

losing up to 8,000 jobs and \$400 million in yearly business activity.

As the Inland Empire continues to grow in population, it needs the Ontario International Airport to be under local control. It is a vital economic resource to our region, with the potential to serve 30 million passengers annually, and it is a conflict of interest for Los Angeles World Airports to control Ontario, a direct competitor.

On a personal note, I am ready to give up the long commute from Riverside to LAX. And in that spirit, 3 years ago I wrote a letter to Mayor Garcetti of Los Angeles outlining the need to transfer control of Ontario Airport to our region. I am happy that we are finally moving forward with this legislation to ensure an arrangement that is best for the Inland Empire.

I would like to thank my colleagues, Congressman KEN CALVERT and Congresswoman NORMA TORRES, and all the rest of our delegation from the Inland Empire of southern California, for their hard work on this issue. I am proud to be an original cosponsor of this legislation. I also extend my thanks to the gentlewoman from Nevada for her support.

I strongly urge a “yes” vote on this bill.

Mrs. COMSTOCK. Mr. Speaker, I have no further speakers. I am prepared to close.

I reserve the balance of my time.

Ms. TITUS. Mr. Speaker, I, too, have no further speakers. I just want to say that I support this legislation. I urge my colleagues to do the same, and I also admonish them to show the same degree of urgency when it comes to reauthorizing the FAA.

I yield back the balance of my time.

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

Mr. Speaker, I urge all Members to support this bill of my colleague, Mr. CALVERT.

I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 4369, “A bill that authorizes the use of passenger facility charges at an airport previously associated with the airport at which the charges are collected.”

As a senior member of the House Committee on Homeland Security and the Ranking Member of the Judiciary Committee’s Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, I strongly support this commonsense measure to improve and sustain airport security.

Since its inception, Passenger Facility Charges (PFCs) have been used to improve safety, enhance security, and increase the capacity of airports to serve the traveling public.

A Passenger Facility Charge is a service fee and is also an additional fee charged to departing and connecting passengers at an airport.

H.R. 4369 clarifies and streamlines opportunities that will help ease travel through our nation’s airports while improving our national security.

For example this bill will enable:

The preservation and protection of the nation’s air transportation system;

Enhanced competition between and among air carriers;

Funding projects that benefit local communities; and

Meeting airline and passenger demands to accommodate future growth for our nation’s economy.

In 2015, more than 700 million passengers and 400 million checked bags were screened by the Transportation Security Administration (TSA).

Each day, TSA processes an average of 1.7 million passengers at more than 450 airports across the nation.

In 2012, TSA screened 637,582,122 passengers.

The Bush International and the William P. Hobby Airports are essential hubs for domestic and international air travel for Houston and the region.

Nearly 40 million passengers traveled through Bush International Airport (IAH) and an additional 10 million traveled through William P. Hobby (HOU).

More than 650 daily departures occur at IAH.

IAH is the 11th busiest airport in the U.S. for total passenger traffic.

IAH has 12 all-cargo airlines and handled more than 419,205 metric tons of cargo in 2012.

Airlines and airports are expected to experience a significant increase in passenger traffic coming into the 2016 summer peak travel months across the nation’s largest airports.

As a result of the Passenger Facility Charges airports will continue to receive the needed funds to modernize and keep up with the growing traffic demands and safety and security challenges of our nation’s airports.

For this reason, I urge my colleagues to support this important legislation.

Mrs. NAPOLITANO. Mr. Speaker, I rise in strong support of H.R. 4369, which would allow for a local settlement agreement in Southern California between the City of Los Angeles and the new Ontario Airport Authority.

I thank Chairman SHUSTER and Ranking Member DEFAZIO for bringing this bill to the House floor today, and I thank Congresswoman TITUS for managing the floor debate.

I would also like to thank my bipartisan colleagues from California, Rep. CALVERT and Rep. TORRES, for their leadership on this bill.

Mr. Speaker, after 5 years of negotiations the City of Los Angeles has agreed to transfer its ownership of the Ontario Airport to a new airport authority created by the City of Ontario and San Bernardino County.

This deal has been supported by all stakeholders in order to give the people of the Inland Empire in Southern California control over their own airport.

The residents, businesses, and cities in my district in the San Gabriel Valley are also very supportive of this agreement. The Ontario Airport is only 15 miles from the center of my district, whereas Los Angeles International Airport (LAX) is 40 miles from the center of my district, and there is constant traffic. San Gabriel Valley residents and businesses would much rather use Ontario Airport than LAX if it had better flight options to more locations, which this bill will help accomplish. Allowing for local control of the airport puts the best interest of our region first in improving and managing the airport. I am also appreciative that this agreement makes sure that airport workers will not lose their jobs during and after the transition.

The major point in this local agreement was providing for the repayment of passenger facility charge fees (PFCs) that Los Angeles had collected at LAX in the 1990s and used to construct a new terminal at Ontario Airport.

The settlement agreement requires Ontario Airport to pay back LAX with future PFCs collected at Ontario. The problem is that federal law only allows the transfer of PFCs from one airport to another airport if they are owned by the same airport authority. This is the current law that allowed LAX to transfer PFCs to Ontario.

Since the new agreement transfers control of Ontario Airport to a new airport authority, without our legislation the new Ontario Airport authority is prohibited from paying back the PFCs to LAX.

Mr. Speaker, our bill today is a narrow change in the use of PFCs to allow those collected at Ontario International Airport to be used for projects at LAX. This amendment was carefully written as to only apply to Ontario Airport and LAX. There are no federal funds used in this amendment, and it does not change any of the policy requirements of the use of PFCs.

Mr. Speaker, I ask for the support of my colleagues for H.R. 4369.

The SPEAKER pro tempore. 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. 4369.

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 2016

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5388) to amend the Homeland Security Act of 2002 to provide for innovative research and development, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5388

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 2016”.

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. 319. 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 section 318 the following new item:

“Sec. 319. 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 “2020”;

(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 “2020”; 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.”

(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) PROHIBITION ON ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this Act and the amendments made by this Act.

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 within which to revise and extend their remarks and include 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, as part of Majority Leader KEVIN MCCARTHY's Innovation Initiative, I am very pleased to bring

two important bills to the floor today that further the leader's efforts for ensuring that government can more effectively leverage cutting-edge cyber technologies.

As chairman of the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee, my colleagues and I have been working diligently with technology innovators, including tech startups, to find solutions that will help spur innovation and break down bureaucratic barriers that are currently preventing government from leveraging the private sector's emerging technologies.

Mr. Speaker, I am grateful that the House is first considering H.R. 5388, the Support for Rapid Innovation Act of 2016, on the floor today. H.R. 5388 requires the Department of Homeland Security's 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. 5388 requires S&T to support the full lifecycle of cyber research and development projects and to identify mature technologies to address cybersecurity gaps. In doing so, S&T must target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within 2 years.

This bill also extends the use of other transaction authority, or OTA, until the year 2020, which will improve DHS' ability to engage tech startups that are developing these cutting-edge technologies.

Finally, Mr. Speaker, H.R. 5388 also includes important accountability requirements to ensure that there will be proper oversight of the authority.

In December of last year, the House passed H.R. 3578, the Science and Technology Reform and Improvement Act. That bill included provisions similar to those in the bill that we are considering today.

Mr. Speaker, over the last several years, we have seen evolving cybersecurity threats from nation-states, including China, Russia, North Korea, and Iran, as well as cyber threats from criminal organizations and terrorist groups like ISIS. Cyber criminals continue to develop even more cutting-edge cyber capabilities.

In 2016, these hackers pose an even greater threat to the U.S. homeland and our critical infrastructure. The Federal Government desperately needs to keep pace with these evolving threats and more actively work with the private sector to find solutions.

Mr. Speaker, the Department of Homeland Security's Directorate of Science and Technology is the primary research and development arm of the Department and, because the Directorate manages basic and applied research and development, including cybersecurity R&D for the Department's operational components and first responders, ensuring that there are

mechanisms in place like S&T's cybersecurity research and development programs and OTA to support the dynamic nature of the cybersecurity research and development is both vital and essential for addressing Homeland Security capability gaps.

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

Mr. Speaker, I urge all Members to join me in supporting this bill, and I reserve the balance of my time.

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,

Washington, DC, June 20, 2016.

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

DEAR MR. CHAIRMAN: I am writing concerning H.R. 5388, the "Support for Rapid Innovation Act of 2016," which your Committee reported on June 8, 2016.

H.R. 5388 contains provisions within the Committee on Science, Space, and Technology's rule X jurisdiction. As a result of your having consulted with the Committee and 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 Committee Report and 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, June 20, 2016.

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

DEAR CHAIRMAN SMITH: Thank you for your letter regarding H.R. 5388, the "Support for Rapid Innovation Act of 2016." 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.

□ 1500

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

I rise in support of H.R. 5388, the Support for Rapid Innovation Act of 2016.

Mr. Speaker, H.R. 5388, the Support for Rapid Innovation Act of 2016, directs the Department of Homeland Security to support advancements in cybersecurity research. Hackers, cyberterrorists, and other cybercriminals are constantly innovating. As such, it is a security imperative that the Federal Government—or, more specifically, DHS—innovate, too. To that end, H.R. 5388 directs DHS to support promising projects to, among other things, improve the detection of cyber attacks or intrusions and mitigation and recovery from such attacks.

This bill is based on two provisions contained in H.R. 3578, the DHS Science and Technology Reform and Improvement Act, which passed the House last December. Specifically, H.R. 5388 directs DHS' Under Secretary for Science and Technology to bolster research and development of cybersecurity technology to improve the sharing of information, analysis, and methodologies to address cybersecurity risk and incidents. Additionally, H.R. 5388 extends for 4 years the Department's authority to utilize other transaction authority instead of the Federal Acquisition Regulation to fund basic, applied, and advanced R&D projects.

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

I reserve the balance of my time.

Mr. RATCLIFFE. Mr. Speaker, I yield 1 minute to the distinguished gentleman from California (Mr. MCCARTHY), the majority leader.

Mr. MCCARTHY. Mr. Speaker, I thank the gentleman for yielding.

Mr. Speaker, the gentleman from Texas (Mr. RATCLIFFE) has put two bills before this House, two bills that are part of our broader Innovation Initiative that take the power of human discovery and apply it to national security.

We know that what protected us in the past isn't sufficient for today or the future. Oceans were our greatest defense for much of our history, but distance became less important in the age of jets and rockets. Radar was a revolutionary discovery that helped us see threats before they arrived, but radar can't help us find a potential terrorist being radicalized in our very own neighborhoods.

We can't rely today on what worked in the past. We need new weapons, new tools, and new defenses. We need more, and the government can't do it alone. The dangers are too pressing for Washington to find the best ways to protect the American people all by itself.

Across this country, there are innovators who are finding the answers, and we need to listen to them. The House knows this, and one of our bills directs the Secretary of Homeland Security to engage with private citi-

zens who can join in the task of making our great country safe.

The second bill of the Innovation Initiative today focuses explicitly on cybersecurity: to update and improve detection of intrusions, improve recovery, and reduce vulnerabilities in the industrial systems we rely on.

We have seen, repeatedly, from the Office of Personnel Management to the IRS to businesses in the private sector that our cyber defenses are simply not up to the task. But we can do better. We always can and we always will.

Mr. Speaker, I am proud of the ideas being put forward for the Innovation Initiative so far. America has unprecedented potential, and through the focus of this initiative, we will discover new and better ways to keep America safe.

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

Mr. Speaker, our Nation faces growing, diverse, and increasingly sophisticated cybersecurity threats. These threats necessitate a Federal response that includes supporting innovative cybersecurity research and development, testing, and evaluation. This response is dependent on strong public and private collaboration. Such collaboration is essential to ensuring that promising technologies are introduced into the marketplace in a timely manner.

With that, Mr. Speaker, I urge my colleagues to support H.R. 5388.

I yield back the balance of my time.

Mr. RATCLIFFE. Mr. Speaker, I once again urge all of my colleagues to support H.R. 5388, and I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 5388, the "Support for Rapid Innovation Act of 2016," 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. 5388 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 2016" 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. 5389.

The SPEAKER pro tempore (Mr. PALMER). 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. 5389.

The question was taken.

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

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

The yeas and nays were ordered.

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

LEVERAGING EMERGING TECHNOLOGIES ACT OF 2016

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5389) to encourage engagement between the Department of Homeland Security and technology innovators, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5389

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 2016".

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 innovative or technology is proven.

(c) PROHIBITION ON ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this Act.

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

Mr. Speaker, I rise in support and I am very pleased that the House is considering H.R. 5389, the Leveraging Emerging Technologies Act of 2016. H.R. 5389 encourages engagement between the Department of Homeland Security and technology innovators, including tech startups.

This important bill requires the Secretary of Homeland Security to proactively engage with innovative and emerging technology developers and firms to address homeland security needs. More specifically, H.R. 5389 provides the Secretary authority to identify geographic areas in the United States where high concentrations of innovative and emerging technology developers and firms exist and to establish personnel and office space in these areas to more effectively collaborate with these technology hubs.

The Federal Government needs to do a better job working with the private sector, and this bill will support that goal by requiring the Secretary to develop and implement a targeted strategy to proactively engage innovative and emerging technology developers and firms. The Secretary must use this strategic plan to address and to reduce barriers to leveraging innovative and emerging technologies and the small business and startup ventures that create those technologies by incorporating them into the Department's acquisition process.

In order to keep pace, the Department of Homeland Security recently established an office in Silicon Valley to encourage engagement and communication with the innovative technology developers in that area. Although a vital technology hub, Silicon Valley is not the only technology hub in the United States. For that reason, the Department should not be limited to a single geographic area from which to identify emerging and innovative technologies.

Mr. Speaker, we are all learning that cybersecurity is national security. The Nation is under constant cyber attack from nation-states, from criminal groups, and from terrorist organizations, and, with each passing day, the attacks and tools that they are using are becoming more sophisticated. Requiring the Department to consider strategically how it will engage these technology developers will strengthen the Department's ability to access innovative and emerging technologies in order to combat these evolving threats.

I am happy to support this measure today and believe it will move us toward further addressing homeland security needs by supporting technology innovation.

Before I close, I include in the RECORD an exchange between the chairman of the Committee on Science,