

Mr. PAYNE. Mr. Speaker, H.R. 5943 was unanimously approved by the committee on Homeland Security on September 13. It recognizes that Transit Security Grant Program grantees can spend their money better and smarter when they have the time necessary to do so.

I congratulate my colleague, Mr. DONOVAN, on this legislation, and I urge all of my colleagues to support H.R. 5943.

I yield back the balance of my time.

Mr. DONOVAN. Mr. Speaker, once again, I urge my colleagues to support H.R. 5943.

I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. DONOVAN) that the House suspend the rules and pass the bill, H.R. 5943, 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.

FIRST RESPONDER ACCESS TO INNOVATIVE TECHNOLOGIES ACT

Mr. DONOVAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5460) to amend the Homeland Security Act of 2002 to establish a review process to review applications for certain grants to purchase equipment or systems that do not meet or exceed any applicable national voluntary consensus standards, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5460

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 “First Responder Access to Innovative Technologies Act”.

SEC. 2. APPROVAL OF CERTAIN EQUIPMENT.

(a) IN GENERAL.—Subsection (f) of section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) by striking “If an applicant” and inserting the following:

“(1) APPLICATION REQUIREMENT.—If an applicant”; and

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

“(2) REVIEW PROCESS.—The Administrator shall implement a uniform process for reviewing applications that, in accordance with paragraph (1), contain explanations to use grants provided under section 2003 or 2004 to purchase equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 647 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 747).

“(3) FACTORS.—In carrying out the review process under paragraph (2), the Administrator shall consider the following:

“(A) Current or past use of proposed equipment or systems by Federal agencies or the Armed Forces.

“(B) The absence of a national voluntary consensus standard for such equipment or systems.

“(C) The existence of an international consensus standard for such equipment or systems, and whether such equipment or systems meets such standard.

“(D) The nature of the capability gap identified by the applicant and how such equipment or systems will address such gap.

“(E) The degree to which such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed existing consensus standards.

“(F) Any other factor determined appropriate by the Administrator.”.

(b) INSPECTOR GENERAL REPORT.—Not later than three years after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security 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 a report assessing the implementation of the review process established under paragraph (2) of subsection (f) of section 2008 of the Homeland Security Act of 2002 (as added by subsection (a) of this section), including information on the following:

(1) The number of requests to purchase equipment or systems that do not meet or exceed any applicable consensus standard evaluated under such review process.

(2) The capability gaps identified by applicants and the number of such requests granted or denied.

(3) The processing time for the review of such requests.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. DONOVAN) and the gentleman from New Jersey (Mr. PAYNE) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. DONOVAN. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days within 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 New York?

There was no objection.

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

As chairman of the Subcommittee on Emergency Preparedness, Response, and Communications, I rise in support of H.R. 5460, the First Responder Access to Innovative Technologies Act, which passed out of my subcommittee with bipartisan support on June 16 and was reported favorably by the Committee on Homeland Security earlier this month.

With threats consistently evolving, it is reassuring to see new technology being developed to ensure the safety of our communities and first responders.

□ 1500

However, emerging technology is frequently developed faster than voluntary consensus standards can be implemented.

Recipients of grants under FEMA’s State Homeland Security Grant Program and the Urban Areas Security Initiative must procure equipment that meets these standards. Unfortunately, if emerging technology or equipment

does not have a voluntary consensus standard and a grant recipient would like to use those funds to purchase such technology, FEMA does not have a uniform review process to consider applications for that equipment. This legislation requires FEMA to develop such a process for reviewing these requests.

I want to thank the subcommittee’s ranking member, Representative PAYNE, for introducing this common-sense bill. I am proud to be an original cosponsor of H.R. 5460 because it will ensure first responders have the ability to purchase equipment and emerging technology needed to effectively adapt to the current threat landscape.

First responders in multiple jurisdictions in New York and New Jersey were recently called upon to respond to a series of improvised explosive devices. It is clear that the threat to our communities is not going away; and we, as Members of Congress, must ensure our first responders can easily access emerging technology without being hampered by unnecessary bureaucracy.

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

I reserve the balance of my time.

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

I rise in support of H.R. 5460, the First Responder Access to Innovative Technologies Act.

Mr. Speaker, a week ago, after we observed the fifteenth anniversary of the September 11 attacks this month, a disturbed man planted bombs in New York City, in Seaside Park, New Jersey, and in Elizabeth, New Jersey. Local law enforcement in my district ultimately apprehended the suspect, but not before a shootout injured two brave officers, Officer Hammer and Officer Padilla of the Linden Police Department.

In our Nation’s darkest hours, the bravest among us rush into situations everyone else tries to escape. Those heroes need the best, most modern technology on the market to do their jobs better and safer.

With the help of the private sector, we have made significant strides in developing first responder technology. Nevertheless, first responders cannot use their Homeland Security grant dollars to purchase the latest technology unless it meets or exceeds voluntary industry standards, which take years to develop. To ensure that our brave first responders have access to the most modern equipment, the First Responder Access to Innovative Technologies Act directs the Federal Emergency Management Agency to develop a transparent process to review requests to purchase equipment for which voluntary industry standards do not exist.

H.R. 5460 has the support of the Securities Industry Association and was approved by the full committee by voice vote.

Mr. Speaker, our first responders are our heroes. Time and time again, they

put themselves in harm's way to protect their communities. The First Responder Access to Innovative Technologies Act will ensure that our first responders have the technology they need to keep themselves safe as they keep us safe.

I want to thank Subcommittee Chairman DONOVAN for his support of this measure. I urge my colleagues to support H.R. 5460.

I yield back the balance of my time.

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

Mr. Speaker, I once again urge my colleagues to support H.R. 5460.

I yield back the balance of my time.

The SPEAKER pro tempore (Mr. BYRNE). The question is on the motion offered by the gentleman from New York (Mr. DONOVAN) that the House suspend the rules and pass the bill, H.R. 5460, 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.

CYBER PREPAREDNESS ACT OF 2016

Mr. DONOVAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5459) to amend the Homeland Security Act of 2002 to enhance preparedness and response capabilities for cyber attacks, bolster the dissemination of homeland security information related to cyber threats, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5459

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 "Cyber Preparedness Act of 2016".

SEC. 2. INFORMATION SHARING.

Title II of the Homeland Security Act of 2002 is amended—

(1) in section 210A (6 U.S.C. 124h)—

(A) in subsection (b)—

(i) in paragraph (10), by inserting before the semicolon at the end the following: ", including, in coordination with the national cybersecurity and communications integration center under section 227, accessing timely technical assistance, risk management support, and incident response capabilities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents (as such terms are defined in such section), which may include attribution, mitigation, and remediation, and the provision of information and recommendations on security and resilience, including implications of cybersecurity risks to equipment and technology related to the electoral process";

(ii) in paragraph (11), by striking "and" after the semicolon;

(iii) by redesignating paragraph (12) as paragraph (14); and

(iv) by inserting after paragraph (11) the following new paragraphs:

"(12) review information relating to cybersecurity risks that is gathered by State,

local, and regional fusion centers, and incorporate such information, as appropriate, into the Department's own information relating to cybersecurity risks;

"(13) ensure the dissemination to State, local, and regional fusion centers of information relating to cybersecurity risks; and";

(B) in subsection (c)(2)—

(i) by redesignating subparagraphs (C) through (G) as subparagraphs (D) through (H), respectively; and

(ii) by inserting after subparagraph (B) the following new subparagraph:

"(C) The national cybersecurity and communications integration center under section 227.;"

(C) in subsection (d)—

(i) in paragraph (3), by striking "and" after the semicolon;

(ii) by redesignating paragraph (4) as paragraph (5); and

(iii) by inserting after paragraph (3) the following new paragraph:

"(4) assist, in coordination with the national cybersecurity and communications integration center under section 227, fusion centers in using information relating to cybersecurity risks to develop a comprehensive and accurate threat picture; and"; and

(D) in subsection (j)—

(i) by redesignating paragraphs (1) through (5) as paragraphs (2) through (6), respectively; and

(ii) by inserting before paragraph (2), as so redesignated, the following new paragraph:

"(1) the term 'cybersecurity risk' has the meaning given that term in section 227.;" and

(2) in section 227 (6 U.S.C. 148)—

(A) in subsection (c)—

(i) in paragraph (5)(B), by inserting ", including State and major urban area fusion centers, as appropriate" before the semicolon at the end;

(ii) in paragraph (7), in the matter preceding subparagraph (A), by striking "information and recommendations" each place it appears and inserting "information, recommendations, and best practices"; and

(iii) in paragraph (9), by inserting "and best practices" after "defensive measures"; and

(B) in subsection (d)(1)(B)(ii), by inserting "and State and major urban area fusion centers, as appropriate" before the semicolon at the end.

SEC. 3. HOMELAND SECURITY GRANTS.

Subsection (a) of section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) by redesignating paragraphs (4) through (14) as paragraphs (5) through (15), respectively; and

(2) by inserting after paragraph (3) the following new paragraph:

"(4) enhancing cybersecurity, including preparing for and responding to cybersecurity risks and incidents and developing State-wide cyber threat information analysis and dissemination activities.;"

SEC. 4. SENSE OF CONGRESS.

It is the sense of Congress that to facilitate the timely dissemination to appropriate State, local, and private sector stakeholders of homeland security information related to cyber threats, the Secretary of Homeland Security should, to the greatest extent practicable, work to share actionable information related to cyber threats in an unclassified form.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. DONOVAN) and the gentleman from New Jersey (Mr. PAYNE) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. DONOVAN. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days 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 New York?

There was no objection.

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

Mr. Speaker, September is National Preparedness Month, and as chairman of the Committee on Homeland Security's Subcommittee on Emergency Preparedness, Response, and Communications, I think it is fitting that we are here today to consider a number of bills that will enhance our homeland security, including legislation I introduced, H.R. 5459, the Cyber Preparedness Act of 2016.

Cybersecurity is a major national security issue, and the threat is real and immediate. For instance, a cyber attack causing widespread power outages could have major cascading consequences on public health and safety; however, it appears that the Nation is not adequately prepared to prevent and respond to cyber attacks.

Since 2012, FEMA has released an annual National Preparedness Report, which highlights States' progress in meeting 32 core capabilities as defined by the National Preparedness Goal. Each year, States have ranked their cybersecurity capabilities as one of their lowest.

In May, my subcommittee, the Emergency Preparedness, Response, and Communications Subcommittee, held a joint hearing with the Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies to look at the current state of cyber preparedness and how the Federal Government can help the States address some of the challenges that they face.

Witnesses explained that, while great progress has been made in enhancing their cybersecurity capabilities, challenges still remain, especially with regard to information sharing of cyber threats and risks and whether Homeland Security grants may be used for cybersecurity enhancements.

I introduced H.R. 5459, the Cyber Preparedness Act of 2016, to address a number of findings from this hearing. My legislation addresses these findings by enhancing cyber risk information sharing with State and major urban area fusion centers; authorizing representatives from State and urban area fusion centers to be assigned to the National Cybersecurity and Communications Integration Center, and permitting the NCCIC personnel to be deployed to fusion centers; sharing information on cyber preparedness best practices with State and local stakeholders; clarifying the eligibility of