pursuant to section 44946 of title 49, United States Code) and appropriate public and private sector stakeholders.

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

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

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

Mr. Speaker, I rise in support of H.R. 5766, the Securing Public Areas of Transportation Facilities Act of 2018. This legislation will improve security coordination among transportation stakeholders by establishing a working group between the Department of Homeland Security and public and private stakeholders to develop recommendations for enhancing public area security of transportation facilities.

H.R. 5766 directs that the working group focus on key areas including information sharing, interoperable communications, incident response, and the prevention of terrorist attacks through strategic planning and security exercises. Taking steps to improve upon these critical components to security preparedness and resiliency is directly correlated to America's ability to mitigate the constantly-evolving threat to our transportation system.

The traveling public must be secure in all modes of transportation security, and the millions of Americans who utilize surface transportation networks every single day to travel to work and school rely upon strong Federal, State, local, and private sector collaboration.

Over the last several years we have seen a marked increase in attacks to public areas of transportation networks. From airports like LAX in Los Angeles, Fort Lauderdale, Istanbul, Brussels, to mass transit hubs in New York City, London, Madrid and Belgium, we have witnessed horrific scenes of attack in crowded public spaces of transportation systems.

I am glad this bill seeks to improve upon the resiliency, preparedness, and overall security infrastructure of these networks, which are absolutely crucial to our economy and the American way of life.

The free movement of people and goods across the United States must never be stymied by violent extremism. That is why it is incumbent upon those of us in Congress to ensure that Homeland Security and TSA are doing all they can to promote effective collaboration among the litany of stakeholders charged with securing the traveling public.

Mr. Speaker, I thank the gentleman from New Jersey (Mr. PAYNE) for his focus on this important issue. I also thank the chairman of the full committee, Mr. MCCAUL, for seeing this bill through the markup process.

I urge my colleagues to support this bill, and I reserve the balance of my time.

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

I rise in support of H.R. 5766, the Securing Public Areas of Transportation Facilities Act of 2018.

Mr. Speaker, H.R. 5766 was introduced to address the growing risk of terrorist attacks in the public areas of transportation facilities.

In recent years, there has been a growing appreciation that public areas of airports and transportation facilities, where crowds tend to gather, have become soft targets for terrorists. We have seen that internationally and domestically, as there have been violent incidents in public airport areas in Brussels, Los Angeles, New Orleans and Fort Lauderdale. Last year, there was an attempted attack on New York City's transit system as well.

H.R. 5766 seeks to bolster protection for the public-facing sides of transportation systems. It does so, in part, by authorizing a working group to streamline communication and collaboration between the Department of Homeland Security and key stakeholders. Additionally, it directs DHS to disseminate technical assistance to operators such as vulnerability assessment tools and cybersecurity guidelines.

Finally, H.R. 5766 requires TSA to review its regulations, policies, and procedures regarding the transportation of firearms and ammunition and submit a comprehensive report to Congress on its findings and any planned modifications. The presence of firearms and ammunition in public areas of transportation facilities is a timely concern.

□ 1945

In January 2017, an arriving airline passenger in Fort Lauderdale retrieved a gun and ammunition from his checked bag and opened fire on travelers in the baggage claim area, killing five people and injuring six others.

In 2017 alone, TSA reported that its officers discovered 3,957 firearms at security checkpoints, 84 percent of which were loaded.

Mr. Speaker, given the prevalence and availability of guns in this country, the very least we can do is evaluate TSA's policies for transporting them and ensure that they are sensible and tailored to the risk.

Mr. Speaker, I urge my House colleagues to support this bipartisan legislation, and I reserve the balance of my time.

Mr. KATKO. Mr. Speaker, I want to thank my colleague from Rhode Island for supporting this bill, and I reserve the balance of my time.

Mr. LANGEVIN. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, H.R. 5766 is an important piece of legislation that has strong support on both sides of the aisle. It is nice to see the bipartisanship once again. It directs meaningful, sensible action to help enhance the security of public-facing areas.

Mr. Speaker, I encourage my colleagues to support H.R. 5766, and I yield back the balance of my time.

Mr. KATKO. Mr. Speaker, my time on the Homeland Security Committee over the past 3½ years has been a true testament to bipartisanship: trying to get the right things done, putting aside political differences to keep the country as safe and secure as we possibly can.

Mr. Speaker, I am honored to support the bill of my colleague from New Jersey (Mr. PAYNE). I urge my colleagues to support the bill, 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. KATKO) that the House suspend the rules and pass the bill, H.R. 5766.

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.

DHS INDUSTRIAL CONTROL SYSTEMS CAPABILITIES ENHANCEMENT ACT OF 2018

Mr. BACON. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5733) to amend the Homeland Security Act of 2002 to provide for the responsibility of the National Cybersecurity and Communications Integration Center to maintain capabilities to identify threats to industrial control systems, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5733

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 ''DHS Industrial Control Systems Capabilities Enhancement Act of 2018''.

SEC. 2. CAPABILITIES OF NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS.

(a) IN GENERAL.—Section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148) is amended—

(1) in subsection (e)(1)—

(A) in subparagraph (G), by striking ''and'' after the semicolon;

(B) in subparagraph (H), by inserting ''and'' after the semicolon; and

(C) by adding at the end the following new subparagraph:

''(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;'';

(2) by redesignating subsections (f) through (m) as subsections (g) through (n), respectively; and

(3) by inserting after subsection (d) the following new subsection:

''(f) INDUSTRIAL CONTROL SYSTEMS.—The Center shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Center shall—

''(1) lead, in coordination with relevant sector specific agencies, Federal Government efforts to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

''(2) maintain cross-sector incident response capabilities to respond to industrial control system cybersecurity incidents;

''(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, and other industrial control system stakeholders to identify and mitigate vulnerabilities;

''(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, and other industrial control systems stakeholders; and

''(5) conduct such other efforts and assistance as the Secretary determines appropriate.''.

(b) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, and every 6 months thereafter during the subsequent four-year period, the National Cybersecurity and Communications Integration Center shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the industrial control systems capabilities of the Center under subsection (f) of section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148), as added by subsection (a).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Nebraska (Mr. BACON) and the gentleman from Rhode Island (Mr. LANGEVIN) each will control 20 minutes.

The Chair recognizes the gentleman from Nebraska.

GENERAL LEAVE

Mr. BACON. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on the bill under consideration.

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

There was no objection.

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

Mr. Speaker, I rise today in support of H.R. 5733, the DHS Industrial Control Systems Capabilities Enhancement Act of 2018.

Industrial control systems are the critical interface between digital controls and a physical process. These systems are ubiquitous in our modern society and are utilized in all 16 sectors of our Nation's critical infrastructure.

Whether they are used in managing the operations of electric power generators, water treatment facilities, medical devices, manufacturing facilities, or transportation networks, disruptions or damage to these systems have the potential to cause catastrophic and cascading consequences to our Nation's national security, our economic security, and our public health and safety.

The Department of Homeland Security's National Cybersecurity and Communications Integration Center, or NCCIC, has a key role in addressing the security of both information technology and operational technology, including the industrial control systems.

DHS, through the NCCIC, currently provides operators of industrial control systems across critical infrastructure sectors with support. They do this with malware and vulnerability analysis, incident response, and briefings on emerging threats and vulnerabilities.

H.R. 5733 codifies DHS' current role and directs them to maintain existing capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in automated control of critical infrastructure processes. This legislation also supports DHS' function to secure ICS technologies by allowing NCCIC to provide cybersecurity technical assistance to ICS end users, product manufacturers, and other stakeholders to mitigate and identify vulnerabilities.

DHS operates a central hub for ICS information exchange, technical expertise, operational partnerships, and ICS-focused cybersecurity capabilities. Mr. Speaker, I urge my colleagues to support H.R. 5733 to codify the work that DHS performs in mitigating industrial control system vulnerabilities, while ensuring that private industry has a permanent place for assistance to address cybersecurity risks.

I want to thank Chairman MCCAUL and Chairman RATCLIFFE for their support of this legislation, as well as Congressman LANGEVIN for his amendment in committee. This is a bipartisan effort.

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

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

Mr. Speaker, I rise in support of H.R. 5733, the DHS Industrial Control Systems Capabilities Enhancement Act. H.R. 5733 would codify the Department of Homeland Security's role in leading Federal efforts to secure industrial control systems.

I want to commend the gentleman from Nebraska (Mr. BACON) for his hard work on this legislation. I have enjoyed collaborating with him on it, and I am grateful for his support and his support of the amendment that I offered in committee to make the act, I think, even better.

Mr. Speaker, we depend on control systems to deliver basic necessities like clean water, a steady energy supply, reliable transportation systems, and medical care.

This is not a new role for DHS, which has been working on control system security since 2004. However, enactment of H.R. 5733 will help provide clarity to DHS and its Federal partners at a critical moment in our Nation's history.

Cyber threats, Mr. Speaker, to critical infrastructure have never been greater, yet leadership from the White House is dangerously lacking. Over the past few months, we have seen top cyber officials at the White House leave, resign, or, in the case of the Cybersecurity Coordinator, have the position eliminated altogether.

What is more, the President appears to be making major foreign policy decisions with little, if any, regard for cybersecurity. The President ignored warnings from the intelligence community about Chinese telecom company ZTE when, in May, he directed the Commerce Department, by tweet, to save this habitual sanctions offender. The same month, the news broke that the Chinese Government had hacked into the networks of a U.S. Navy contractor and syphoned off sensitive military data.

This month, DHS officials reported that the North Korean Government is ramping up its cyber intrusions on critical infrastructure in the U.S. and around the world.

With respect to Russia, we know that the Kremlin has the capability to turn off the lights with a cyber intrusion, as it has done in Ukraine. We also know that Russia has been able to successfully infiltrate the networks of a wide range of U.S. critical infrastructure operators, including power plants.

DHS, through the National Cybersecurity and Communications Integration Center, or the NCCIC, provides critical infrastructure owners and operators with valuable cyber assistance and resources to help secure their systems. The NCCIC, and specifically the Industrial Control Systems Computer Emergency Response Team, or ICS-CERT, has longstanding relationships with critical infrastructure stakeholders and the expertise to help owners and operators harden their defenses.

Expertise in operational technology, or OT, cybersecurity is even harder to come by than the more traditional information and communications technology, or ICT, space, and all of my colleagues know how much of a workforce challenge we are facing there.

Congress is wise to recognize the amazing resource we have in ICS-CERT by formally authorizing it with Mr. BACON's bill. Security solutions in the ICT space do not always map well onto operational technology, and being conversant in the nuances is essential if we are to protect the systems that we so heavily rely on.

During the committee consideration, I was also proud to offer an amendment to codify ICS-CERT's coordinated vulnerability disclosure program that ensures ICS vulnerabilities can be reported securely, promptly, and responsibly. Through this program, manufacturers are assured of a chance to patch

vulnerabilities before they are publicly announced, and security researchers are assured that their voices will be heard.

ICS-CERT is to be commended for running a progressive program that recognizes that most security researchers want to help make the internet and the scary devices that connect to it a safer place. The coordinated vulnerability program does just that by helping critical infrastructure owners and operators who receive notices from ICS-CERT about discovered vulnerabilities and effective patches before malicious actors have a chance to exploit any flaws. Mr. Speaker, this bill would empower ICS-CERT to carry out this mission fully and effectively.

Mr. Speaker, I want to again commend the gentleman for his work on this important piece of legislation. I urge my colleagues to support the measure.

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

Mr. BACON. Mr. Speaker, I just want to say it has been a pleasure working with Mr. LANGEVIN not only on the Homeland Security Committee, but also on the Armed Services Committee. We have partnered on quite a few things, and it is wonderful to make a difference with him.

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

Mr. LANGEVIN. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, there is no question that industrial control systems are a high-value target for our adversaries. Critical infrastructure owners and operators use these systems to deliver the services that underpin our day-to-day lives, and destruction to one of those systems could have tremendous economic ramifications or could even be the difference between life and death.

We know that our adversaries—most notably Russia, China, Iran, and North Korea—have all targeted U.S. critical infrastructure and the operational technology employed across these sectors. Mr. Speaker, it is important that we solidify DHS' longstanding leadership role in securing critical infrastructure, particularly with respect to industrial control systems.

It has been a pleasure working with my colleague Mr. BACON, the gentleman from Nebraska, on this bill. I deeply appreciate both his service to the country as well as his contributions both on the Armed Services Committee and on the Homeland Security Committee. Likewise, it has been a pleasure working with him over these years.

Mr. Speaker, I encourage my colleagues to support H.R. 5733, and I yield back the balance of my time.

Mr. BACON. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, first, I again want to thank my colleague from Rhode Island for his partnership on this, and his comments were absolutely right. The Russians and the Chinese are both working to be able to attack our energy grid, among other parts of our infrastructure, and we need to be prepared. And it doesn't start on day one of a war. It starts now, when we have the time to prepare.

The next December 7 will not be like Pearl Harbor with aircraft and torpedoes and bombs coming to attack our Pacific Fleet. It is going to be preceded by a cyber attack that is going to try to shut down our energy grid and other parts of our infrastructure, and the time to prepare is now. This bill starts that process, or continues that process, so that we are prepared.

Mr. Speaker, I urge my colleagues to support this bill, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Nebraska (Mr. BACON) that the House suspend the rules and pass the bill, H.R. 5733, 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.

□ 2000

OFFICE OF BIOMETRIC IDENTITY MANAGEMENT AUTHORIZATION ACT OF 2018

Ms. MCSALLY. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5206) to amend the Homeland Security Act of 2002 to establish the Office of Biometric Identity Management, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5206

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 ''Office of Biometric Identity Management Authorization Act of 2018'' or the ''OBIM Authorization Act of 2018''.

SEC. 2. ESTABLISHMENT OF THE OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et. seq.) is amended by adding at the end the following new section:

''SEC. 710. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

''(a) ESTABLISHMENT.—The Office of Biometric Identity Management is established within the Management Directorate of the Department.

''(b) DIRECTOR.—

''(1) IN GENERAL.—The Office of Biometric Identity Management shall be administered by the Director of the Office of Biometric Identity Management (in this section referred to as the 'Director') who shall report to the Secretary, or to another official of the Department, as the Secretary may direct.

''(2) QUALIFICATIONS AND DUTIES.—The Director shall—

''(A) have significant professional management experience, as well as experience in the field of biometrics and identity management;

''(B) lead the Department's biometric identity services to support anti-terrorism, counter-terrorism, border security, credentialing, national security, and public safety;

''(C) enable operational missions across the Department by receiving, matching, storing, sharing, and analyzing biometric and associated biographic and encounter data;

''(D) deliver biometric identity information and analysis capabilities to—

''(i) the Department and its components;

''(ii) appropriate Federal, State, local, and tribal agencies;

''(iii) appropriate foreign governments; and

''(iv) appropriate private sector entities;

''(E) support the law enforcement, public safety, national security, and homeland security missions of other Federal, State, local, and tribal agencies, as appropriate;

''(F) manage the operation of the Department's primary biometric repository and identification system;

''(G) manage Biometric Support Centers to provide biometric identification and verification analysis and services to the Department, appropriate Federal, State, local, and tribal agencies, appropriate foreign governments, and appropriate private sector entities;

''(H) oversee the implementation of Department-wide standards for biometric conformity, and work to make such standards Government-wide;

''(I) in coordination with the Department's Office of Policy, and in consultation with relevant component offices and headquarters offices, enter into data sharing agreements with appropriate Federal, State, local, and foreign agencies to support immigration, law enforcement, national security, and public safety missions;

''(J) maximize interoperability with other Federal, State, local, and foreign biometric systems, as appropriate;

''(K) ensure the activities of the Office of Biometric Identity Management are carried out in compliance with the policies and procedures established by the Privacy Officer appointed under section 222; and

''(L) carry out other duties and powers prescribed by law or delegated by the Secretary.

''(c) DEPUTY DIRECTOR.—There shall be in the Office of Biometric Identity Management a Deputy Director, who shall assist the Director in the management of the Office.

''(d) OTHER AUTHORITIES.—

''(1) IN GENERAL.—The Director may establish such other offices within the Office of Biometric Identity Management as the Director determines necessary to carry out the missions, duties, functions, and authorities of the Office.

''(2) NOTIFICATION.—If the Director exercises the authority provided by paragraph (1), the Director shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 30 days before exercising such authority.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 709 the following new item:

''Sec. 710. Office of Biometric Identity Management.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from Arizona (Ms. MCSALLY) and the gentleman from Rhode Island (Mr. LANGEVIN) each will control 20 minutes.