout this legislation's development, we have worked tirelessly with the same end goal in mind: to enhance the security of our Nation's airports and mitigate threats to aviation workers and the traveling public.

The insider threat to aviation is real, and it is critical that we evolve our security standards and best practices to stay abreast of changing threats to transportation.

I wish to thank Ranking Member RICE and Ranking Member THOMPSON

for their hard work and attention to this issue, as we have focused heavily on these problems in a bipartisan manner.

I also wish the thank the chairman of the full committee, Mr. MCCAUL, for his support on the committee's oversight efforts and for seeing this bill through the committee.

Together—together—we can fix these problems and assure the American public that their aviation system is secure and adaptive to changing threats.

I urge all Members to join me in supporting this bill.

I reserve the balance of my time.

Mr. RICHMOND. Mr. Speaker, I yield myself such time as I may consume.

I rise to speak in support of H.R. 3102.

Last year we learned that airport employees used their access to the secure areas of airports to bypass screening to smuggle weapons and drugs onto commercial flights.

In response, then-Acting Administrator Melvin Carraway requested that TSA's stakeholder advisory committee, the Aviation Security Advisory Committee, take on the challenge of evaluating airport access controls and come up with approaches to address security vulnerabilities.

In April, the ASAC issued a thoughtful report with 28 recommendations designated to mitigate threats and risks associated with airport access controls.

Congress approved legislation in December 2014 to codify ASAC in law in the hopes that it would result in better aviation security policymaking at TSA.

We envisioned a process in which various stakeholders throughout the aviation community were able to come together and address security issues affecting the industry. In this instance, the process worked as envisioned, and TSA is making sure and steady progress towards addressing many of the recommendations.

I believe that, by advancing this bill today, we will send a message to TSA and aviation stakeholders that we have a strong interest in raising the bar when it comes to securing our Nation's airports.

Mr. Speaker, in closing, I simply reiterate that the committee remains interested in raising the level of security within our Nation's airports. As such, we will continue to track TSA's efforts at bolstering access controls and addressing the ASAC's recommendations.

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

Mr. KATKO. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, the issues addressed in H.R. 3102 are a pressing concern to the security of our Nation's airports. It is critical that we send this bill to the Senate today. Congress cannot stand idly by and grant tacit approval to lax security standards for employees when we have the authority and responsibility to spur action and keep the traveling public safe from harm.

I want to thank Mr. RICHMOND for his bipartisan comments. That truly is the nature of what we have done today, is act in a bipartisan manner to attack a problem.

I urge my colleagues to support this bill.

I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, as a senior member of the Homeland Security Committee, I rise to speak on H.R. 3102, the "Airport Access Control Security Improvement Act of 2015," which amends the Homeland Security Act of 2002 to reform programs of the Transportation Security Administration, and streamline transportation security regulations.

The objective of the bill is to establish a risk-based, intelligence-driven model for the screening of employees at airports based on level of access and employment positions at domestic airports.

The model is intended to ensure that only those individuals authorized to have access to secure areas of a domestic airport are permitted such access.

The model must be able to differentiate between individuals authorized to have access to an entire secure area and those who are not permitted access.

The Director of the FBI and Director of the Aviation Security Advisory Committee are directed to review the disqualifying criminal offenses in the Code of Federal Regulations to determine the adequacy for an individual to have continued access to Secure Identification Display Areas of airports.

The review based on the current language of the bill would consider whether the list of disqualifying offenses should be amended to include other offenses.

As House Judiciary Committee's Ranking Member on the Subcommittee on Crime, Terrorism and Investigation, I am concerned that the bill contains this language.

At a time when we are discussing the rights of non-violent offenders to have an opportunity, if their conduct and records dictate to be able to fully reintegration into society, that there may be other efforts to make this process more difficult without a serious review of why such measures should be taken and for whom should they be applied?

I would offer to work with my fellow members on the House Committee on Homeland Security to consider carefully the reasons for any expansion on this list, especially if the expansion only involves the Department of Homeland Security.

There are similar concerns regarding language in the bill that may extend the period of time that may be considered between a particular situation and the life a person is currently leading.

Considering behavior of a teenager when considering the conduct of a 35 year-old adult, the weight of the consideration should be on the life of the adult and the seriousness of the offense.

Any new model that may be developed that would impact the employability of current persons who hold access credentials and future employees should be further reviewed by the full committee prior to becoming policy.

The bill's goals are important—the House should consider every aspect of airport security to improve aviation safety.

I will continue to work in my capacity on both the House Committee on Homeland Security and the House Committee on the Judiciary to improve aviation security.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. KATKO) that the House suspend the rules and pass the bill, H.R. 3102, 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 CYBERSECURITY STRATEGY ACT OF 2015

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3510) to amend the Homeland Security Act of 2002 to require the Secretary of Homeland Security to develop a cybersecurity strategy for the Department of Homeland Security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3510

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 Cybersecurity Strategy Act of 2015".

SEC. 2. CYBERSECURITY STRATEGY FOR THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

"SEC. 230. CYBERSECURITY STRATEGY.

"(a) IN GENERAL.—Not later than 60 days after the date of the enactment of this section, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in law.

"(b) CONTENTS.—The strategy required under subsection (a) shall include the following:

"(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

"(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs, policies, and activities in furtherance of the following:

"(A) Cybersecurity functions set forth in the second section 226 (relating to the national cybersecurity and communications integration center).

"(B) Cybersecurity investigations capabilities.

"(C) Cybersecurity research and development.

"(D) Engagement with international cybersecurity partners.

"(c) CONSIDERATIONS.—In developing the strategy required under subsection (a), the Secretary shall—

"(1) consider—

"(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

"(B) the Department of Homeland Security Fiscal Years 2014–2018 Strategic Plan; and

"(C) the most recent Quadrennial Homeland Security Review issued pursuant to section 707; and