

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New Mexico (Ms. TORRES SMALL) that the House suspend the rules and pass the bill, H.R. 4432, 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.

PROTECTING CRITICAL INFRASTRUCTURE AGAINST DRONES AND EMERGING THREATS ACT

Ms. TORRES SMALL of New Mexico. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4432) to require the Department of Homeland Security to prepare a terrorism threat assessment relating to unmanned aircraft 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. 4432

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 "Protecting Critical Infrastructure Against Drones and Emerging Threats Act".

SEC. 2. DRONE AND EMERGING THREAT ASSESSMENT.

(a) *IN GENERAL.*—Not later than 120 days after the date of enactment of this Act, the Under Secretary for Intelligence and Analysis of the Department of Homeland Security shall—

(1) *in consultation with other relevant officials of the Department, request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of unmanned aircraft systems and other emerging threats associated with such new technologies;*

(2) *in consultation with relevant officials of the Department and other appropriate agencies of the Federal Government, develop and disseminate a security threat assessment regarding unmanned aircraft systems and other emerging threats associated with such new technologies; and*

(3) *establish and utilize, in conjunction with the Chief Information Officer of the Department and other relevant entities, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, including by establishing a voluntary mechanism whereby critical infrastructure owners and operators may report information on emerging threats, such as the threat posed by unmanned aircraft systems.*

(b) *REPORT.*—Not later than one year after the date of the enactment of this Act, the Under Secretary for Intelligence and Analysis of the Department of Homeland Security shall prepare a threat assessment and report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the threat posed by unmanned aircraft systems, including information collected from critical infrastructure owners and operators and Federal, State, and local government agencies. Such assessment and report shall also include a classified plan to mitigate such threat, as appropriate.

(c) *DEFINITIONS.*—

(1) *CRITICAL INFRASTRUCTURE.*—The term "critical infrastructure" has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(2) *UNMANNED AIRCRAFT SYSTEM.*—The term "unmanned aircraft system" has the meaning given such term in section 331 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note; Public Law 112–95).

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New Mexico (Ms. TORRES SMALL) and the gentleman from Texas (Mr. CRENSHAW) each will control 20 minutes.

The Chair recognizes the gentlewoman from New Mexico.

GENERAL LEAVE

Ms. TORRES SMALL of New Mexico. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days 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 gentlewoman from New Mexico?

There was no objection.

Ms. TORRES SMALL of New Mexico. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, H.R. 4432, would require the Department of Homeland Security to take action and address an emerging threat to our Nation's security, the threat posed by unmanned aerial systems, or drones, to critical infrastructure.

Drone technology is far from new. However, as technology evolves, so do the capabilities of bad actors who may want to cause harm to the people of this country. We know the drones can be weaponized and used to carry out terrorist attacks, particularly on vulnerable, critical infrastructure. Earlier this fall, drones struck Saudi Arabian crude oil infrastructure, disrupting the production of 5.7 million barrels of oil per day and causing a spike in oil prices around the world.

In an evolving threat environment, understanding the threats that drones present to critical infrastructure here in the United States is critical to mitigating those threats.

Critical infrastructure owners and operators recognize the benefits of drone technology; many even put them to good use in their own businesses. Nevertheless, they do have concerns about the threats that unauthorized drones may pose to their facilities.

Currently, when a drone is detected in a facility's airspace, there is no DHS official agency to call. At the very least, owners and operators should be able to report unauthorized drone activity when they detect it.

H.R. 4432 would allow for information sharing between critical infrastructure owners and operators and DHS in several ways:

First, it would require DHS to establish a channel for the voluntary reporting information on drones, as well as other emerging threats, over a secure communications infrastructure developed in conjunction with the Department's Chief Information Officer.

Additionally, H.R. 4432, would mandate that the DHS' Under Secretary for Intelligence and Analysis develop and disseminate a threat assessment on unmanned aerial systems and other emerging threats associated with drone technology. This assessment would consider threat intelligence from Federal, State, local, and private-sector partners and would be prepared in consultation with other DHS components, like the Cybersecurity and Infrastructure Security Agency, that have relevant expertise.

Finally, H.R. 4432 would require DHS to report its findings to Congress within 1 year.

Collectively, this bill would require DHS to take the lead on understanding the threat that drones present to this Nation's critical infrastructure, while also creating an enduring mechanism for DHS to gather information on emerging threats, as they arise, from the owners and operators who stand on the front line of our defense.

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

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

Mr. Speaker, I rise in support of H.R. 4432, the Protecting Critical Infrastructure Against Drones and Emerging Threats Act.

In the wrong hands, unmanned aerial systems can pose a threat to the American people. At our borders, criminals are using drones to smuggle drugs and surveil law enforcement. Terrorists like ISIS have used them in the past to carry out attacks overseas.

We must do more to address this threat, and with this bill we do just that. H.R. 4432 protects the American people from the threat posed by these criminal drone operators.

□ 1630

This legislation requires the Under Secretary for Intelligence and Analysis at DHS to prepare an assessment of the threat from drones with information gathered from Federal, State, local, and private-sector partners.

This bill also requires DHS to establish a secure communications network to receive and analyze information on the threat and a voluntary mechanism for reporting threat information from owners and operators of critical infrastructure.

During committee consideration of this bill, I proposed an amendment to allow DHS to produce this information in a classified form, as appropriate. I am pleased that language was included in this legislation.

Mr. Speaker, I urge my colleagues to support this legislation.

Mr. Speaker, I urge adoption of the bill, and I yield back the balance of my time.

Ms. TORRES SMALL of New Mexico. Mr. Speaker, this is an important bill that will position DHS to address the threat that drones pose to critical infrastructure. This measure was previously introduced by my colleague

from Louisiana (Mr. RICHMOND) in the 115th Congress and passed the House by a voice vote.

Mr. Speaker, I hope my colleagues will do the same today, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New Mexico (Ms. TORRES SMALL) that the House suspend the rules and pass the bill, H.R. 4432, 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.

DRONE ORIGIN SECURITY ENHANCEMENT ACT

Ms. TORRES SMALL of New Mexico. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4753) to prohibit the Secretary of Homeland Security from operating or procuring foreign-made unmanned aircraft systems, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4753

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 “Drone Origin Security Enhancement Act”.

SEC. 2. PROHIBITION ON OPERATION OR PROCUREMENT OF FOREIGN-MADE UNMANNED AIRCRAFT SYSTEMS.

(a) PROHIBITION ON AGENCY OPERATION OR PROCUREMENT.—The Secretary of Homeland Security may not operate, provide financial assistance for, or enter into or renew a contract for the procurement of—

(1) an unmanned aircraft system (UAS) that—

(A) is manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country;

(B) uses flight controllers, radios, data transmission devices, cameras, or gimbals manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country;

(C) uses a ground control system or operating software developed in a covered foreign country or by a corporation domiciled in a covered foreign country; or

(D) uses network connectivity or data storage located in or administered by a corporation domiciled in a covered foreign country; or

(2) a system manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country for the detection or identification of covered unmanned aircraft systems.

(b) WAIVER.—The Secretary of Homeland Security may waive the prohibition under subsection (a) on a case by case basis by certifying in writing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate that the operation or procurement that is the subject of such a waiver is required—

(1) in the national interest of the United States;

(2) for counter-UAS surrogate testing and training; or

(3) for intelligence, electronic warfare, or information warfare operations, testing, analysis, and or training.

(c) DEFINITIONS.—In this section:

(1) COVERED FOREIGN COUNTRY.—The term “covered foreign country” means a country labeled as a strategic competitor in the “Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge” issued by the Department of Defense pursuant to section 113 of title 10, United States Code.

(2) COVERED UNMANNED AIRCRAFT SYSTEM.—The term “unmanned aircraft system” has the meaning given such term in section 331 of the FAA Modernization and Reform Act of 2012 (Public Law 112–95; 49 U.S.C. 44802 note).

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New Mexico (Ms. TORRES SMALL) and the gentleman from Texas (Mr. CRENSHAW) each will control 20 minutes.

The Chair recognizes the gentlewoman from New Mexico.

GENERAL LEAVE

Ms. TORRES SMALL of New Mexico. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days 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 gentlewoman?

There was no objection.

Ms. TORRES SMALL of New Mexico. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, first, I want to thank my colleague, Congressman CRENSHAW, for introducing this important legislation.

To help carry out its many missions, the Department of Homeland Security, DHS, relies on drones to improve situational awareness. Drones can be used to survey damage from natural disasters or monitor remote locations along the border, including in my district. If data collected by a DHS drone was to be stolen by a foreign government, it could jeopardize the national or homeland security.

Recent reports suggest that Chinese-manufactured drones, otherwise known as unmanned aircraft systems, in the American market might be compromised and used to send sensitive information to the Chinese Government. In response to these cybersecurity concerns, the Department of the Interior recently grounded all of its foreign-made drones. The DOD similarly banned the purchase and use of all commercial off-the-shelf drones, except under limited circumstances.

It is time for the DHS to take similar protective measures. H.R. 4753 would prohibit DHS from purchasing or using drone technology manufactured in certain foreign countries designated as strategic competitors by the National Defense Strategy. The legislation permits the use of such drone technology only when DHS notifies Congress that the technology is being used in a limited manner, such as counter-drone testing and training.

I am proud to be an original cosponsor of this bipartisan bill, grateful to

have joined Congressman CRENSHAW on this initiative, and pleased that it was reported out of committee by unanimous consent.

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

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

Mr. Speaker, the Department of Homeland Security is charged with protecting Americans here at home, and it is critical that the technologies used to carry out this mission are secure. The risk posed by certain foreign drone manufacturers is well documented and presents a national security threat.

Chinese-manufactured drones could provide a backdoor for the Chinese Government to access sensitive flight data from drones used by DHS. My bill, H.R. 4753, seeks to address this vulnerability.

The Cybersecurity and Infrastructure Security Agency has stated that these unmanned aircraft systems are a potential risk to an organization’s information and that drones could contain components that could compromise your data.

The potential for comprised data to fall into the hands of a foreign government should concern everyone. It threatens to disrupt the law enforcement and national security objectives of DHS.

My bill, the Drone Origin Security Enhancement Act, addresses the threat by prohibiting DHS from acquiring unmanned aircraft systems manufactured in a foreign country labeled a strategic competitor by the Department of Defense. This is similar to a prohibition included in the National Defense Authorization Act of 2019 for the military.

Simply put, my bill will ensure that DHS is not using drone equipment from a foreign government that our military already views as a threat.

Much like the Department of Defense, DHS and its components have a critical mission. The risk introduced into these missions by foreign-manufactured drones is not something that can be ignored. This legislation addresses this very real threat and will keep our adversaries from compromising the technology we use to keep Americans safe.

Mr. Speaker, I want to thank my colleague from New Mexico for her leadership on this bill. I urge my colleagues to pass H.R. 4753, and I yield back the balance of my time.

Ms. TORRES SMALL of New Mexico. Mr. Speaker, H.R. 4753 takes the much-needed step of protecting the Department of Homeland Security from cybersecurity threats associated with certain foreign-made drones.

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 gentlewoman from New Mexico (Ms. TORRES SMALL) that the House