will postpone further proceedings today on motions to suspend the rules on which the yeas and nays are ordered.

The House will resume proceedings on postponed questions at a later time.

## DHS SOFTWARE SUPPLY CHAIN RISK MANAGEMENT ACT OF 2021

Mr. THOMPSON of Mississippi. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4611) to direct the Secretary of Homeland Security to issue guidance with respect to certain information and communications technology or services contracts, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4611

*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 Software Supply Chain Risk Management Act of 2021''.

**SEC. 2. DEPARTMENT OF HOMELAND SECURITY GUIDANCE WITH RESPECT TO CERTAIN INFORMATION AND COMMUNICATIONS TECHNOLOGY OR SERVICES CONTRACTS.**

(a) GUIDANCE.—The Secretary of Homeland Security, acting through the Under Secretary, shall issue guidance with respect to new and existing covered contracts.

(b) NEW COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each new covered contract, as a condition on the award of such a contract, each contractor responding to a solicitation for such a contract shall submit to the covered officer—

(1) a planned bill of materials when submitting a bid proposal; and

(2) the certification and notifications described in subsection (e).

(c) EXISTING COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each existing covered contract, each contractor with an existing covered contract shall submit to the covered officer—

(1) the bill of materials used for such contract, upon the request of such officer; and

(2) the certification and notifications described in subsection (e).

(d) UPDATING BILL OF MATERIALS.—With respect to a covered contract, in the case of a change to the information included in a bill of materials submitted pursuant to subsections (b)(1) and (c)(1), each contractor shall submit to the covered officer the update to such bill of materials, in a timely manner.

(e) CERTIFICATION AND NOTIFICATIONS.—The certification and notifications referred to in subsections (b)(2) and (c)(2), with respect to a covered contract, are the following:

(1) A certification that each item listed on the submitted bill of materials is free from all known vulnerabilities or defects affecting the security of the end product or service identified in—

(A) the National Institute of Standards and Technology National Vulnerability Database; and

(B) any database designated by the Under Secretary, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, that tracks security vulnerabilities and defects in open source or third-party developed software.

(2) A notification of each vulnerability or defect affecting the security of the end product or service, if identified, through—

(A) the certification of such submitted bill of materials required under paragraph (1); or

(B) any other manner of identification.

(3) A notification relating to the plan to mitigate, repair, or resolve each security vulnerability or defect listed in the notification required under paragraph (2).

(f) ENFORCEMENT.—In developing guidance under subsection (a), the Secretary shall instruct covered officers with respect to—

(1) the processes available to such officers enforcing subsections (b) and (c); and

(2) when such processes should be used.

(g) EFFECTIVE DATE.—The guidance required under subsection (a) shall take effect on the date that is 180 days after the date of the enactment of this section.

(h) GAO REPORT.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Secretary, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes—

(1) a review of the implementation of this section;

(2) information relating to the engagement of the Department of Homeland Security with industry;

(3) an assessment of how the guidance issued pursuant to subsection (a) complies with Executive Order 14208 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity); and

(4) any recommendations relating to improving the supply chain with respect to covered contracts.

(i) DEFINITIONS.—In this section:

(1) BILL OF MATERIALS.—The term ''bill of materials'' means a list of the parts and components (whether new or reused) of an end product or service, including, with respect to each part and component, information relating to the origin, composition, integrity, and any other information as determined appropriate by the Under Secretary.

(2) COVERED CONTRACT.—The term ''covered contract'' means a contract relating to the procurement of covered information and communications technology or services for the Department of Homeland Security.

(3) COVERED INFORMATION AND COMMUNICATIONS TECHNOLOGY OR SERVICES.—The term ''covered information and communications technology or services'' means the terms—

(A) ''information technology'' (as such term is defined in section 11101(6) of title 40, United States Code);

(B) ''information system'' (as such term is defined in section 3502(8) of title 44, United States Code);

(C) ''telecommunications equipment'' (as such term is defined in section 3(52) of the Communications Act of 1934 (47 U.S.C. 153(52))); and

(D) ''telecommunications service'' (as such term is defined in section 3(53) of the Communications Act of 1934 (47 U.S.C. 153(53))).

(4) COVERED OFFICER.—The term ''covered officer'' means—

(A) a contracting officer of the Department; and

(B) any other official of the Department as determined appropriate by the Under Secretary.

(5) SOFTWARE.—The term ''software'' means computer programs and associated data that may be dynamically written or modified during execution.

(6) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary for Management of the Department of Homeland Security.

**SEC. 3. DETERMINATION OF BUDGETARY EFFECTS.**

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the House Budget Committee, provided that such statement has been submitted prior to the vote on passage.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Mississippi (Mr. THOMPSON) and the gentleman from Mississippi (Mr. GUEST) each will control 20 minutes.

The Chair recognizes the gentleman from Mississippi (Mr. THOMPSON).

GENERAL LEAVE

Mr. THOMPSON of Mississippi. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and to include extraneous material on this measure.

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

There was no objection.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in strong support of H.R. 4611, the DHS Software Supply Chain Risk Management Act of 2021.

With each passing day, we see cyberattacks becoming increasingly more frequent and sophisticated, posing a significant threat to homeland security and the U.S. economy.

The tactics cybercriminals use to steal information or disrupt access to critical information systems are ever evolving. Many prey upon vulnerabilities within the victim's security measures or the victim's software supply chain.

The ransomware attack on the Colonial Pipeline and the attempted hack of a water treatment plan in Oldsmar, Florida, earlier this year, show just how easily critical infrastructure systems can be compromised.

Last year's compromise of the SolarWinds Orion software supply chain demonstrated how widespread and damaging such attacks can be.

In the SolarWinds attack, cybercriminals were able to add malicious code to a commercial software product that was subsequently downloaded by several Federal agencies, including the Department of Homeland Security.

As the lead Federal agency for cybersecurity, it is important that DHS lead by example, aggressively protecting its own networks.

To that end, H.R. 4611 would enhance the Department's ability to protect its networks by modernizing how it buys information and communications technology or services.

H.R. 4611 directs DHS to issue Department-wide guidance to improve visibility into the supply chain for software purchased from new and existing contractors.

Specifically, under this legislation, contractors would have to provide a bill of materials that identifies each part or component of the software supplied to DHS and take steps to ensure that each item is free from known security vulnerabilities or defects.

The bill of materials process is akin to the listing of ingredients on a package of food.

Once DHS has this detailed supply chain information, it will have far greater visibility into what it is purchasing and installing on its networks.

□ 1545

With this information, DHS can take more timely action to mitigate risks associated with software on its network.

Importantly, H.R. 4611, which was introduced by my colleague from New York (Mr. TORRES), requires DHS to instruct personnel on how to enforce the new requirements to hold contractors accountable.

Finally, the bill requires the Government Accountability Office to review the department-wide guidance and assess how it aligns with President Biden's recent executive order on improving the Nation's cybersecurity.

As the President stated in this order, the Federal Government must take decisive steps to modernize its approach to cybersecurity to keep pace with today's dynamic and increasingly sophisticated cyber threat environment.

I could not agree more.

Enactment of H.R. 4611 would be a decisive step toward improving DHS's ability to prevent, detect, and respond to cyberattacks on its own networks.

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

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

Madam Speaker, I rise today in support of H.R. 4611, the DHS Software Supply Chain Risk Management Act of 2021.

As we have seen over the past year, our software supply chains are increasingly vulnerable. It is vital that the Department of Homeland Security does its part to ensure that software in use by the Department and its contractors is secure.

This legislation will help DHS better understand and track the software and systems in use by its contractors so that it can better mitigate risk within the software supply chain.

I urge Members to join me in supporting H.R. 4611, and I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield 2 minutes to the gentleman from New York (Mr. TORRES), the vice chair of the Committee on Homeland Security and the sponsor of the bill.

Mr. TORRES of New York. Madam Speaker, a cyberattack on a software supply chain is like an infectious disease outbreak, spreading widely and rapidly, and causing untold damage far and wide.

The SolarWinds espionage campaign against the United States, which spread surreptitiously through a software product, represents the greatest intrusion into the Federal Government in the history of the United States.

SolarWinds should serve as a wake-up call. The United States Government can no longer take for granted the safety of the software it uses. The Federal Government must be proactive in identifying and correcting cyber vulnerabilities; and as the lead agency on cybersecurity, DHS in particular must emerge as the gold standard.

I am therefore proud to partner, on a bipartisan basis, with my colleague, the gentleman from New York (Mr. GARBARINO), to pass H.R. 4611, the DHS Software Supply Chain Risk Management Act of 2021.

H.R. 4611 would require the DHS Under Secretary for Management to issue department-wide guidance that in turn requires DHS contractors to submit a software bill of materials, identifying the origin of each component of software provided to DHS.

DHS should know the precise origin of the software it uses; whether a software component comes from a questionable firm that fails to follow best practices in cybersecurity; whether it comes from a hostile nation-state intent on planting back doors.

Homeland security can easily die in darkness, and the purpose of H.R. 4611 is to bring greater light, greater transparency to the software supply chains which for far too long have been left wide open to cyber espionage and sabotage. We owe it to ourselves to learn from the experience of SolarWinds, for those who fail to learn from history are doomed to repeat it.

Mr. GUEST. Madam Speaker, I have no further speakers, and I urge Members to support this bill. I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield myself the balance of my time to close.

As the lead Federal agency for cybersecurity, DHS has taken steps to increase public awareness of software vulnerabilities routinely exploited by malicious cyber actors.

To identify and manage these types of vulnerabilities on its own network, DHS needs better visibility into the supply chains of the software it procures.

Enactment of H.R. 4611 would ensure that DHS has access to the information it needs to enhance its ability to manage the risks to its own networks.

I urge my colleagues to support H.R. 4611, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Mississippi (Mr. THOMPSON) that the House suspend the rules and pass the bill, H.R. 4611, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. POSEY. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

## DARREN DRAKE ACT

Mr. THOMPSON of Mississippi. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4089) to direct the Secretary of Homeland Security to develop and disseminate best practices for rental companies and dealers to report suspicious behavior to law enforcement agencies at the point of sale of a covered rental vehicle to prevent and mitigate acts of terrorism using motor vehicles, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4089

*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 ''Darren Drake Act''.*

***SEC. 2. BEST PRACTICES RELATED TO CERTAIN INFORMATION COLLECTED BY RENTAL COMPANIES AND DEALERS.***

*(a) DEVELOPMENT AND DISSEMINATION.—*

*(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall develop and disseminate best practices for rental companies and dealers to report suspicious behavior to law enforcement agencies at the point of sale of a covered rental vehicle.*

*(2) CONSULTATION; UPDATES.—The Secretary shall develop and, as necessary, update the best practices described in paragraph (1) after consultation with Federal, State, local, and Tribal law enforcement agencies and relevant transportation security stakeholders.*

*(3) GUIDANCE ON SUSPICIOUS BEHAVIOR.—The Secretary shall include, in the best practices developed under paragraph (1), guidance on defining and identifying suspicious behavior in a manner that protects civil rights and civil liberties.*

*(b) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the implementation of this section, including an assessment of—*

*(1) the impact of the best practices described in subsection (a) on efforts to protect the United States against terrorist attacks; and*

*(2) ways to improve and expand cooperation and engagement between—*

*(A) the Department of Homeland Security;*

*(B) Federal, State, local, and Tribal law enforcement agencies; and*

*(C) rental companies, dealers, and other relevant rental industry stakeholders.*

*(c) DEFINITIONS.—In this section:*

*(1) The terms ''dealer'' and ''rental company'' have the meanings given those terms in section 30102 of title 49, United States Code.*

*(2) The term ''covered rental vehicle'' means a motor vehicle that—*

*(A) is rented without a driver for an initial term of less than 4 months; and*

*(B) is part of a motor vehicle fleet of 35 or more motor vehicles that are used for rental purposes by a rental company.*

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from