failed to keep the pace with breakthroughs in technology. As a result, we have found that first responders cannot always access the most up-to-date equipment because they cannot use Homeland Security grant funds to purchase equipment and technology that does not meet or exceed voluntary industry standards.

H.R. 687 would require FEMA to develop a transparent process for reviewing requests to use grant funds to purchase technologies that do not meet or exceed voluntary industry standards and/or that are not on the authorized equipment list.

The bill has the support of the Security Industry Association and unanimously passed the House last September. Mr. Speaker, I include in the RECORD a letter from the Security Industry Association.

SECURITY INDUSTRY ASSOCIATION,
Silver Spring, MD, January 27, 2017.

Hon. DAN DONOVAN,
Chairman, House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications, Washington, DC.

Hon. DONALD PAYNE,
Ranking Member, House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications, Washington, DC.

DEAR CHAIRMAN DONOVAN AND RANKING MEMBER PAYNE: On behalf of the Security Industry Association (SIA), I would like to express our strong support for H.R. 687, the First Responder Access to Innovative Technologies Act, which would streamline the existing process for first responders utilizing homeland security grants to purchase innovative equipment. SIA is a non-profit international trade association representing nearly 700 global security and life safety solutions providers, and our members develop, manufacture and integrate equipment that is vital to carrying out a variety of homeland security missions.

Under current law, equipment purchased with homeland security grants must meet or exceed ''national voluntary consensus standards,'' unless an explanation as to why an exception is necessary is provided to, reviewed and approved by the Department. For some products, including first responder equipment, technology innovations have outpaced the process of developing voluntary consensus standards, and no such standards may yet exist. Among other provisions, H.R. 687 directs FEMA to develop a more consistent and transparent process for reviewing these requests, which would expedite consideration and provide more certainty to stakeholders.

Like you, we believe that first responders must be able to choose the most appropriate and advanced equipment to meet urgent and changing needs as they work to protect the public. SIA and its members stand ready to serve as a resource to you as you continue work on this critical issue. Thank you for your leadership and attention to this important matter.

Sincerely,

DON ERICKSON,
CEO, Security Industry Association.

□ 1600

Mr. PAYNE. Mr. Speaker, our first responders are on the front lines of emergency response. In recognition of their bravery and sacrifices they make every day, in and out, we must make sure that they have the access to the most up-to-date technologies to help them do their jobs better and safer. To that end, I urge my colleagues to support H.R. 687.

Mr. Speaker, 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. 687, and I yield back the balance of my time.

The SPEAKER pro tempore (Mr. JODY B. HICE of Georgia). 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. 687.

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.

CYBER PREPAREDNESS ACT OF 2017

Mr. DONOVAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 584) 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.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 584

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 2017''.

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, access to 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 ''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 (as such terms are defined in section 227) and developing statewide 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 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. DONOVAN. Mr. Speaker, I yield myself such time I may consume.

Mr. Speaker, I rise today in support of H.R. 584, the Cyber Preparedness Act of 2017.

Cybersecurity is a major national security issue and the threat is real and immediate. Day in and day out nation-states or criminal actors target the United States' critical infrastructure, the private sector, and everyday Americans, and they are succeeding. However, even with the heightened awareness on cybersecurity, it appears that the United States 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. Every year, States have ranked their cybersecurity capabilities as one of their lowest.

I found these facts very alarming and wanted to learn more about the current state of cyber preparedness. That is why, last Congress, my subcommittee, the Emergency Preparedness, Response, and Communications Subcommittee, held a joint hearing with the committee's Cybersecurity and Infrastructure Protection Subcommittee to look at cyber preparedness and how the Federal Government can help States address some of the challenges they face.

We heard from a Homeland Security adviser, a fusion center representative, the Center for Internet Security, a chief information officer, and a chief technology officer, who explained the great progress the United States has made in enhancing their security capabilities. However, they cautioned that 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.

Last Congress, I introduced this bill to address the findings from that hearing. I introduced this bill in this Congress to ensure that States and first responders have the resources needed to prepare for and protect against cyber attacks.

This commonsense legislation will: Enhance cyber risk information sharing with State and major urban area fusion centers; authorize representatives from State and urban area fusion centers to be assigned to the National Cybersecurity and Communications Integration Center; and permit the NCCIC personnel to be deployed to the fusion centers.

It will allow information sharing on cyber preparedness best practices with State and local stakeholders. It will clarify the eligibility of State Homeland Security Grant Program and Urban Area Security Initiative funding for cybersecurity enhancements; and it will work to combat the overclassification of cyber risk information so that it can be shared more broadly with stakeholders who have a need to know.

I appreciate that Chairman MCCAUL, Chairman RATCLIFFE, and Ranking Member PAYNE joined me again as original cosponsors of H.R. 584. This bipartisan legislation passed the House by voice vote last Congress. I am pleased that the House is willing to take up this measure again in the new Congress.

I urge my colleagues to join me in supporting this bipartisan bill.

Mr. Speaker, I reserve the balance of my time.

Mr. PAYNE. Mr. Speaker, I rise in support of H.R. 584, the Cyber Preparedness Act of 2017, and I yield myself such time as I may consume.

Mr. Speaker, since I became ranking member of the Subcommittee on Emergency Preparedness, Response, and Communications 4 years ago, States have repeatedly expressed concern about the ability to confront the cyber threat and have rated cybersecurity among the core capabilities in which they had the least confidence.

Last Congress, the subcommittee held a hearing on State and local efforts to counter the cyber threat where State emergency managers and chief information officers testified about activities they were undertaking to secure their networks and infrastructure.

For example, my home State of New Jersey has begun developing its own cyber information-sharing capability, similar to DHS' National Cybersecurity and Communications Integration Center.

Since the subcommittee held its hearing last year, the Federal Government has made significant progress in providing cybersecurity guidance to Federal, State, and local stakeholders.

In December of 2016, the Department of Homeland Security issued its national Cyber Incident Response Plan, which describes roles and responsibilities among stakeholders with respect to preventing, disrupting, and responding to a cyber event.

Additionally, the plan also provides guidance on information sharing related to cyber threats.

H.R. 584 would help facilitate implementation of the National Cyber Incident Response Plan by promoting the sharing of cyber threat indicators and information, as well as cybersecurity's best practices, with State and major urban area fusion centers.

The bill also designates ''cybersecurity'' as an allowable use of State Homeland Security grants and Urban Area Security Initiative funds, which would help other States replicate the cyber threat information-sharing capabilities developed in New Jersey.

This is commonsense legislation, passed by the House last Congress, and I urge my colleagues to support the measure once again.

Mr. Speaker, last fall, the range of cyber threats we faced came into focus when a foreign government attempted to interfere and undermine the integrity of our Presidential election by hacking into the campaign and political party databases.

H.R. 584 includes language to address this threat by directing DHS to share cyber threat information regarding election equipment and technology with fusion centers.

H.R. 584 seems to secure our critical cyber networks by improving cyber information sharing with fusion centers on the full spectrum of cyber threats.

Mr. Speaker, I urge my colleagues to support H.R. 584, and 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. 584, and 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. 584.

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.

GAINS IN GLOBAL NUCLEAR DETECTION ARCHITECTURE ACT

Mr. DONOVAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 690) to amend the Homeland Security Act of 2002 to enhance certain duties of the Domestic Nuclear Detection Office, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 690

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 ''Gains in Global Nuclear Detection Architecture Act''.

SEC. 2. DUTIES OF THE DOMESTIC NUCLEAR DETECTION OFFICE.

Section 1902 of the Homeland Security Act of 2002 (6 U.S.C. 592) is amended—

(1) by redesignating subsection (b) as subsection (c); and

(2) by inserting after subsection (a) the following new subsection:

''(b) IMPLEMENTATION.—In carrying out paragraph (6) of subsection (a), the Director of the Domestic Nuclear Detection Office shall—

''(1) develop and maintain documentation, such as a technology roadmap and strategy, that—

''(A) provides information on how the Office's research investments address—

''(i) gaps in the enhanced global nuclear detection architecture, as developed pursuant to paragraph (4) of such subsection; and

''(ii) research challenges identified by the Director; and

''(B) defines in detail how the Office will address such research challenges;