As a Senior Member on the House Committee on Homeland Security who sits on the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, I know well of the need to encourage and train women to thrive in the Science, Technology, Engineering, and Mathematics (STEM) fields.

Promoting diversity in the STEM professions is more than just an idea; it requires an understanding that there is a need to have a process that will ensure the inclusion of all minorities and women in all areas of American life.

Studies have found that women make up almost 50 percent of the workforce.

Studies note that 23 percent of STEM workers are women; however, women make up 48 percent of workers in all occupations.

Only 26 percent of women who do attain degrees in STEM fields work in STEM jobs.

According to the most recent available data women are less likely to focus on the STEM disciplines in undergraduate and graduate studies.

In 1991, women received 29.6 percent of computer science B.A.'s, compared to just 18.2 percent in 2010.

Jobs in computer systems design and related services, a field dependent upon high-level math and problem-solving skills, are projected to grow 45 percent between 2008 and 2018.

There are approximately 6 million women and minority owned businesses in the United States, representing a significant aspect of our economy.

My home city of Houston, Texas, the energy capital of the world, knows the importance of professionals in the STEM industries.

It has been reported that the highest-paying STEM occupations are petroleum engineers with an annual salary of $147,520, architectural and engineering managers with an annual salary of $138,720, natural sciences managers with an annual salary of $136,450, computer and information systems managers with an annual salary of $136,280, and physicists with a reported annual salary of $117,300.

There is an increasing demand for individuals with STEM degrees to extend their focus beyond the laboratory so they can be leaders in discovery and commercialization.

Women deserve a fair shot in the STEM programs in this nation.

In addition, I believe that work needs to be done to modernize key contracting developmental programs designed to increase opportunities for women, minorities and low-income individuals who pursue STEM degrees and STEM job training.

I support programs at the National Science Foundation that have worked to reduce the current barriers and ensure women have the support they need in the STEM fields.

Mr. Speaker, we should encourage women to pursue degrees and careers in the STEM fields so we can continue to compete in the global economy.

The SPEAKER pro tempore (Mr. MARCHANT). The question is on the motion offered by the gentlewoman from Virginia (Mrs. COMSTOCK) that the House suspend the rules and pass the bill, H.R. 255.

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.

SUPPORT FOR RAPID INNOVATION ACT OF 2017

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 239) to amend the Homeland Security Act of 2002 to provide for innovative research and development, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 239

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 ''Support for Rapid Innovation Act of 2017''.

SEC. 2. CYBERSECURITY RESEARCH AND DEVELOPMENT PROJECTS.

(a) CYBERSECURITY RESEARCH AND DEVELOPMENT.—

(1) IN GENERAL.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

''SEC. 321. CYBERSECURITY RESEARCH AND DEVELOPMENT.

''(a) IN GENERAL.—The Under Secretary for Science and Technology shall support the research, development, testing, evaluation, and transition of cybersecurity technologies, including fundamental research to improve the sharing of information, analytics, and methodologies related to cybersecurity risks and incidents, consistent with current law.

''(b) ACTIVITIES.—The research and development supported under subsection (a) shall serve the components of the Department and shall—

''(1) advance the development and accelerate the deployment of more secure information systems;

''(2) improve and create technologies for detecting attacks or intrusions, including real-time continuous diagnostics and real-time analytic technologies;

''(3) improve and create mitigation and recovery methodologies, including techniques and policies for real-time containment of attacks, and development of resilient networks and information systems;

''(4) support, in coordination with non-Federal entities, the review of source code that underpins critical infrastructure information systems;

''(5) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies;

''(6) assist the development and support of technologies to reduce vulnerabilities in industrial control systems; and

''(7) develop and support cyber forensics and attack attribution capabilities.

''(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate activities with—

''(1) the Under Secretary appointed pursuant to section 103(a)(1)(H);

''(2) the heads of other relevant Federal departments and agencies, as appropriate; and

''(3) industry and academia.

''(d) TRANSITION TO PRACTICE.—The Under Secretary for Science and Technology shall support projects carried out under this title through the full life cycle of such projects, including research, development, testing, evaluation, pilots, and transitions. The Under Secretary shall identify mature technologies that address existing or imminent cybersecurity gaps in public or private information systems and networks of information systems, identify and support necessary improvements identified during pilot programs and testing and evaluation activities, and introduce new cybersecurity technologies throughout the homeland security enterprise through partnerships and commercialization. The Under Secretary shall target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within two years and that is expected to have a notable impact on the public or private information systems and networks of information systems.

''(e) DEFINITIONS.—In this section:

''(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in section 227.

''(2) HOMELAND SECURITY ENTERPRISE.—The term 'homeland security enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

''(3) INCIDENT.—The term 'incident' has the meaning given such term in section 227.

''(4) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in section 3502(8) of title 44, United States Code.''.

(2) 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 the second section 319 the following new item:

''Sec. 321. Cybersecurity research and development.''.

(b) RESEARCH AND DEVELOPMENT PROJECTS.—Section 831 of the Homeland Security Act of 2002 (6 U.S.C. 391) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking ''2016'' and inserting ''2021'';

(B) in paragraph (1), by striking the last sentence; and

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

''(3) PRIOR APPROVAL.—In any case in which the head of a component or office of the Department seeks to utilize the authority under this section, such head shall first receive prior approval from the Secretary by providing to the Secretary a proposal that includes the rationale for the utilization of such authority, the funds to be spent on the use of such authority, and the expected outcome for each project that is the subject of the use of such authority. In such a case, the authority for evaluating the proposal may not be delegated by the Secretary to anyone other than the Under Secretary for Management.'';

(2) in subsection (c)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking ''2016'' and inserting ''2021''; and

(B) by amending paragraph (2) to read as follows:

''(2) REPORT.—The Secretary shall annually submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report detailing the projects for which the authority granted by subsection (a) was utilized, the rationale for such utilizations, the funds spent utilizing such authority, the extent of cost-sharing for such projects among Federal and non-Federal sources, the extent to which utilization of such authority has addressed a homeland security capability gap or threat to the homeland identified by the Department, the total

amount of payments, if any, that were received by the Federal Government as a result of the utilization of such authority during the period covered by each such report, the outcome of each project for which such authority was utilized, and the results of any audits of such projects.''; and

(3) by adding at the end the following new subsection:

''(e) TRAINING.—The Secretary shall develop a training program for acquisitions staff on the utilization of the authority provided under subsection (a).''.

(c) NO ADDITIONAL FUNDS AUTHORIZED.—No additional funds are authorized to carry out the requirements of this Act and the amendments made by this Act. Such requirements shall be carried out using amounts otherwise authorized.

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

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. RATCLIFFE. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and to include any extraneous material 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. RATCLIFFE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I am very pleased to bring two important bills to the floor today that strengthen the government's ability to effectively leverage cutting-edge cyber technologies. Last year, the House passed both of these provisions as part of Majority Leader MCCARTHY's Innovation Initiative, and I am excited that we are able to bring them to the floor here so early in the 115th Congress.

Mr. Speaker, over the past 2 years, my colleagues and I have been working diligently with technology innovators and tech startups to find solutions that will spur innovation and break down the bureaucratic barriers that prevent the government from effectively leveraging the private sector's emerging technologies.

H.R. 239, the Support for Rapid Innovation Act of 2017, addresses this problem by requiring the science and technology directorate, or S&T, to more effectively coordinate with industry and academia to support the research and development of cybersecurity technologies.

H.R. 239 does so because it requires S&T to support the full life cycle of cyber research and development projects and identify mature technologies to address cybersecurity gaps. In doing so, S&T will be required to target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within 2 years.

This bill will also extend the use of other transactional authority, or OTA, until the year 2021, a move that will improve DHS's ability to engage with tech startups that are developing these cutting-edge technologies. H.R. 239 also includes additional accountability requirements to ensure that there is proper oversight of the authority.

Mr. Speaker, our digital borders are constantly being barraged by cybercriminals, by nation-states, and by terrorists seeking to exploit and harm innocent Americans. Almost daily, we read news stories on how these hackers are intruding into our networks and doing so with increased sophistication. One thing is for certain, we have seen that cyber intrusions and their impact on victims quickly morph and increase both in frequency and in their severity.

In 2017, these hackers will unfortunately continue to pose a great threat to the U.S. homeland and to our critical infrastructure. The Federal Government, therefore, needs to keep pace with these evolving threats by more actively working with the private sector to find effective solutions.

DHS's Directorate of Science and Technology is the primary research and development arm of the Department. The directorate manages basic and applied research and development, including cybersecurity R&D, for the Department's operational components and for our first responders.

Ensuring there are mechanisms in place, like S&T's cybersecurity R&D programs and the OTA, to support the dynamic nature of cybersecurity research and development is essential for addressing homeland security capability gaps.

Thank you again, Mr. Speaker, for calling up this important bill today. I believe it will have an incredibly positive impact on encouraging technology innovation across the Nation to address our vital homeland security needs.

Mr. Speaker, I urge all Members to join me in supporting this very important bill.

I reserve the balance of my time.

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, DC, January 9, 2017.

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

DEAR MR. CHAIRMAN: I am writing concerning H.R. 239, the ''Support for Rapid Innovation Act of 2017,'' which was introduced on January 4, 2017.

H.R. 239 contains provisions within the Committee on Science, Space, and Technology's Rule X jurisdiction. In order to expedite this bill for floor consideration, the Committee on Science, Space, and Technology will forego action on the bill. This is being done on the basis of our mutual understanding that doing so will in no way diminish or alter the jurisdiction of the Committee on Science, Space, and Technology with respect to the appointment of conferees, or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation.

I would appreciate your response to this letter confirming this understanding, and would request that you include a copy of this letter and your response in the Congressional Record during the floor consideration of this bill. Thank you in advance for your cooperation.

Sincerely,

LAMAR SMITH,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, January 10, 2017.

Hon. LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology, Washington, DC.

DEAR CHAIRMAN SMITH: Thank you for your letter regarding H.R. 239, the ''Support for Rapid Innovation Act of 2017.'' I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Science, Space, and Technology will not seek a sequential referral on the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing a sequential referral of this bill at this time, the Committee on Science, Space, and Technology 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 a request by the Committee on Science, Space, and Technology for conferees on those provisions within your jurisdiction.

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. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume. I rise in support of H.R. 239, the Support for Rapid Innovation Act.

Mr. Speaker, this timely legislation authorizes the Department of Homeland Security to support cybersecurity research and development and to help innovators with promising cybersecurity technologies to help commercialize their products.

Government and private sector networks are under constant attack by increasingly sophisticated cyber hackers. The cyber hacking campaign carried out by the Russian Government against U.S. political and business institutions, during the 2016 election, is a recent, high-profile example.

Concern has also been growing about the threat of cybercriminals carrying out attacks by exploiting unprotected Internet-enabled consumer products. This threat was brought into sharp focus last October with the denial of service attack against Dyn. During that attack, malware was used to direct tens of thousands of Internet-connected cameras, DVRs, and other consumer products to carry out successive, highly sophisticated attacks.

Our adversaries are constantly innovating. It is imperative that the Federal Government—and specifically DHS—innovate, too. To that end, H.R. 239 directs DHS to invest in innovative cybersecurity technologies and provide DHS with flexibility to overcome bureaucratic obstacles that sometimes

discourage smaller companies, like tech startups, from working with the Federal Government.

H.R. 239 directs DHS to pursue cybersecurity projects that will improve detection, mitigation, and recovery from attacks and bolster the security and resilience of our networks, particularly for critical infrastructure.

Mr. Speaker, I urge my colleagues to support this bipartisan legislation to ensure that DHS does its part to advance cybersecurity research and development.

Cybersecurity threats to our Nation are growing in diversity and sophistication. We cannot afford to let promising technologies languish.

The Department of Homeland Security should work with the private sector in support of innovative cybersecurity research, development, testing, and evaluation. We have seen that public-private collaboration can give these technologies the boost they need to enter the market. Just last month, DHS announced the commercialization of an eight cybersecurity product launched with the help of the Department's Transition to Practice program.

I urge my colleagues to support H.R. 239.

I yield back the balance of my time.

Mr. RATCLIFFE. Mr. Speaker, I thank Ranking Member THOMPSON for his leadership on the committee, and I want to thank the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee staff for their hard work.

Once again, I urge my colleagues to support H.R. 239.

I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 239, the "Support for Rapid Innovation Act of 2017," which amends the Homeland Security Act of 2002 to provide for improved innovative research and development.

I support this bill because it would extend the Department of Homeland Security secretary's pilot program for research and development projects and prototype projects through 2020.

This bill would require the secretary to report annually to the House Homeland Security and Science committees and the Senate Homeland Security Committee on the dynamics of the projects undertaken.

Specifically, H.R. 239 would amend the Homeland Security Act of 2002 to include fundamental improvements to facilitate information, analytics, and methodologies related to cybersecurity risks and incidents, consistent with the current law.

In particular, it adds a new section to the Homeland Security Act, directing the Department of Homeland Security to support—whether within itself, other agencies, or in academia and private industry—the research and development of cybersecurity-related technologies.

As a senior member of the Homeland Security Committee and Ranking Member of the Judiciary Committee and Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, I support this bill as it directs the Under Secretary for Science and Technology to bolster research and development, along with the testing and evaluation of cybersecurity technology to improve the sharing of information, analysis, and methodologies related to cybersecurity risks and incidents.

The Rapid Innovation Act is a smart bill that will enable the Department of Homeland Security to establish and improve technologies for detecting attacks or intrusions.

The "Support for Rapid Innovation Act of 2017" will equip the Department of Homeland Security with vital tools and resources to prevent and remove attacks and threats implemented by those who target our nation.

Mr. Speaker, we face growing cybersecurity threats, which demands that we increase research and development, along with the testing and evaluation of cybersecurity technology to expand the sharing of information, analysis, and methodologies related to cybersecurity risks and incidents.

This is a comprehensive bill that will help protect all Americans in every corner of this nation.

I urge all Members to join me in voting to pass H.R. 239.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. RATCLIFFE) that the House suspend the rules and pass the bill, H.R. 239, 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.

LEVERAGING EMERGING TECHNOLOGIES ACT OF 2017

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 240) to encourage engagement between the Department of Homeland Security and technology innovators, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 240

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 ''Leveraging Emerging Technologies Act of 2017''.

SEC. 2. INNOVATION ENGAGEMENT.

(a) INNOVATION ENGAGEMENT.—

(1) IN GENERAL.—The Secretary of Homeland Security—

(A) shall engage with innovative and emerging technology developers and firms, including technology-based small businesses and startup ventures, to address homeland security needs; and

(B) may identify geographic areas in the United States with high concentrations of such innovative and emerging technology developers and firms, and may establish personnel and office space in such areas, as appropriate.

(2) ENGAGEMENT.—Engagement under paragraph (1) may include innovative and emerging technology developers or firms with proven technologies, supported with outside investment, with potential applications for the Department of Homeland Security.

(3) CO-LOCATION.—If the Secretary of Homeland Security determines that it is appropriate to establish personnel and office space in a specific geographic area in the United States pursuant to paragraph (1)(B), the Secretary shall co-locate such personnel and office space with other existing assets of—

(A) the Department of Homeland Security, where possible; or

(B) Federal facilities, where appropriate.

(4) OVERSIGHT.—Not later than 30 days after establishing personnel and office space in a specific geographic area in the United States pursuant to paragraph (1)(B), the Secretary of Homeland Security shall inform Congress about the rationale for such establishment, the anticipated costs associated with such establishment, and the specific goals for such establishment.

(b) STRATEGIC PLAN.—Not later than six months after the date of the enactment of this section, the Secretary of Homeland Security shall develop, implement, and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a Department of Homeland Security-wide strategy to proactively engage with innovative and emerging technology developers and firms, including technology-based small businesses and startup ventures, in accordance with subsection (a). Such strategy shall—

(1) focus on sustainable methods and guidance to build relationships, including with such innovative and emerging technology developers and firms in geographic areas in the United States with high concentrations of such innovative and emerging technology developers and firms, and in geographic areas outside such areas, to establish, develop, and enhance departmental capabilities to address homeland security needs;

(2) include efforts to—

(A) ensure proven innovative and emerging technologies can be included in existing and future acquisition contracts;

(B) coordinate with organizations that provide venture capital to businesses, particularly small businesses and startup ventures, as appropriate, to assist the commercialization of innovative and emerging technologies that are expected to be ready for commercialization in the near term and within 36 months; and

(C) address barriers to the utilization of innovative and emerging technologies and the engagement of small businesses and startup ventures in the acquisition process;

(3) include a description of how the Department plans to leverage proven innovative and emerging technologies to address homeland security needs; and

(4) include the criteria the Secretary plans to use to determine an innovation or technology is proven.

(c) NO ADDITIONAL FUNDS AUTHORIZED.—No additional funds are authorized to carry out the requirements of this Act. Such requirements shall be carried out using amounts otherwise authorized.

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

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

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

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

There was no objection.