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

''(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such strategy.

''(d) IMPLEMENTATION PLAN.—Not later than 90 days after the development of the strategy required under subsection (a), the Secretary shall issue an implementation plan for the strategy that includes the following:

''(1) Strategic objectives and corresponding tasks.

''(2) Projected timelines and costs for such tasks.

''(3) Metrics to evaluate performance of such tasks.

''(e) CONGRESSIONAL OVERSIGHT.—The Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate for assessment the following:

''(1) A copy of the strategy required under subsection (a) upon issuance.

''(2) A copy of the implementation plan required under subsection (d) upon issuance, together with detailed information on any associated legislative or budgetary proposals.

''(f) CLASSIFIED INFORMATION.—The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

''(g) RULE OF CONSTRUCTION.—Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

''(h) DEFINITIONS.—In this section:

''(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in the second section 226, relating to the national cybersecurity and communications integration center.

''(2) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

''(3) INCIDENT.—The term 'incident' has the meaning given such term in the second section 226, relating to the national cybersecurity and communications integration center.''.

(b) PROHIBITION ON REORGANIZATION.—The Secretary of Homeland Security may not change the location or reporting structure of the National Protection and Programs Directorate of the Department of Homeland Security, or the location or reporting structure of any office or component of the Directorate, unless the Secretary receives prior authorization from Congress permitting such change.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding at the end of the list of items for subtitle C of title II the following new item:

''Sec. 230. Cybersecurity strategy.''.

(d) AMENDMENT TO DEFINITION.—Paragraph (2) of subsection (a) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the national cybersecurity and communications integration center) is amended to read as follows:

''(2) the term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;''.

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

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. RATCLIFFE. 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 any extraneous material on the bill under consideration.

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

There was no objection.

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

Mr. Speaker, I rise today in support of H.R. 3510, the Department of Homeland Security Cybersecurity Strategy Act of 2015, sponsored by Representative CEDRIC RICHMOND, ranking member of the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee, of which I am the chairman.

This legislation would require the Department of Homeland Security to develop and to submit to Congress a cybersecurity strategy and implementation plan. Because the Department of Homeland Security is charged with securing the dot-gov domain and working with the private sector to secure the dot-com domain, a comprehensive strategic plan and implementation plan will support DHS' essential cybersecurity mission.

Mr. Speaker, too often these days cyber attacks disrupt the operations of government, of businesses, and of the lives of the American people. The increasingly sophisticated nature of the cyber threats we face on a daily basis underscore the need to manage and strengthen the cybersecurity of our Nation's critical infrastructure.

The Government Accountability Office has recommended the implementation of an overarching Federal cybersecurity strategy. H.R. 3510 is an important step toward accomplishing this task.

H.R. 3510 also precludes any reorganization effort of the Department of Homeland Security's National Protection and Programs Directorate, or NPPD, without congressional approval. This is an effort to ensure that congressional oversight is conducted.

Mr. Speaker, in June of this year, a story in the press announced that the NPPD was planning a significant reorganization. Since June, very few specifics have emerged, and even those that have have been very sparse in detail.

The details that have been made public elicit concern because they support overhauling the infrastructure protection and cybersecurity functions of the directorate without providing details on exactly what this would mean for the mission, for the structure, or for the workforce of the directorate.

The language in this bill follows a bipartisan letter sent just last month to the Department expressing congressional concern with the lack of transparency surrounding this proposed reorganization and communicating the congressional intent to provide oversight on this issue. The letter also clearly stated that any reorganization or realignment should require congressional authorization.

Over the past several years, the Committee on Homeland Security, on which I serve, has built up a collaborative working relationship with the NPPD, consulting with it to pass several strong and bipartisan pieces of legislation to improve chemical security and to strengthen DHS' cybersecurity mission and stature in the Federal Government.

Given our shared goal of protecting this country and the committee's continued legislative oversight efforts to strengthen DHS' cybersecurity functions, it is essential that the Department submit any proposal to Congress prior to reorganization or realignment.

It is Congress' role and responsibility to authorize the key responsibilities of the executive branch to include strengthening our cybersecurity posture and ensuring the security and resiliency of our Nation's critical infrastructure.

I would like to thank Mr. RICHMOND for the work that he and his staff have done to come together in a bipartisan way on this legislation.

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 in support of H.R. 3510.

Mr. Speaker, I want to thank the chairman of the subcommittee, Mr. RATCLIFFE. I want to thank the chairman of the full committee, Mr. MCCAUL, and the ranking member of the full committee, Mr. THOMPSON, who all signed on and support this legislation.

H.R. 3510, the Department of Homeland Security Cybersecurity Strategy Act of 2015, will require the Secretary of Homeland Security to develop a comprehensive strategy and implementation plan for carrying out its diverse and complex cyber and information security missions.

Today the Department of Homeland Security is not only responsible for working with Federal agencies to protect Federal civilian networks, but also for helping to bolster information security within the private sector, principally through the National Cybersecurity and Communications Integration Center.

It also plays a major role in information security research and development, cyber crime investigations, and international engagement with cybersecurity partners.

My bill requires DHS to put in place a strategy that includes necessary strategic and operational goals for executing the Secretary's broad responsibilities.

In September, the inspector general issued a report highlighting the need for such strategy. The report, entitled ''DHS Can Strengthen Its Cyber Mission Coordination Efforts,'' found that intradepartmental coordination was lacking and recommended that the Department develop a comprehensive cross-departmental strategic implementation plan that defines each component's cyber missions and responsibilities.

The Department operates frontline programs that protect this Nation from manmade and natural disasters. With cyber threats increasingly at the forefront today, it is essential that all of the Department's day-to-day programs, policies, and activities are effective and meeting its multi-layered cybersecurity responsibilities.

As the lead Federal agency responsible for securing Federal civilian networks and as the vital cyber information-sharing partner to national critical infrastructures, it is crucial that the Department have a comprehensive and achievable strategic plan in place.

Mr. Speaker, in recent years, Congress has provided significant resources to the Department to expand its cyber operations and workforce.

A lot of money has been spent to respond to cyber events and persistent information security threats. We must make sure our investments in operational plans and research and development are technically achievable and transparent where they can be.

Fundamentally, my bill seeks to ensure that the Department takes a measurable, strategic posture that can be a model for others and to help protect our Nation's vulnerable information security networks.

I ask for my colleagues' support.

I yield back the balance of my time.

□ 1730

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

Mr. Speaker, I once again urge my colleagues to support H.R. 3510.

I thank Congressman RICHMOND for his bipartisan approach in bringing this bill to the floor today.

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. 3510, the ''Department of Homeland Security Cybersecurity Strategy Act of 2015,'' which amends the Homeland Security Act of 2002, to require the Secretary of Homeland Security to develop a cybersecurity strategy for the Department of Homeland Security.

The strategy must include information on the programs, policies, and activities that are required to successfully execute the full range of the cybersecurity programs, policies, and activities in furtherance of the Department of Homeland Security's mission regarding the National Cybersecurity and Communication Integration Center.

The National Cybersecurity and Communication Integration Center addresses cybersecurity risks faced by federal and non-federal entities.

In July of this year it was reported that the Office of Personnel Management lost personal information on 21.5 million current and former federal employees and their families.

In 2014, the following agencies reported breaches: The State Department revealed that its unclassified email network had been breached in a cyberattack; the U.S. Postal Service reported that 800,000 personnel files were potentially affected by a cyber breach; the Department of Health and Human Services reported cyber intruders had accessed a server used to test code for the healthcare.gov website and installed malicious software; and the Nuclear Regulatory Commission, the agency that oversees the U.S. nuclear power industry, revealed a number of attempted intrusions and three successful intrusions into its computer systems.

In cyber time, which is near the speed of light—federal computer networks will not get a warning from a determined enemy that an attack is occurring.

Our nation's critical infrastructure and civilian government agencies depend on the cybersecurity talent and resources that the Department of Homeland Security can provide on the frontline to defend against attacks.

As with other threats that this nation has faced and overcome, we must create the resources and the institutional responses to protect our nation against cyber threats while preserving our liberties and freedoms.

We cannot accomplish this task without the full cooperation and support of the private sector, computing research community and academia.

This level of engagement requires the trust and confidence of the American people that this new cyber threat center will be used for the purpose it was created and that the collaboration of others in this effort to better protect computing networks will be used only for protection and defense.

There are people with skills and those with the potential to develop skills that would be of benefit to our nation's efforts to develop an effective cybersecurity defense and deterrence posture.

It is my hope that as we move forward the Committee on Homeland Security will continue in a bipartisan manner to seek out the best ways to bring the brightest and most qualified people into the government as cybersecurity professionals.

Toward that end, I am hosting a Town Hall on Wednesday, October 7, 2015, Town Hall'' on Minority Representation in the Cybersecurity Workforce.

I am pleased to have the Chair of the Congressional Hispanic Caucus join me in support of this important Town Hall.

The message from the federal government to the public regarding the employment opportunities available in STEM careers that include cybersecurity.

It is my commitment that Historically Black Colleges and Universities, Hispanic Serving Institutions, Native American Colleges and Women's Colleges and Universities should be actively engaged when agencies conduct outreach and program development on cybersecurity.

The Brookings' Metropolitan Policy Program's report ''The Hidden STEM Economy,'' reported that in 2011, 26 million jobs or 20 percent of all occupations required knowledge in 1 or more STEM areas.

Half of all STEM jobs are available to workers without a 4 year degree and these jobs pay on average $53,000 a year, which is 10 percent higher than jobs with similar education requirements.

There will be STEM winners and losers, but not because the skills needed are too difficult to obtain, but because people are not aware of the jobs that are going unfilled today, nor do they know what education or training will create job security for the next 2 to 3 decades.

I am very aware of the importance of STEM job training and education.

A third of Houston jobs are in STEM-based fields.

Houston has the second largest concentrations of engineers (22.4 for every 1,000 workers according to the Greater Houston Partnership.)

Houston has 59,070 engineers, the second largest populations in the nation.

STEM jobs are at the core of Houston's economic success, but what we have done with STEM innovation and job creation in the city of Houston is not enough to satisfy the regions demand for STEM trained workers.

We anticipate that in the next 5 years the gap in the number of people with STEM skills and training will not keep up with the number of positions requiring those skills.

I ask my colleagues to join me in support of H.R. 3510, the ''Department of Homeland Security Cybersecurity Strategy Act of 2015.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. RATCLIFFE) that the House suspend the rules and pass the bill, H.R. 3510, 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.

ADOPTIVE FAMILY RELIEF ACT

Mr. FRANKS of Arizona. Mr. Speaker, I move to suspend the rules and pass the bill (S. 1300) to amend section 221 of the Immigration and Nationality Act to provide relief for adoptive families from immigrant visa fees in certain situations.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 1300

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 ''Adoptive Family Relief Act''.

SEC. 2. WAIVER OF FEES FOR RENEWAL OF IMMIGRANT VISA FOR ADOPTED CHILD IN CERTAIN SITUATIONS.

Section 221(c) of the Immigration and Nationality Act (8 U.S.C. 1201(c)) is amended to read as follows:

''(c) PERIOD OF VALIDITY; RENEWAL OR REPLACEMENT.—

''(1) IMMIGRANT VISAS.—An immigrant visa shall be valid for such period, not exceeding six months, as shall be by regulations prescribed, except that any visa issued to a child lawfully adopted by a United States citizen and spouse while such citizen is serving abroad in the United States Armed Forces, or is employed abroad by the United