May all that is done this day be for Your greater honor and glory.

Amen.

THE JOURNAL

The SPEAKER pro tempore. The Chair has examined the Journal of the last day's proceedings and announces to the House his approval thereof.

Pursuant to clause 1, rule I, the Journal stands approved.

PLEDGE OF ALLEGIANCE

The SPEAKER pro tempore. Will the gentlewoman from the District of Columbia (Ms. NORTON) come forward and lead the House in the Pledge of Allegiance.

Ms. NORTON led the Pledge of Allegiance as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

CAMERAS IN THE UNITED STATES SUPREME COURT

(Mr. POE of Texas asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. POE of Texas. Mr. Speaker, it is time to remove the veil of secrecy from the hallowed halls of the Supreme Court.

Americans have the right to watch the proceedings in person, but only 50 members of the public can get into the small courtroom at a time.

Technology allows discreet videoing, but for some reason, there are those who want to keep these proceedings hidden from the American public.

We have the best judicial system ever created. We should not hide it.

Cameras should be allowed in the most important court in the world.

I know cameras can be placed in a courtroom without disruption or distraction, because I did it. For 22 years, I served as a felony court judge in Houston, Texas. I heard over 25,000 criminal cases and nearly 1,000 jury trials, and many of those were filmed by the television media.

Justice would be better served if the black robe of secrecy was removed from the United States Supreme Court and the proceedings were filmed. Because justice is the one thing we should always find in America.

And that is just the way it is.

WHY HAS JUDGE KAVANAUGH NOT REQUESTED AN FBI INVESTIGATION

(Ms. NORTON asked and was given permission to address the House for 1 minute and to revise and extend her remarks.)

Ms. NORTON. Mr. Speaker, although the Republican Senate has refused the customary FBI investigation into allegations against Judge Kavanaugh by Dr. Ford and others, there is evidence that should be weighed.

Dr. Ford is not only willing to offer sworn testimony at the hearing, she has requested an FBI investigation with the required FBI questioning under penalty of perjury.

Judge Kavanaugh is an expert on all our legal processes. Why hasn't he asked for the standard FBI investigation?

Moreover, apparently understanding the seriousness of her allegations, Dr. Ford has also taken the unusual step of being polygraphed. A lie detector test is not required, although law enforcement sometimes requests it.

It would be a fair question for Senators to ask Judge Kavanaugh why he did not request an FBI investigation and whether he would take a polygraph test, too.

CELEBRATING 100TH BIRTHDAY OF WALTER ''STICKY'' BURCH

(Mr. BUDD asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. BUDD. Mr. Speaker, I rise today to recognize Walter ''Sticky'' Burch, who is going to be 100 years old on October 21. And that is a great day, Mr. Speaker. It is also my birthday, although mine is just a few years after his.

Walter Burch was born in Asheville but grew up in Greensboro and spent much of his life serving in the Greensboro Police Department. His service to our Nation began just 9 days after the bombing of Pearl Harbor.

During the Second World War, he helped gather intelligence on enemy operations in Europe, but his service to his country did not end there.

Walter returned home and joined the police department, where he served for nearly 50 years.

He officially retired in 1981, but he ran for sheriff just a few years later. He went on to serve two terms as the sheriff of Guilford County.

Since retiring from law enforcement, Walter has remained deeply involved in our community, and the people of Guilford County are lucky to have him.

Mr. Speaker, please join me in celebrating the 100th birthday of Walter ''Sticky'' Burch and his lifelong commitment to public service.

COMMUNICATION FROM THE CLERK OF THE HOUSE

The SPEAKER pro tempore laid before the House the following communication from the Clerk of the House of Representatives:

OFFICE OF THE CLERK,
HOUSE OF REPRESENTATIVES,
Washington, DC, September 25, 2018.

Hon. PAUL D. RYAN,
The Speaker, House of Representatives, Washington, DC.

DEAR MR. SPEAKER: Pursuant to the permission granted in Clause 2(h) of Rule II of the Rules of the U.S. House of Representatives, the Clerk received the following message from the Secretary of the Senate on September 25, 2018, at 11:49 a.m.:

That the Senate passed without amendment H.R. 2259.

With best wishes, I am,

Sincerely,

KAREN L. HAAS.

COMMUNICATION FROM THE DEMOCRATIC LEADER

The SPEAKER pro tempore laid before the House the following communication from the Honorable NANCY PELOSI, Democratic Leader:

SEPTEMBER 24, 2018.

Hon. PAUL D. RYAN,
Speaker of the House of Representatives, U.S. Capitol, Washington, DC.

DEAR SPEAKER RYAN: Pursuant to Section 1652(b) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232), I am pleased to appoint the following Member to serve as a Commissioner to the Cyberspace Solarium Commission:

The Honorable James Langevin of Rhode Island

And from private life:

The Honorable Patrick Murphy of Bristol, Pennsylvania

Thank you for your attention to these recommendations.

Sincerely,

NANCY PELOSI,
Democratic Leader.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which a recorded vote or the yeas and nays are ordered, or votes objected to under clause 6 of rule XX.

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

PUBLIC-PRIVATE CYBERSECURITY COOPERATION ACT

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6735) to direct the Secretary of Homeland Security to establish a vulnerability disclosure policy for Department of Homeland Security internet websites, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6735

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 ''Public-Private Cybersecurity Cooperation Act''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY DISCLOSURE OF SECURITY VULNERABILITIES.

(a) VULNERABILITY DISCLOSURE POLICY.—The Secretary of Homeland Security shall establish a policy applicable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of Department of Homeland Security. Such policy shall include each of the following:

(1) The appropriate information systems of the Department that individuals, organizations, and companies may use to discover and report security vulnerabilities on appropriate information systems.

(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

(4) The ways in which the Department may communicate with individuals, organizations, and companies that report security vulnerabilities.

(5) The process the Department shall use for public disclosure of reported security vulnerabilities.

(b) REMEDIATION PROCESS.—The Secretary of Homeland Security shall develop a process for the Department of Homeland Security to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (a).

(c) CONSULTATION.—In developing the security vulnerability disclosure policy under subsection (a), the Secretary of Homeland Security shall consult with each of the following:

(1) The Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the policy developed under subsection (a) are protected from prosecution under section 1030 of title 18, United States Code, civil lawsuits, and similar provisions of law with respect to specific activities authorized under the policy.

(2) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

(3) Non-governmental security researchers.

(d) PUBLIC AVAILABILITY.—The Secretary of Homeland Security shall make the policy developed under subsection (a) publicly available.

(e) SUBMISSION TO CONGRESS.—

(1) DISCLOSURE POLICY AND REMEDIATION PROCESS.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a copy of the policy required under subsection (a) and the remediation process required under subsection (b).

(2) REPORT AND BRIEFING.—

(A) REPORT.—Not later than one year after establishing the policy required under subsection (a), the Secretary of Homeland Security shall submit to Congress a report on such policy and the remediation process required under subsection (b).

(B) ANNUAL BRIEFINGS.—One year after the date of the submission of the report under subparagraph (A), and annually thereafter for each of the next three years, the Secretary of Homeland Security shall provide to Congress a briefing on the policy required under subsection (a) and the process required under subsection (b).

(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the briefings required under subparagraph (B) shall include each of the following with respect to the policy required under subsection (a) and the process required under subsection (b) for the period covered by the report or briefing, as the case may be:

(i) The number of unique security vulnerabilities reported.

(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of such vulnerabilities.

(f) DEFINITIONS.—In this section:

(1) The term ''security vulnerability'' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)), in information technology.

(2) The term ''information system'' has the meaning given that term by section 3502(12) of title 44, United States Code.

(3) The term ''appropriate information system'' means an information system that the Secretary of Homeland Security selects for inclusion under the vulnerability disclosure policy required by subsection (a).

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 within 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 as much time as I may consume.

Mr. Speaker, I rise today in support of the Public-Private Cybersecurity Cooperation Act.

Strengthening our cybersecurity must be a top national priority. International hackers and nation-states are waging a war against us in cyberspace.

These threats are aimed at our economic, political, and national security institutions.

Between 2011 and 2013, Iranian hackers attacked dozens of American banks and even tried to shut down a dam in New York.

In 2014, Chinese hackers stole over 22.5 million security clearances, including my own, from the Office of Personnel Management.

In 2016, Russia meddled in our presidential election.

Because we use computer networks in our personal and professional lives, almost everyone is a target.

With each passing day, cyber threats continue to grow, but the government cannot face these threats alone. We need help from the private sector.

Today's legislation will direct the Department of Homeland Security Secretary to develop and implement a vulnerability disclosure program that will allow threat researchers from the private sectors to identify and report cybersecurity flaws found in the Department's information systems.

Currently, there is no legal avenue that allows them to do so. This legislation solves that problem.

Mr. Speaker, I would like to thank Leader MCCARTHY for his years of commitment to innovation and cybersecurity, and for his work on this bill in particular.

He truly understands the nature of this threat and why it is so important to have a strong cyber partnership between the public and private sectors.

Mr. Speaker, I believe that this bipartisan legislation will help DHS better protect its vital networks, and I urge my colleagues to support it.

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

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

Mr. Speaker, I rise in support of H.R. 6735, the Public-Private Cybersecurity Cooperation Act.

Mr. Speaker, protecting our Federal information systems is an enormous task.

As ranking member of the Cybersecurity and Infrastructure Protection Subcommittee, I hear more often than I would like about the challenges of recruiting and maintaining the Federal cyber workforce. That is true even at the Department of Homeland Security.

As DHS works to address ongoing workforce challenges, we have to think creatively and leverage untapped resources of talent.

Across the country, there are white hat hackers who want to apply their considerable cyber skills to report vulnerabilities found on government information systems to Federal authorities. But today, these ethical hackers cannot research and report bugs on DHS' systems without being in violation of the Computer Fraud and Abuse Act.

In 2016, the Department of Defense piloted Hack the Pentagon, which gave white hat hackers 24 days to find unique vulnerabilities in certain DOD information systems and report them for a reward.

The program was so successful, DOD established a permanent vulnerability disclosure program to allow ethical hackers to search for and report bugs on DOD information systems without violating the law.

That program has enjoyed similar success to Hack the Pentagon.

Members of the Homeland Security Committee have been urging DHS to establish a vulnerability disclosure program for several years.

At a hearing with Secretary Nielsen in April, my colleague on the Cybersecurity Subcommittee, Mr. LANGEVIN, asked the Secretary whether the Department had in place a mechanism for vulnerabilities to be reported. Secretary Nielsen testified that the Department had no clear process in place to accept information about bugs in DHS information systems and agreed to work with the committee to establish one.

Five months have passed, and the Department is not any closer to establishing a vulnerability disclosure program of its own.

Vulnerability disclosure programs are an emerging industry best practice and are recommended by the updated NIST Cybersecurity Framework.

White hat hackers are an enormous pool of talent that the Federal Government has largely failed to leverage. DHS can no longer afford to leave that kind of talent on the table.

H.R. 6735 would push DHS in the right direction by requiring it to put in place policies to ensure that civic-minded hackers can research and report bugs found on certain information systems without breaking the law.

Before I close, I would like to express my disappointment that S. 1281, the Hack DHS Act, is not being considered on the floor today.

S. 1281, which would create a bug bounty pilot program at DHS, was approved by voice vote in the committee and is consistent with the objectives of H.R. 6735, which I support.

□ 1415

It is unclear why S. 1281 is not being considered today. I urge House leadership to bring S. 1281 to the floor later this fall.

Mr. Speaker, I urge my colleagues to support H.R. 6735. In the current security environment, vulnerability disclosure policies have emerged as a critical component of cybersecurity without any organization. DHS is the lead Federal Department charged with securing government civilian networks.

DHS should be leading by example, not playing catchup. Today, the Department of Defense and the GSA have vulnerability disclosure programs in operation. It is time for DHS to join them.

Mr. Speaker, I urge my colleagues to support H.R. 6735, and I yield back the balance of my time.

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

Mr. Speaker, I once again urge my colleagues to support this bill. It is at a time when there is a lot of partisanship going on. I think it is healthy to see a truly bipartisan bill on such an important issue regarding our national security.

I think, as the gentleman from Louisiana pointed out, this is modeled after a program that the Department of Defense successfully deployed, and I am proud of the record my committee has had on passing, I think, close to 110 bills now, and almost all of them are bipartisan.

Mr. Speaker, I urge my Senate colleagues to at least take up some of them and do the same, 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. 6735, 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. MCCAUL. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this question will be postponed.

The point of no quorum is considered withdrawn.

BORDER TUNNEL TASK FORCE ACT

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6740) to amend the Homeland Security Act of 2002 to establish Border Tunnel Task Forces, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6740

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 ''Border Tunnel Task Force Act''.

SEC. 2. BORDER TUNNEL DETECTION.

(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. BORDER TUNNEL TASK FORCES.

''(a) ESTABLISHMENT.—The Secretary shall establish Border Tunnel Task Forces in jurisdictions in which such Border Tunnel Task Forces can contribute to border security missions after evaluating—

''(1) whether the areas in which such Border Tunnel Task Forces would be established are significantly impacted by cross-border threats; and

''(2) the availability of Federal, State, local, and Tribal law enforcement resources to participate in such Border Tunnel Task Forces.

''(b) PURPOSE.—The purpose of the Border Tunnel Task Forces under subsection (a) is to enhance and integrate border security efforts by addressing and reducing cross-border tunnel related threats and violence by—

''(1) facilitating collaboration among Federal, State, local, and Tribal law enforcement agencies to execute coordinated activities in furtherance of border security and homeland security; and

''(2) enhancing information-sharing, including the dissemination of homeland security information, among such agencies.

''(c) COMPOSITION AND ESTABLISHMENT OF BORDER TUNNEL TASK FORCES.—Border Tunnel Task Forces may be comprised of the following:

''(1) Personnel from U.S. Customs and Border Protection, including the U.S. Border Patrol.

''(2) Personnel from U.S. Immigration and Customs Enforcement, including Homeland Security Investigations.

''(3) Personnel from other Department components and offices, as appropriate.

''(4) Personnel from other Federal, State, local, and Tribal law enforcement agencies, as appropriate.

''(5) Other appropriate personnel at the discretion of the Secretary.

''(d) DUPLICATION OF EFFORTS.—In determining whether to establish a new Border Tunnel Task Force or to expand an existing Border Tunnel Task Force in a given jurisdiction, the Secretary shall ensure that the Border Tunnel Task Force under consideration does not unnecessarily duplicate the efforts of other existing interagency task forces or centers within such jurisdiction.

''(e) COORDINATION AMONG COMPONENTS.—The Secretary shall—

''(1) establish targets and performance measures for the Border Tunnel Task Forces that include consideration of whether border barriers impact cross-border tunnel threats;

''(2) direct leadership of each Border Tunnel Task Force to monitor progress on such targets and performance measures for each such task force; and

''(3) periodically report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate regarding progress on such targets and performance measures.''.

(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. Border Tunnel Task Forces.''.

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 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 the Border Tunnel Task Force Act.

Mr. Speaker, some of the most dangerous threats to our homeland are coming across our southern border. Drug smugglers are bringing dangerous narcotics and fueling America's epidemic of opioids. Human traffickers and transnational gangs like MS–13 are infecting our neighborhoods and endangering our kids. Even potential known or suspected terrorists are trying to make their way into America by exploiting our weak borders.

All of these groups are a serious national security concern. They are also very determined and creative, and one of the ways they avoid detection is by digging cross-border tunnels.

In August, a tunnel the length of two football fields was discovered below a closed fast-food restaurant in Arizona. This pathway was used to smuggle cocaine, heroin, fentanyl, and methamphetamines.

In 2016, 7 tons of marijuana and 1 ton of cocaine were found in a tunnel not far from San Diego. In my home State of Texas, a tunnel was discovered under the Rio Grande in El Paso back in 2010, also for smuggling drugs.

Unfortunately, the problem is not new. Authorities have discovered nearly 200 cross-border tunnels since 1990. We must do more to shut these tunnels down. This legislation will establish Border Tunnel Task Forces to enhance the ability of DHS to detect these tunnels and identify criminal networks.

These teams will be made up of ICE, CBP, and other Department personnel. They will be assisted by State, local, and Tribal law enforcement agencies. These teams will deploy to locations along the border where the greatest