

Small businesses are built with families, values of unity, caring for elders. We must keep our promise.

#### BOSTON MARATHON ATTACK

(Mr. CANTOR asked and was given permission to address the House for 1 minute.)

Mr. CANTOR. Mr. Speaker, on a day meant to celebrate patriots' freedom and personal strength, we witnessed terror and tragedy. My prayers remain with the victims and everyone in Boston. I'm grateful for the first responders, the medical professionals, and fellow citizens who responded so heroically.

We don't know yet who is responsible for this terrorist attack. The United States Government must—and will—use all tools at its disposal to track down the perpetrators and hold them accountable.

This vicious act of terror cannot stand, and we must remain committed to the task of combating the scourge of terrorism no matter where it raises its ugly head.

The Boston Marathon is a symbol of so much of what is great about America. It honors personal fortitude and perseverance. Let it continue to be a symbol of fortitude and perseverance for Boston and for our entire Nation.

#### GUN VIOLENCE PREVENTION LEGISLATION

(Ms. JACKSON LEE asked and was given permission to address the House for 1 minute and to revise and extend her remarks.)

Ms. JACKSON LEE. I have been on this floor yesterday and today, earlier this morning, to offer my sympathy to those who lost their lives and suffer in Boston and say that we are united with them. But this Congress now is proceeding on some important business, and I offer to my colleagues that we cannot wait to pass legislation on gun safety and gun violence prevention.

Homicide is the second leading cause of death for young people ages 15 to 24. Homicide is the leading cause of death for many minorities in this country. 82.8 percent of young people who are killed are killed with a firearm. Every 30 minutes, a child or teenager in America is injured by a gun. Every 3 hours and 15 minutes, a child or a teenager loses their life to a firearm. And in 2010, 82 children under 5 years of age lost their lives due to guns.

We must respond.

I have introduced H.R. 65, which indicates prevention, or a system to prevent children from having access to guns. Children have accidentally shot themselves, shot their parents because guns have been accessible because we as adults have not been responsible.

As we work across the Houses, it is important to pass gun violence prevention legislation and do it now. It does not violate the Second Amendment.

#### SENATE IMMIGRATION BILL STRIKES OUT

(Mr. SMITH of Texas asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. SMITH of Texas. Mr. Speaker, it is three strikes and you're out for the Senate's immigration proposal.

First, it legalizes almost everyone in the country illegally before the border is secured. This of course will encourage even more illegal immigration.

Second, it puts the interests of foreign workers ahead of the interests of American workers. The immigration plan allows millions of illegal immigrants to compete with American workers, driving down their wages.

And third, it treats illegal immigrants better than those who have played by the rules and waited their turn in line to come into the United States. Illegal immigrants get legal status immediately. The law abiding, well, they just have to continue waiting.

I don't think the American people are going to give the Senate another turn at bat.

#### WHAT HAPPENED IN CYPRUS CAN HAPPEN IN U.S.

(Mr. MICA asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. MICA. Mr. Speaker, the indebtedness of the United States is reaching \$17 trillion. Just a few weeks ago, Europe, the entire world, and Americans shuddered when they saw, in Cyprus, what took place.

Imagine going to the bank and having the door closed. Imagine putting your ATM card in and not being able to get funds. Imagine being restricted to taking \$300 a day.

What happened in Cyprus can happen in the United States.

Remember, also, accounts for people who worked hard, had invested and put their accounts and money away. They came in; and if you had \$100,000, the government skimmed off the top.

Look at President Obama's proposal in his budget. Look at his restrictions, and also taxing and taking from those who have retired.

The same thing can happen in America that's happened in other countries.

#### POW/MIA ACCOUNTING AND RECOVERY SUPPORT ACT

(Mr. THOMPSON of Pennsylvania asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. THOMPSON of Pennsylvania. Mr. Speaker, I rise today to urge my colleagues to support H.R. 1520, the POW/MIA Accounting and Recovery Support Act of 2013.

The Joint POW/MIA Accounting Command, or JPAC, is a task force

within the Department of Defense with a mission to account for prisoners of war or those missing in action from all past conflicts. It's part of a commitment we have made to these American heroes, along with their families and loved ones seeking closure.

As most are aware, the Pentagon recently announced plans to furlough as many as 800,000 Federal civilian workers in order to achieve spending reductions under the Budget Control Act. These workers will be required to take 14 unpaid days off between now and October. As a result, JPAC employees will have to take at least 1 furlough day a week, with no exceptions. This will significantly impact JPAC's accounting and recovery teams, which are actually deployed on operations that last between 35 and 45 days.

The POW/MIA Accounting and Recovery Support Act will allow JPAC civilian employees to continue these critical missions without unnecessary disruption or delay. I encourage my colleagues to join me and Representative STEPHEN LYNCH in cosponsoring H.R. 1520.

#### HEROES AMONG US

(Mr. YODER asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. YODER. Mr. Speaker, over 100 Kansans traveled across the country to take part in the world's most recognized marathon yesterday in Boston.

We've all seen the images of the destruction caused by the cowardly acts of violence. But, Mr. Speaker, what was not cowardly was the instinct and immediate reaction of so many first responders and countless spectators who were watching their loved ones partake in the Patriots' Day tradition.

Cowardly doesn't describe runners who passed the finish line after running 26 miles and immediately, without hesitation, turning around, running back to help.

Those heroes include Dr. Chris Rupe from Salina, Kansas. Chris finished the race and was only 10 yards away from the first explosion. Dr. Rupe turned and ran to help the injured, the way Kansans do, the way so many Americans did.

Mr. Speaker, there is still much to determine in regards to the details from yesterday, and we will get those answers I'm sure of it. What is known for certain is the bravery and courage of the American people and Kansans like Dr. Rupe in emergencies and times of tragedy like yesterday in Boston.

□ 1230

#### ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (Mr. FORTENBERRY). 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.

## FEDERAL INFORMATION SECURITY AMENDMENTS ACT OF 2013

Mr. ISSA. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1163) to amend chapter 35 of title 44, United States Code, to revise requirements relating to Federal information security, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1163

*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 “Federal Information Security Amendments Act of 2013”.

### SEC. 2. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

#### “SUBCHAPTER II—INFORMATION SECURITY

##### “§ 3551. Purposes

“The purposes of this subchapter are to—

“(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

“(2) recognize the highly networked nature of the current Federal computing environment and provide effective Governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities assets;

“(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

“(4) provide a mechanism for improved oversight of Federal agency information security programs and systems through a focus on automated and continuous monitoring of agency information systems and regular threat assessments;

“(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information systems important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and

“(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

##### “§ 3552. Definitions

“(a) SECTION 3502 DEFINITIONS.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

“(b) ADDITIONAL DEFINITIONS.—In this subchapter:

“(1) ADEQUATE SECURITY.—The term ‘adequate security’ means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access

to or loss, misuse, destruction, or modification of information.

“(2) AUTOMATED AND CONTINUOUS MONITORING.—The term ‘automated and continuous monitoring’ means monitoring, with minimal human involvement, through an uninterrupted, ongoing real time, or near real-time process used to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time with rapidly changing information technology and threat development.

“(3) INCIDENT.—The term ‘incident’ means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

“(4) INFORMATION SECURITY.—The term ‘information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

“(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

“(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

“(C) availability, which means ensuring timely and reliable access to and use of information.

“(5) INFORMATION SYSTEM.—The term ‘information system’ means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information and includes—

“(A) computers and computer networks;

“(B) ancillary equipment;

“(C) software, firmware, and related procedures;

“(D) services, including support services; and

“(E) related resources.

“(6) INFORMATION TECHNOLOGY.—The term ‘information technology’ has the meaning given that term in section 11101 of title 40.

“(7) NATIONAL SECURITY SYSTEM.—

“(A) DEFINITION.—The term ‘national security system’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

“(i) the function, operation, or use of which—

“(I) involves intelligence activities;

“(II) involves cryptologic activities related to national security;

“(III) involves command and control of military forces;

“(IV) involves equipment that is an integral part of a weapon or weapons system; or

“(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

“(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

“(B) EXCEPTION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

“(8) THREAT ASSESSMENT.—The term ‘threat assessment’ means the formal description and evaluation of threat to an information system.

##### “§ 3553. Authority and functions of the Director

“(a) IN GENERAL.—The Director shall oversee agency information security policies and practices, including—

“(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

“(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

“(A) information collected or maintained by or on behalf of an agency; or

“(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

“(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

“(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

“(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3554(b);

“(6) coordinating information security policies and procedures with related information resources management policies and procedures;

“(7) overseeing the operation of the Federal information security incident center required under section 3555; and

“(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

“(A) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

“(B) significant deficiencies in agency information security practices;

“(C) planned remedial action to address such deficiencies; and

“(D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

“(b) NATIONAL SECURITY SYSTEMS.—Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

“(c) DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY SYSTEMS.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the