1. Information on how Administration solicitation, testing, evaluation, piloting, acquisition, and procurement processes impact the Administrator's ability to acquire from a technology stakeholder, including a small business innovator, that has not previously provided technology to the Administration, an innovative technology or capability with the potential to enhance transportation security;

2. Specific actions that the administrator will take to foster diversification within the technology stakeholder market along with a timeline for such actions;

3. Plans for how the administrator may assist a small business innovator at certain points in such process; and

4. A feasibility assessment of partnering with an organization described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code.

I represent the 18th Congressional District of Texas which is situated in Houston and home to 2 major airports, the George Bush International Airport and William P. Hobby Airport, which are essential hubs for domestic and international air travel for Houston and the region.

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

More than 650 daily departures occur at George Bush International Airport, which is also the 11th busiest airport in the U.S. for total passenger traffic and annually handles more than 419,205 metric tons of cargo.

As better transportation security technology becomes available, it is imperative that it be adequately evaluated for use in our nation's airports.

The size of a company should not limit it from contributing to the important work of aviation security.

We should support advances in transportation security technology that are positive and help fulfill the TSA's mission to protect our nation's transportation systems from terrorist threats.

I ask that all members join me in voting to pass H.R. 6459, the ''TSA OPEN for Business 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. 6459.

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.

SECURING THE HOMELAND SECURITY SUPPLY CHAIN ACT OF 2018

Mr. KING of New York. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 6430) to amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to implement certain requirements for information relating to supply chain risk, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6430

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 ''Securing the Homeland Security Supply Chain Act of 2018''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is amended by adding at the end the following new section:

''SEC. 836. REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.

''(a) AUTHORITY.—Subject to subsection (b), the Secretary may—

''(1) carry out a covered procurement action;

''(2) limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information, including classified information, relating to the basis for carrying out such an action; and

''(3) exclude, in whole or in part, a source carried out in the course of such an action applicable to a covered procurement of the Department.

''(b) DETERMINATION AND NOTIFICATION.—Except as authorized by subsection (c) to address an urgent national security interest, the Secretary may exercise the authority provided in subsection (a) only after—

''(1) obtaining a joint recommendation, in unclassified or classified form, from the Chief Acquisition Officer and the Chief Information Officer of Department, including a review of any risk assessment made available by an appropriate person or entity, that there is a significant supply chain risk in a covered procurement;

''(2) notifying any source named in the joint recommendation described in paragraph (1) advising—

''(A) that a recommendation has been obtained;

''(B) to the extent consistent with the national security and law enforcement interests, the basis for such recommendation;

''(C) that, within 30 days after receipt of notice, such source may submit information and argument in opposition to such recommendation; and

''(D) of the procedures governing the consideration of such submission and the possible exercise of the authority provided in subsection (a);

''(3) notifying the relevant components of the Department that such risk assessment has demonstrated significant supply chain risk to a covered procurement; and

''(4) making a determination in writing, in unclassified or classified form, that after considering any information submitted by a source under paragraph (2), and in consultation with the Chief Information Officer of the Department, that—

''(A) use of authority under subsection (a)(1) is necessary to protect national security by reducing supply chain risk;

''(B) less intrusive measures are not reasonably available to reduce such risk;

''(C) a decision to limit disclosure of information under subsection (a)(2) is necessary to protect national security interest; and

''(D) the use of such authorities will apply to a single covered procurement or a class of covered procurements, and otherwise specifies the scope of such determination;

''(5) providing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a classified or unclassified notice of the determination made under paragraph (4) that includes—

''(A) the joint recommendation described in paragraph (1);

''(B) a summary of any risk assessment reviewed in support of such joint recommendation; and

''(C) a summary of the basis for such determination, including a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk;

''(6) notifying the Director of the Office of Management and Budget, and the heads of other Federal agencies as appropriate, in a manner and to the extent consistent with the requirements of national security; and

''(7) taking steps to maintain the confidentiality of any notifications under this subsection.

''(c) PROCEDURES TO ADDRESS URGENT NATIONAL SECURITY INTERESTS.—In any case in which the Secretary determines that national security interests require the immediate exercise of the authorities under subsection (a), the Secretary—

''(1) may, to the extent necessary to address any such national security interest, and subject to the conditions specified in paragraph (2)—

''(A) temporarily delay the notice required by subsection (b)(2);

''(B) make the determination required by subsection (b)(4), regardless of whether the notice required by subsection (b)(2) has been provided or whether the notified source at issue has submitted any information in response to such notice;

''(C) temporarily delay the notice required by subsections (b)(4) and (b)(5); and

''(D) exercise the authority provided in subsection (a) in accordance with such determination; and

''(2) shall take actions necessary to comply with all requirements of subsection (b) as soon as practicable after addressing the urgent national security interest that is the subject of paragraph (1), including—

''(A) providing the notice required by subsection (b)(2);

''(B) promptly considering any information submitted by the source at issue in response to such notice, and making any appropriate modifications to the determination required by subsection (b)(4) based on such information; and

''(C) providing the notice required by subsections (b)(5) and (b)(6), including a description of such urgent national security, and any modifications to such determination made in accordance with subparagraph (B).

''(d) ANNUAL REVIEW OF DETERMINATIONS.—The Secretary shall annually review all determinations made under subsection (b).

''(e) DELEGATION.—The Secretary may not delegate the authority provided in subsection (a) or the responsibility identified in subsection (d) to an official below the Deputy Secretary.

''(f) LIMITATION OF REVIEW.—Notwithstanding any other provision of law, no action taken by the Secretary under subsection (a) may be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

''(g) CONSULTATION.—In developing procedures and guidelines for the implementation of the authorities described in this section, the Secretary shall review the procedures and guidelines utilized by the Department of Defense to carry out similar authorities.

''(h) DEFINITIONS.—In this section:

''(1) COVERED ARTICLE.—The term 'covered article' means:

''(A) Information technology, including cloud computing services of all types.

''(B) Telecommunications equipment.

''(C) Telecommunications services.

''(D) The processing of information on a Federal or non-Federal information system,

subject to the requirements of the Controlled Unclassified Information program of the Department.

''(E) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

''(2) COVERED PROCUREMENT.—The term 'covered procurement' means—

''(A) a source selection for a covered article involving either a performance specification, as provided in subsection (a)(3)(B) of section 3306 of title 41, United States Code, or an evaluation factor, as provided in subsection (c)(1)(A) of such section, relating to supply chain risk, or with respect to which supply chain risk considerations are included in the Department's determination of whether a source is a responsible source as defined in section 113 of such title;

''(B) the consideration of proposals for and issuance of a task or delivery order for a covered article, as provided in section 4106(d)(3) of title 41, United States Code, with respect to which the task or delivery order contract includes a contract clause establishing a requirement relating to supply chain risk;

''(C) any contract action involving a contract for a covered article with respect to which such contract includes a clause establishing requirements relating to supply chain risk; or

''(D) any procurement made via Government Purchase Care for a covered article when supply chain risk has been identified as a concern.

''(3) COVERED PROCUREMENT ACTION.—The term 'covered procurement action' means any of the following actions, if such action takes place in the course of conducting a covered procurement:

''(A) The exclusion of a source that fails to meet qualification requirements established pursuant to section 3311 of title 41, United States Code, for the purpose of reducing supply chain risk in the acquisition or use of a covered article.

''(B) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

''(C) The determination that a source is not a responsible source based on considerations of supply chain risk.

''(D) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source from consideration for a subcontract.

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

''(5) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given such term in section 11101 of title 40, United States Code.

''(6) RESPONSIBLE SOURCE.—The term 'responsible source' has the meaning given such term in section 113 of title 41, United States Code.

''(7) SUPPLY CHAIN RISK.—The term 'supply chain risk' means the risk that a malicious actor may sabotage, maliciously introduce an unwanted function, extract or modify data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered article so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the information technology or information stored or transmitted on the covered articles.

''(8) TELECOMMUNICATIONS EQUIPMENT.—The term 'telecommunications equipment' has the meaning given such term in section 153(52) of title 47, United States Code.

''(9) TELECOMMUNICATIONS SERVICE.—The term 'telecommunications service' has the meaning given such term in section 153(53) of title 47, United States Code.

''(i) EFFECTIVE DATE.—The requirements of this section shall take effect on the date that is 90 days after the date of the enactment of this Act and shall apply to—

''(1) contracts awarded on or after such date; and

''(2) task and delivery orders issued on or after such date pursuant to contracts awarded before, on, or after such date.''.

(b) RULEMAKING.—Section 553 of title 5, United States Code, and section 1707 of title 41, United States Code, shall not apply to the Secretary of Homeland Security when carrying out the authorities and responsibilities under section 836 of the Homeland Security Act of 2002, as added by subsection (a).

(c) 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 835 the following new item:

''Sec. 836. Requirements for information relating to supply chain risk.''.

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

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. KING of New York. Madam Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include any extraneous material on the bill under consideration.

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

There was no objection.

Mr. KING of New York. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, on July 24, the Committee on Homeland Security voted to favorably report H.R. 6430. I want to thank the Oversight and Management Efficiency Subcommittee chairman, Mr. PERRY; the full committee chairman, Mr. MCCAUL; Ranking Member THOMPSON; the Counterterrorism and Intelligence Subcommittee ranking member, Miss RICE; the Oversight and Management Efficiency ranking member, Mr. CORREA; Congressman DONOVAN; and Congressman PAYNE for working with me and cosponsoring this legislation.

The legislation under consideration is a result of several years of oversight into supply chain and counterintelligence risks in the procurement process.

There is no question that nation-states and criminal actors are constantly trying to exploit U.S. Government and private-sector systems to steal information or insert potentially harmful hardware or software. The recent cases involving Kaspersky, ZTE, and Huawei underscore the threats posed to the Federal supply chain and the urgency in developing stronger mechanisms to secure it.

On July 12, I held a hearing to review DHS' current supply chain risk management programs as well as assess the need for additional authority. At the hearing, the Department's chief information officer noted: ''Gaps exist in the Department's authority to use intelligence to support its procurement decisions. . . . In those exceptional cases where mitigation is not possible, the Department needs the capability to react swiftly while appropriately restricting the disclosure of other national security sensitive information.''

Clearly, Madam Speaker, this is a problem. The bill under consideration today provides the DHS Secretary with authority to restrict information technology procurements if the vendor poses a threat to the DHS supply chain.

This bill establishes true coordination between the acquisition process and intelligence. This authority is modeled after existing authority granted to the Department of Defense in 2011. The legislation also includes important enhancements recommended by the Office of Management and Budget based on a governmentwide supply chain risk management proposal released at the end of July.

I am hopeful that, as this bill moves through the process, we will also have an opportunity to consider the legislation that provides similar authority to ensure national security vetting is incorporated into the wider government procurement process.

As a national security agency, it is vital that DHS also have robust supply chain risk management practices and tools to identify, mitigate, and remove potential threats to its systems and contracts. With this legislation, Congress is ensuring that DHS will have the authority necessary to fully vet and restrict, if necessary, vendors who pose a threat.

Madam Speaker, I urge all Members to join me in supporting H.R. 6430, and I reserve the balance of my time.

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

Mr. Speaker, I rise in support of H.R. 6430, the Securing the Homeland Security Supply Chain Act of 2018.

Mr. Speaker, H.R. 6430 would authorize the Secretary of Homeland Security to exclude an information technology and communication vendor that is deemed to pose significant national security risk from contracts for equipment and services.

I strongly believe that DHS must have the necessary tools to address evolving cyber incursions and espionage by nation-states to keep our country safe. The most significant risk to the supply chain comes from Chinese and Russian companies.

For years, the intelligence community has warned that information and communication technology produced by Chinese companies, most notably ZTE and Huawei, could be used to carry out cyber theft and espionage.

Some companies with ties to the Russian Government also pose national

security risks. The U.S. Government has particularly highlighted concerns about Kaspersky Lab. In September 2017, DHS issued a directive requiring Federal agencies to remove all Kaspersky products from their networks, given ties between certain Kaspersky officials and Russian intelligence.

The risks to the supply chain are all too real and must be mitigated. That is why I am proud to cosponsor H.R. 6430, a measure that acts upon the information provided to us by our intelligence community to help DHS better counter these mounting threats.

H.R. 6430 provides DHS with needed authority to exclude vendors who are bad actors from the information technology and communications supply chain. If enacted, H.R. 6430 will allow the Department to be proactive and effective in addressing these complex threats in the future.

Importantly, the bill includes robust oversight provisions to ensure that Congress receives notification and justification of any exercise of authority under this act. Notably, this measure is based on a similar authority provided to the Department of Defense in 2011 and incorporates language provided by the Office of Management and Budget.

H.R. 6430 provides the Secretary of Homeland Security with a much-needed tool to eliminate national security threats to our supply chain. Enactment of H.R. 6430 will help DHS secure information technology and telecommunications equipment and services that are so essential to keeping our Nation secure.

Mr. Speaker, I would like to compliment the gentleman from New York, who has significant experience in this area, for offering this legislation.

Mr. Speaker, I encourage my colleagues to support H.R. 6430, and I yield back the balance of my time.

Mr. KING of New York. Mr. Speaker, I yield myself the balance of my time.

Let me again thank the gentleman from Mississippi and the ranking member for his service on this bill and his service to the committee over the years.

Mr. Speaker, this legislation provides DHS vital authority to protect the Department from vendors who pose a risk. The bill includes important accountability measures to ensure that decisions are risk based, allows the vendor to provide feedback, and requires annual reviews any time the authority is used.

This is commonsense legislation that will provide important national security protections for the Department similar to what already exists for the Department of Defense and the intelligence community.

Mr. Speaker, I once again urge my colleagues to support H.R. 6430, the Securing the Homeland Security Supply Chain Act of 2018, and I yield back the balance of my time.

The SPEAKER pro tempore (Mr. HILL). The question is on the motion offered by the gentleman from New York (Mr. KING) that the House suspend the rules and pass the bill, H.R. 6430.

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.

ADVANCING CYBERSECURITY DIAGNOSTICS AND MITIGATION ACT

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6443) to amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program at the Department of Homeland Security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6443

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 ''Advancing Cybersecurity Diagnostics and Mitigation Act''.

SEC. 2. ESTABLISHMENT OF CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM IN DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 230 of the Homeland Security Act of 2002 (6 U.S.C. 151) is amended by adding at the end the following new subsection:

''(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

''(1) PROGRAM.—

''(A) IN GENERAL.—The Secretary shall deploy, operate, and maintain a continuous diagnostics and mitigation program. Under such program, the Secretary shall—

''(i) develop and provide the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks;

''(ii) make program capabilities available for use, with or without reimbursement;

''(iii) employ shared services, collective purchasing, blanket purchase agreements, and any other economic or procurement models the Secretary determines appropriate to maximize the costs savings associated with implementing an information system;

''(iv) assist entities in setting information security priorities and managing cybersecurity risks; and

''(v) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under such program.

''(B) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the continuous diagnostics and mitigation program required under subparagraph (A), as appropriate, to improve the program.

''(2) ACTIVITIES.—In carrying out the continuous diagnostics and mitigation program under paragraph (1), the Secretary shall ensure, to the extent practicable, that—

''(A) timely, actionable, and relevant cybersecurity risk information, assessments, and analysis are provided in real time;

''(B) share the analysis and products developed under such program;

''(C) all information, assessments, analyses, and raw data under such program is made available to the national cybersecurity and communications integration center of the Department; and

''(D) provide regular reports on cybersecurity risks.''.

(b) CONTINUOUS DIAGNOSTICS AND MITIGATION STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop a comprehensive continuous diagnostics and mitigation strategy to carry out the continuous diagnostics and mitigation program required under subsection (g) of section 230 of such Act, as added by subsection (a).

(2) SCOPE.—The strategy required under paragraph (1) shall include the following:

(A) A description of the continuous diagnostics and mitigation program, including efforts by the Secretary of Homeland Security to assist with the deployment of program tools, capabilities, and services, from the inception of the program referred to in paragraph (1) to the date of the enactment of this Act.

(B) A description of the coordination required to deploy, install, and maintain the tools, capabilities, and services that the Secretary of Homeland Security determines to be necessary to satisfy the requirements of such program.

(C) A description of any obstacles facing the deployment, installation, and maintenance of tools, capabilities, and services under such program.

(D) Recommendations and guidelines to help maintain and continuously upgrade tools, capabilities, and services provided under such program.

(E) Recommendations for using the data collected by such program for creating a common framework for data analytics, visualization of enterprise-wide risks, and real-time reporting.

(F) Recommendations for future efforts and activities, including for the rollout of new tools, capabilities and services, proposed timelines for delivery, and whether to continue the use of phased rollout plans, related to securing networks, devices, data, and information technology assets through the use of such program.

(3) FORM.—The strategy required under subparagraph (A) shall be submitted in an unclassified form, but may contain a classified annex.

(c) REPORT.—Not later than 90 days after the development of the strategy required under subsection (b), the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representative a report on cybersecurity risk posture based on the data collected through the continuous diagnostics and mitigation program under subsection (g) of section 230 of the Homeland Security Act of 2002, as added by subsection (a).

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 in which to revise and extend their remarks and 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, earlier this year, the Office of Management and Budget and the Department of Homeland Security