Maritime Security Subcommittee, to require DHS to determine whether border barriers impact the proliferation of cross-border tunnels.

With DHS having dedicated nearly $9 million over the past decade to remediating and countering cross-border tunnel threats, DHS needs to know whether its wall agenda is driving more illicit cross-border tunnels.

Mr. Speaker, I urge my colleagues to support H.R. 6740, and I yield back the balance of my time.

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

Mr. Speaker, every day, we are seeing drugs coming in from Mexico, known or suspected terrorists, and dangerous opioids. We see fentanyl coming in from China into Mexico where they mix it with methamphetamines and heroin. It is really toxic, poisonous stuff. Fentanyl is so toxic that our canines die when they sniff it, yet that is being put into drugs coming across the U.S.-Mexico border into the United States to pollute and infect our children and our veterans. It is time for this to stop.

I hope that we will be able to take up, perhaps in November, our border security bill, which I think would go a long ways to getting this job done. In the meantime, this bill, I think, will go a long ways to stopping a very organized, sophisticated route of drugs, bad people, and bad things into the United States, and that is shutting down these tunnels.

Mr. Speaker, I urge support of 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 Texas (Mr. MCCAUL) that the House suspend the rules and pass the bill, H.R. 6740, 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

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6620) to require the Department of Homeland Security to prepare a threat assessment relating to 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. 6620

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.

(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 gentleman from Texas (Mr. MCCAUL) and the gentleman from Louisiana (Mr. RICHMOND) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include any extraneous materials on the bill under consideration.

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

There was no objection.

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

Mr. Speaker, I rise today in support of this legislation that will help protect the American people from threatening drones. Drones are being used to cross America more and more every year. News outlets use drones to capture footage for a breaking story. Photographers use them to take photos and videos at weddings, sporting events, and rock concerts. They also are used by law enforcement to help document crime scenes or assist with search and rescue operations. Those are all good things.

However, drones or other unmanned aerial systems can also pose a threat if they are controlled by terrorists or criminals. For example, ISIS used them to carry out attacks and conduct reconnaissance overseas. Here at home, criminals are using drones to smuggle drugs across our borders and surveil law enforcement. The FBI even disrupted a plot to attack the Pentagon with a drone loaded with grenades.

The threats we face from drones are constantly evolving as the technology becomes more accessible across the globe. We need to do more to confront these dangers.

This legislation requires the Under Secretary for Intelligence and Analysis at DHS to develop a drone threat assessment with information gathered from Federal, State, local, and private sector partners.

It also directs the Under Secretary to establish a secure communications infrastructure for receiving and analyzing such threat information.

Further, this bill sets up a voluntary mechanism for critical infrastructure owners and operators to report information on similar emerging threats.

Mr. Speaker, I thank Congressman RICHMOND and Congressman RATCLIFFE for their hard work on this issue. I think this bill will allow us to strengthen our intelligence gathering and stay one step ahead of our enemies.

I am pleased that the Senate and House were also able to include the Preventing Emerging Threats Act, legislation I introduced with Congressman CHABOT, in the FAA bill that will be on the floor tomorrow. This will give DHS the authority to counter drones in our airspace if they are determined to be a threat to national security.

This bill provides DHS and DOJ with the ability to act quickly and effectively when a drone poses a security risk to large-scale events, national security events, and government facilities.

Secretary Nielsen described this legislation as ''a critical step in enabling the Department to address this threat.''

Let's provide DHS with the tools it needs to confront these threats before they get worse.

Mr. Speaker, I urge my colleagues to support these bipartisan bills, and I reserve the balance of my time.

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE, HOUSE OF REPRESENTATIVES,
Washington, DC, September 21, 2018.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I write concerning H.R. 6620, the Protecting Critical Infrastructure Against Drones and Emerging Threats Act. This legislation includes matters that fall within the Rule X jurisdiction

of the Committee on Transportation and Infrastructure.

In order to expedite floor consideration of H.R. 6620, the Committee on Transportation and Infrastructure will forgo action on this bill. However, this is conditional on our mutual understanding that forgoing consideration of the bill would not prejudice the Committee with respect to the appointment of conferees or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation that fall within the Committee's Rule X jurisdiction. I request you urge the Speaker to name members of the Committee to any conference committee named to consider such provisions.

Please place a copy of this letter and your response acknowledging our jurisdictional interest in the Congressional Record during House Floor consideration of the bill. I look forward to working with the Committee on Homeland Security as the bill moves through the legislative process.

Sincerely,

BILL SHUSTER,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, September 21, 2018.

Hon. BILL SHUSTER,
Chairman, Committee on Transportation and Infrastructure, Washington, DC.

DEAR CHAIRMAN SHUSTER: Thank you for your letter regarding H.R. 6620, the ''Protecting Critical Infrastructure Against Drones and Emerging Threats Act.'' I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Transportation and Infrastructure will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Transportation and Infrastructure does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee.

I will insert copies of this exchange in the Congressional Record during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

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

Mr. Speaker, I rise in support of H.R. 6620, the Protecting Critical Infrastructure Against Drones and Emerging Threats Act.

Mr. Speaker, H.R. 6620 would require the Department of Homeland Security to take action to better understand and address an emerging threat posed by unmanned aerial systems—or drones—to our Nation's critical infrastructure.

These technologies are not new, but their applications have evolved rapidly in recent years. Some of these uses are important to keeping the public safe, growing our economy, and providing new ways to explore the world, including giving first responders better information in an emergency, for example. But, we also know that drones can be used for espionage, be weaponized, or even to carry out a terrorist attack.

My district in Louisiana has one of the Nation's highest concentrations of critical infrastructure, including pipelines, refineries, ports, airports, stadiums, and a wide range of other key assets and resources.

When I speak with critical infrastructure owners and operators, they recognize the benefits of drone technology. Many of them even put them to good use in their own businesses. At the same time, they are troubled by the risks posed by unknown, unauthorized drones operating over their facilities.

Over the past year, I have asked owners and operators what we in government can do to help them address this threat. What I heard is that, at a minimum, they need a way to report potentially dangerous drone activity to DHS when they detect it.

In a hearing this spring before the Cybersecurity and Infrastructure Protection Subcommittee, where I serve as ranking member, stakeholders from the chemical industry testified about this challenge on the record. They told us that when a facility detects a drone in their airspace, they aren't sure what to do about it, or even who to tell.

H.R. 6620 would address this gap in a few ways.

First, it would require DHS to establish a channel for reporting information on drones, as well as other emerging threats, securely, through a communications infrastructure, developed in conjunction with the Department's chief information officer.

This bill would also direct DHS's Under Secretary for Intelligence and Analysis to develop and disseminate a threat assessment on unmanned aerial systems and other emerging threats associated with drone technology. The assessment would be informed by Federal, State, local, and private sector partners, and prepared in consultation with other DHS components, like the National Protection and Programs Directorate, that have relevant expertise.

Finally, H.R. 6620 would require DHS to report its findings to Congress within 1 year.

Together, these provisions call on DHS to take a closer look at a significant threat to our Nation's critical infrastructure—the threat of drone-enabled attacks—while also creating an enduring mechanism for DHS to continue gathering information on emerging threats from the owners and operators who stand on the front line of defense.

Mr. Speaker, H.R. 6620 would direct the Department of Homeland Security to do more to understand, assess, and respond to the threat posed by drones, while also creating an avenue for two-way information sharing about emerging threats.

My bill creates a new channel for critical infrastructure owners and operators to report potentially dangerous drone activity in their airspace, and other new threats as they evolve. Creating a way for owners and operators to relay this information, on a voluntary basis, would give DHS access to better data and a more comprehensive view of the threat environment.

Before I yield back, I would like to also express support for a related provision in the FAA package that is expected to be considered tomorrow. It would allow DHS to research technologies to counter threats of unmanned aerial systems being exploited to carry out terrorism or dangerous activity.

Mr. Speaker, I urge my colleagues to support H.R. 6620, and I yield back the balance of my time.

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

Mr. Speaker, on September 11, a United Airlines flight was headed towards the Capitol. Thank God those heroes that day brought down that airliner in Shanksville, Pennsylvania, and this great building that we are standing in today was not destroyed with an image I don't think the American people could accept.

However, those terrorists are exploiting these drones. We have seen them in Iraq and Syria with explosives and chemical weapons. We have also disrupted plots for the use of drones against both the Pentagon and the United States Capitol. A drone, unlike an airplane, could hit the United States Capitol very quickly. We need to give the Department the tools and the authorities necessary to protect our American institutions.

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

Ms. JACKSON LEE. Mr. Speaker, I rise today in support of H.R. 6620, the Protecting Critical Infrastructure Against Drones and Emerging Threats Act.

This much needed measure would direct the Department of Homeland Security to complete a vulnerability assessment of the threat posed by Unmanned Air Systems (UAS) to our critical infrastructure assets.

The results of the assessment would be reported to Congress, providing policymakers with much needed information to better protect our critical infrastructure assets.

Unmanned Air Systems, or drones, hold great promise, and may one day change the world as we know it.

As the technology develops however, there is always the risk that malicious actors may seek to use it to cause harm or destruction.

Drones offer the ability for almost anyone to bypass most physical security measures of our critical infrastructure facilities.

These facilities, such as nuclear power plants and oil refineries, depend on physical security and access control to ensure that operations are secured and remain operational.

Drones could potentially allow a malicious actor to bypass the security of a facility, carry out an explosive or chemical attack, or conduct surveillance of prohibited areas.

At a time when our critical infrastructure assets are under constant attack, and have suffered serious breaches in recent years, we must take action to ensure that the ability of our citizens and the ability of federal agencies to carry out their duties are resilient.

As a long-time advocate of a government that works efficiently for the people, it is clear that current security practices protecting our critical infrastructure are neither sufficient nor consistent.

Without an honest effort to even get a obtain view of the security risks facing critical infrastructure assets we will continue to be increasingly vulnerable.

While conducting threat assessments like this will harden the security posture of the federal government and our critical infrastructure assets, we are still suffering from a shortage of workers with the requisite skills to secure them.

To address this, I have introduced the Cyber Security Education and Federal Workforce Enhancement Act (H.R. 1981), which would address our cyber workforce shortage by establishing an Office of Cybersecurity Education and Awareness within DHS which will focus on:

Recruiting information assurance, cybersecurity, and computer security professionals;

Providing grants, training programs, and other support for kindergarten through grade 12, secondary, and post-secondary computer security education programs;

Supporting guest lecturer programs in which professional computer security experts lecture computer science students at institutions of higher education;

Identifying youth training programs for students to work in part-time or summer positions at federal agencies; and

Developing programs to support underrepresented minorities in computer security fields with programs at minority-serving institutions, including Historically Black Colleges and Universities, Hispanic-serving institutions, Native American colleges, Asian-American institutions, and rural colleges and universities.

Mr. Speaker, government agencies and the owners of critical infrastructure alike continue to struggle to identify the factors and technologies that put them at risk.

In closing, Mr. Speaker, I urge all members to join me in voting to pass H.R. 6620, the ''Protecting Critical Infrastructure Against Drones and Emerging Threats Act''.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. MCCAUL) that the House suspend the rules and pass the bill, H.R. 6620.

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.

SECURE BORDER COMMUNICATIONS ACT

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6742) to amend the Homeland Security Act of 2002 to ensure that appropriate officers and agents of U.S. Customs and Border Protection are equipped with secure radios or other two-way communication devices, supported by system interoperability, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6742

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 ''Secure Border Communications Act''.

SEC. 2. SECURE BORDER COMMUNICATIONS.

(a) IN GENERAL.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.) is amended by adding at the end the following new section:

''SEC. 420. SECURE BORDER COMMUNICATIONS.

''(a) IN GENERAL.—The Secretary shall ensure that each U.S. Customs and Border Protection officer or agent, if appropriate, is equipped with a secure radio or other two-way communication device, supported by system interoperability, that allows each such officer or agent to communicate—

''(1) between ports of entry and inspection stations; and

''(2) with other Federal, State, Tribal, and local law enforcement entities.

''(b) U.S. BORDER PATROL AGENTS.—The Secretary shall ensure that each U.S. Border Patrol agent assigned or required to patrol in remote mission critical locations, and at border checkpoints, has a multi- or dual-band encrypted portable radio.

''(c) COMMERCIAL MOBILE BROADBAND CONNECTIVITY.—In carrying out subsection (b), the Secretary shall acquire radios or other devices with the option to connect to appropriate commercial mobile broadband networks for deployment in areas where such networks enhance operations and are cost effective.

''(d) EMERGING COMMUNICATIONS TECHNOLOGIES CONSIDERED.—In carrying out this section, the Secretary may evaluate new or emerging communications technologies to determine their suitability for the unique conditions of border security operations.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 419 the following new item:

''Sec. 420. Secure border communications.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. MCCAUL) and the gentleman from Louisiana (Mr. RICHMOND) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include any extraneous materials on the bill under consideration.

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

There was no objection.

□ 1445

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

Mr. Speaker, I rise today in support of the Secure Border Communications Act.

Every day our CBP agents and officers serve on the front lines in the fight to secure our homeland. They face threats from armed drug cartels, dangerous gangs like MS–13, human traffickers, and potential terrorists.

These brave individuals take pride in serving with vigilance, integrity, and professionalism in order to keep us safe.

To be successful, however, they must be equipped with the tools they need to do their jobs well. Too often, the communications devices and radios used by CBP officers and other agents are outdated and unreliable.

For instance, Border Patrol agents patrolling on the ground may not have direct radio contact with CBP air assets or other law enforcement officers working the area. This hinders interagency communications and jeopardizes their mission and safety.

At a subcommittee hearing earlier this year, a Border Patrol agent stated that she had been issued a radio that often failed. At times, she would need to communicate with a fellow agent but was forced to use her personal cell phone.

We cannot allow these kinds of technical failures to endanger the lives of our agents and weaken our national security. We must do better.

Fortunately, we can begin to fix this problem today. This legislation will ensure that CBP agents and officers are equipped with interoperable and secure radios or two-way communication devices.

In addition, this bill highlights the importance of reliable encrypted communications that will prevent powerful cartels from intercepting sensitive information, such as our CBP agents' and officers' locations.

Passing this bill is a simple step that we can take to help our CBP agents do their jobs and protect our homeland.

I would like to thank Congressman MAST for all his hard work on this issue. Congressman MAST is no stranger to service and sacrifice, serving overseas in our wars in Iraq and Afghanistan, and he has the scars to prove it. We thank him for his service. It is a great honor to have him sponsor a bill from our committee.

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

COMMITTEE ON WAYS AND MEANS,
HOUSE OF REPRESENTATIVES,
Washington, DC, September 24, 2018.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I write to you regarding H.R. 6742, the ''Secure Border Communications Act'', on which the Committee on Ways and Means was granted an additional referral.

As a result of your having consulted with us on provisions in H.R. 6742 that fall within the Rule X jurisdiction of the Committee on Ways and Means, I agree to waive formal consideration of this bill. The Committee on Ways and Means takes this action with the mutual understanding that we do not waive any jurisdiction over the subject matter contained in this or similar legislation, and the Committee will be appropriately consulted and involved as the bill or similar legislation moves forward so that we may address any remaining issues that fall within our jurisdiction. The Committee also reserves the right to seek appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, and requests your support for such request.