

but I must acknowledge that over the past few weeks, the Trump administration has taken several alarming actions that work to counter the work we are trying to do today with this legislation.

Mr. Speaker, I urge the Trump administration to work with Congress and not against Congress' efforts to strengthen America's ability to compete with China like this bill that aims to do exactly that.

Mr. Speaker, I urge all Members to support this legislation, and I yield back the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Tennessee (Mr. GREEN) that the House suspend the rules and pass the bill, H.R. 708.

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.

#### RESEARCH SECURITY AND ACCOUNTABILITY IN DHS ACT

Mr. GREEN of Tennessee. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 901) to require the Under Secretary of the Science and Technology Directorate of the Department of Homeland Security to develop a Department-wide policy and process to safeguard research and development from unauthorized access to or disclosure of sensitive information in research and development acquisitions, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 901

*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 "Research Security and Accountability in DHS Act".

##### SEC. 2. SAFEGUARDING SENSITIVE RESEARCH IN THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 302 of the Homeland Security Act of 2002 (6 U.S.C. 182) is amended—

(1) in paragraph (13), by striking "and" after the semicolon;

(2) in paragraph (14), by striking the period and inserting ":", and"; and

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

"(15) developing, in coordination with appropriate agency officials, a Department-wide policy and process to safeguard research and development from unauthorized access to or disclosure of sensitive information in research and development acquisitions."

(b) GAO REPORT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall 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 report on how the Department of Homeland Security

has complied with National Security Presidential Memorandum-33 (NSPM-33) and adopted the National Science and Technology Council's 2022 implementation guidance.

(2) ELEMENTS.—The report required under paragraph (1) shall address the following:

(A) How the Department of Homeland Security has complied with disclosure requirements outlined in NSPM-33, and how violations are reported to the relevant executive agencies, including in the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(B) Coordination and compliance with guidelines established by the National Science Foundation, the National Science Technology Council, the Office of Science and Technology Policy, and other executive agencies regarding Federal research security.

(C) The role of the Science and Technology Directorate of the Department regarding establishing a research security framework for research and development projects across the Department.

(c) CONGRESSIONAL BRIEFING.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing addressing the development of policies and processes to safeguard Department of Homeland Security research and development in accordance with paragraph (15) of section 302 of the Homeland Security Act of 2002 (6 U.S.C. 182), as added by subsection (a).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Tennessee (Mr. GREEN) and the gentleman from California (Mr. CORREA) each will control 20 minutes.

The Chair recognizes the gentleman from Tennessee.

##### GENERAL LEAVE

Mr. GREEN of Tennessee. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and to include extraneous material on H.R. 901.

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

There was no objection.

Mr. GREEN of Tennessee. Mr. Speaker, I yield myself such time as I may consume.

I rise today in support of H.R. 901, the Research Security and Accountability in DHS Act. The Science and Technology Directorate is the principal of research and development for DHS. In 2022, the DHS Office of Inspector General found that S&T failed to safeguard sensitive information in research and development projects.

This bill requires S&T to develop a proper standard for safeguarding sensitive information which has become especially critical given the heightened activity of our adversaries. This bill carried by former Representative Anthony D'Esposito passed the House last Congress, and I thank the gentleman from Alabama (Mr. STRONG) for his attention to this issue this Congress.

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

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

Mr. Speaker, I rise in support of H.R. 901, the Research Security and Accountability in DHS Act. This bill seeks to enhance security measures by directing the Department of Homeland Security's Science and Technology Directorate to establish a comprehensive policy and process to protect research and development activities from unauthorized access or disclosure of sensitive information.

Additionally, this bill would task the Government Accountability Office to assess DHS' adherence to the National Science and Technology Council's 2022 implementation guidance and a 2021 National Security Presidential Memorandum focused on safeguarding U.S. research from foreign interference.

This bill also requires the Secretary of Homeland Security to provide Congress with a briefing on its implementation.

Time and time again, we have seen bad actors attempt to exploit our sensitive information. This measure strengthens DHS' ability to prevent such threats and protects our national security.

This bill is a critical step in ensuring DHS upholds strong policies and procedures to secure research and development efforts.

Mr. Speaker, I encourage my colleagues to join me in supporting H.R. 901, and I reserve the balance of my time.

Mr. GREEN of Tennessee. Mr. Speaker, I yield such time as he may consume to the gentleman from Alabama (Mr. STRONG).

Mr. STRONG. Mr. Speaker, I rise today in strong support of H.R. 901, the Research Security and Accountability in DHS Act.

I understand how important new technologies are in saving lives and protecting the American homeland as threats and challenges evolve.

Whether the Department of Homeland Security is working to prevent a terrorist act, inhibiting drug traffic at the southwest border, or responding to a life-threatening natural disaster, DHS relies heavily on research and development projects to enhance its operational effectiveness.

The critical role that R&D projects and new technologies play in helping protect our homeland cannot be understated. It is no secret that Federal R&D projects are a target for foreign theft, espionage, and influence.

It is our responsibility to safeguard them from malicious actors and prevent the unauthorized access to, or disclosure of, sensitive information.

This is why I reintroduced H.R. 901, the Research Security and Accountability in DHS Act. This legislation requires the Science and Technology Directorate to develop a process that safeguards sensitive information in R&D projects across all components of the Department.

Both the Trump and Biden administrations have made Federal research

security a priority by issuing executive orders and Federal research security guidance for government agencies like DHS to follow.

Despite this, S&T has not demonstrated how it will protect its \$461 million worth of R&D projects from unauthorized access.

Every taxpayer dollar spent on R&D to improve our national security should be safeguarded from foreign and domestic bad actors who seek to do us harm.

This is why H.R. 901 also requires GAO to submit a report on how DHS has complied with existing Federal guidance to safeguard these R&D projects.

I thank Chairman GREEN and all the members who have supported this legislation.

By passing this commonsense bill and protecting sensitive R&D projects throughout the Department, we will improve the effectiveness of DHS' mission, the safety of our Nation's law enforcers, and, ultimately, our national security.

I urge all Members to join me in supporting this vital piece of legislation to better safeguard DHS and the American people.

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

Mr. Speaker, the passage of this legislation is a key step in protecting DHS' research and development capabilities from bad actors.

Mr. Speaker, I urge my colleagues to support H.R. 901, and I yield back the balance of my time.

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

I again urge my colleagues to support H.R. 901, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Tennessee (Mr. GREEN) that the House suspend the rules and pass the bill, H.R. 901.

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. GREEN of Tennessee. 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.

#### EMERGING INNOVATIVE BORDER TECHNOLOGIES ACT

Mr. GREEN of Tennessee. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 993) to require the Secretary of Homeland Security to develop a plan to identify, integrate, and deploy new, innovative, disruptive, or other emerging or advanced technologies to enhance, or address capability gaps in, border security operations, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 993

*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 "Emerging Innovative Border Technologies Act".

#### SEC. 2. INNOVATIVE AND EMERGING BORDER TECHNOLOGY PLAN.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Commissioner of U.S. Customs and Border Protection (CBP) and the Under Secretary for Science and Technology of the Department of Homeland Security, shall 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 plan to identify, integrate, and deploy new, innovative, disruptive, or other emerging or advanced technologies that may incorporate artificial intelligence, machine-learning, automation, fiber-optic sensing technology, nanotechnology, optical and cognitive radar, modeling and simulation technology, hyperspectral and LIDAR sensors, imaging, identification, and categorization systems, or other emerging or advanced technologies, to enhance, or address capability gaps in, border security operations.

(b) CONTENTS.—The plan required under subsection (a) shall include the following:

(1) Information regarding how CBP utilizes CBP Innovation Team authority under subsection (c) and other mechanisms to carry out the purposes specified in subsection (a).

(2) An assessment of the contributions directly attributable to such utilization.

(3) Information regarding the composition of each CBP Innovation Team, and how each such Team coordinates and integrates efforts with the CBP acquisition program office and other partners within CBP and the Department of Homeland Security.

(4) Identification of technologies used by other Federal departments or agencies not in use by CBP that could assist in enhancing, or addressing capability gaps in, border security operations.

(5) An analysis of authorities available to CBP to procure technologies referred to subsection (a), and an assessment as to whether additional or alternative authorities are needed to carry out the purposes specified in such subsection.

(6) An explanation of how CBP plans to scale existing programs related to emerging or advanced technologies into programs of record.

(7) A description of each planned security-related technology program, including objectives, goals, and timelines for each such program.

(8) An assessment of the privacy and security impact on border communities of security-related technology.

(9) An assessment of CBP legacy border technology programs that could be phased out and replaced by technologies referred to in subsection (a), and cost estimates relating to such phase out and replacement.

(10) Information relating to how CBP is coordinating with the Department of Homeland Security's Science and Technology Directorate to carry out the following:

(A) Research and develop new, innovative, disruptive, or other emerging or advanced technologies to carry out the purposes specified in subsection (a).

(B) Identify security-related technologies that are in development or deployed by the private and public sectors that may satisfy the mission needs of CBP, with or without adaptation.

(C) Incentivize the private sector to develop technologies that may help CBP meet mission needs to enhance, or address capability gaps in, border security operations.

(D) Identify and assess ways to increase opportunities for communication and collaboration with the private sector, small and disadvantaged businesses, intra-governmental entities, university centers of excellence, and Federal laboratories to leverage emerging technology and research within the public and private sectors.

(11) Information on metrics and key performance parameters for evaluating the effectiveness of efforts to identify, integrate, and deploy new, innovative, disruptive, or other emerging or advanced technologies to carry out the purposes specified in subsection (a).

(12) An identification of recent technological advancements in the following:

(A) Manned aircraft sensor, communication, and common operating picture technology.

(B) Unmanned aerial systems and related technology, including counter-unmanned aerial system technology.

(C) Surveillance technology, including the following:

(i) Mobile surveillance vehicles.

(ii) Associated electronics, including cameras, sensor technology, and radar.

(iii) Tower-based surveillance technology.

(iv) Advanced unattended surveillance sensors.

(v) Deployable, lighter-than-air, ground surveillance equipment.

(D) Nonintrusive inspection technology, including non-X-ray devices utilizing muon tomography and other advanced detection technology.

(E) Tunnel detection technology.

(F) Communications equipment, including the following:

(i) Radios.

(ii) Long-term evolution broadband.

(iii) Miniature satellites.

(13) Any other information the Secretary determines relevant.

(c) CBP INNOVATION TEAM AUTHORITY.—

(1) IN GENERAL.—The Commissioner of CBP is authorized to maintain one or more CBP Innovation Teams to research and adapt commercial technologies that are new, innovative, disruptive, or otherwise emerging or advanced that may be used by CBP to enhance, or address capability gaps in, border security operations and urgent mission needs, and assess potential outcomes, including any negative consequences, of the introduction of emerging or advanced technologies with respect to which documented capability gaps in border security operations are yet to be determined.

(2) OPERATING PROCEDURES, PLANNING, STRATEGIC GOALS.—The Commissioner of CBP shall require each team maintained pursuant to paragraph (1) to establish the following:

(A) Operating procedures that include specificity regarding roles and responsibilities within each such team and with respect to Department of Homeland Security and non-Federal partners, and protocols for entering into agreements to rapidly transition such technologies to existing or new programs of record to carry out the purposes specified in subsection (a).

(B) Planning and strategic goals for each such team that includes projected costs, time frames, metrics, and key performance parameters relating to the achievement of identified strategic goals, including a metric to measure the rate at which technologies described in subsection (a) are transitioned to existing or new programs of record in accordance with subparagraph (A).