

every year. H.R. 437 would make enhancing medical preparedness and medical surge capacity and capabilities eligible uses of Homeland Security Grant funds under the law.

This measure passed in the House last Congress, and I urge my colleagues to again support this measure.

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

Mr. DONOVAN. Mr. Speaker, I yield such time as he may consume to the gentleman from Florida (Mr. BILIRAKIS).

Mr. BILIRAKIS. Mr. Speaker, I thank the ranking member for his support.

I rise today in support of critical legislation to support public safety and first responders, the Medical Preparedness Allowable Use Act, H.R. 437.

My bill will help secure medical countermeasures for first responders, ensuring we are prepared for any type of emergency. For instance, last year, in Florida, we faced the outbreak of the Zika virus.

The Medical Preparedness Allowable Use Act means that reliable grant funding would be available to conduct medical preparedness activities such as planning, training, and purchasing protective equipment to combat Zika or other public health threats going forward nationwide. When the worst occurs, our first responders are there for us on the front lines.

I consistently find myself in awe of these brave men and women and the sacrifices they make on the public's behalf. They are heroes. The least we can do is make sure they have the tools they need to do their jobs and keep us safe. That is what my bill seeks to accomplish. We want to keep them safe as well, Mr. Speaker.

The legislation authorizes grant funds for the stockpiling of countermeasures, including medical kits, protective gear, ventilators, and more. This should give us all peace of mind to know this vital equipment will be there in case of a crisis.

Importantly, the grant fund used in H.R. 437 already exists. The bill does not require new or additional funding. Also significant, this bill has received strong bipartisan support.

I thank my colleagues, Representatives SUSAN BROOKS and PETER KING, for being original cosponsors of H.R. 437.

I was inspired to write this legislation during my time as subcommittee chairman on the Homeland Security Committee after a series of hearings with folks from the emergency response community. They expressed the urgent need for stockpiling these medical countermeasures and for providing first responders the assurance that grant funding may be used to support them now and in the future. They need certainty, Mr. Speaker.

I am proud to have the support of the Emergency Services Coalition for Medical Preparedness and the International Association of Fire Chiefs on

this issue. The Medical Preparedness Allowable Use Act is going to make a difference to protect the public and protect our protectors. I strongly urge passage today.

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

Mr. Speaker, I strongly support H.R. 437. Developing and maintaining medical preparedness is an important part of national preparedness. State and local governments should not have to wonder whether they will be able to use DHS grant funds for this purpose from year to year.

I urge my colleagues to support H.R. 437.

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

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

Mr. Speaker, I once again urge my colleagues to support H.R. 437.

I yield back the balance of my time. The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. DONOVAN) that the House suspend the rules and pass the bill, H.R. 437.

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.

UNITED STATES-ISRAEL CYBERSECURITY COOPERATION ENHANCEMENT ACT OF 2017

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 612) to establish a grant program at the Department of Homeland Security to promote cooperative research and development between the United States and Israel on cybersecurity.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 612

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 "United States-Israel Cybersecurity Cooperation Enhancement Act of 2017".

SEC. 2. UNITED STATES-ISRAEL CYBERSECURITY COOPERATION.

(a) GRANT PROGRAM.—

(1) ESTABLISHMENT.—The Secretary, in accordance with the agreement entitled the "Agreement between the Government of the United States of America and the Government of the State of Israel on Cooperation in Science and Technology for Homeland Security Matters", dated May 29, 2008 (or successor agreement), and the requirements specified in paragraph (2), shall establish a grant program at the Department to support—

(A) cybersecurity research and development; and

(B) demonstration and commercialization of cybersecurity technology.

(2) REQUIREMENTS.—

(A) APPLICABILITY.—Notwithstanding any other provision of law, in carrying out a research, development, demonstration, or com-

mercial application program or activity that is authorized under this section, the Secretary shall require cost sharing in accordance with this paragraph.

(B) RESEARCH AND DEVELOPMENT.—

(i) IN GENERAL.—Except as provided in clause (ii), the Secretary shall require not less than 50 percent of the cost of a research, development, demonstration, or commercial application program or activity described in subparagraph (A) to be provided by a non-Federal source.

(ii) REDUCTION.—The Secretary may reduce or eliminate, on a case-by-case basis, the percentage requirement specified in clause (i) if the Secretary determines that such reduction or elimination is necessary and appropriate.

(C) MERIT REVIEW.—In carrying out a research, development, demonstration, or commercial application program or activity that is authorized under this section, awards shall be made only after an impartial review of the scientific and technical merit of the proposals for such awards has been carried out by or for the Department.

(D) REVIEW PROCESSES.—In carrying out a review under subparagraph (C), the Secretary may use merit review processes developed under section 302(14) of the Homeland Security Act of 2002 (6 U.S.C. 182(14)).

(3) ELIGIBLE APPLICANTS.—An applicant shall be eligible to receive a grant under this subsection if the project of such applicant—

(A) addresses a requirement in the area of cybersecurity research or cybersecurity technology, as determined by the Secretary; and

(B) is a joint venture between—

(i) a for-profit business entity, academic institution, National Laboratory (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), or nonprofit entity in the United States; and

(ii) a for-profit business entity, academic institution, or nonprofit entity in Israel; or

(i) the Federal Government; and

(ii) the Government of Israel.

(4) APPLICATIONS.—To be eligible to receive a grant under this subsection, an applicant shall submit to the Secretary an application for such grant in accordance with procedures established by the Secretary, in consultation with the advisory board established under paragraph (5).

(5) ADVISORY BOARD.—

(A) ESTABLISHMENT.—The Secretary shall establish an advisory board to—

(i) monitor the method by which grants are awarded under this subsection; and

(ii) provide to the Secretary periodic performance reviews of actions taken to carry out this subsection.

(B) COMPOSITION.—The advisory board established under subparagraph (A) shall be composed of three members, to be appointed by the Secretary, of whom—

(i) one shall be a representative of the Federal Government;

(ii) one shall be selected from a list of nominees provided by the United States-Israel Binational Science Foundation; and

(iii) one shall be selected from a list of nominees provided by the United States-Israel Binational Industrial Research and Development Foundation.

(6) CONTRIBUTED FUNDS.—Notwithstanding any other provision of law, the Secretary may accept or retain funds contributed by any person, government entity, or organization for purposes of carrying out this subsection. Such funds shall be available, subject to appropriation, without fiscal year limitation.

(7) REPORT.—Not later than 180 days after the date of completion of a project for which a grant is provided under this subsection, the

grant recipient shall submit to the Secretary a report that contains—

(A) a description of how the grant funds were used by the recipient; and

(B) an evaluation of the level of success of each project funded by the grant.

(8) CLASSIFICATION.—Grants shall be awarded under this subsection only for projects that are considered to be unclassified by both the United States and Israel.

(b) TERMINATION.—The grant program and the advisory board established under this section terminate on the date that is seven years after the date of the enactment of this Act.

(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.

(d) DEFINITIONS.—In this section—

(1) the term “cybersecurity research” means research, including social science research, into ways to identify, protect against, detect, respond to, and recover from cybersecurity threats;

(2) the term “cybersecurity technology” means technology intended to identify, protect against, detect, respond to, and recover from cybersecurity threats;

(3) the term “cybersecurity threat” has the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (enacted as title I of the Cybersecurity Act of 2015 (division N of the Consolidated Appropriations Act, 2016 (Public Law 114-113)));

(4) the term “Department” means the Department of Homeland Security; and

(5) the term “Secretary” means the Secretary of Homeland Security.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. RATCLIFFE) and the gentleman from Rhode Island (Mr. LANGEVIN) 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 today in support of H.R. 612, the United States-Israel Cybersecurity Cooperation Enhancement Act of 2017.

I was grateful for the opportunity to work closely with my colleague, Mr. LANGEVIN from Rhode Island, on this vitally important legislation that will build upon the existing collaboration between the United States and the State of Israel on critical cybersecurity issues.

Following our successful congressional delegation to Israel in May of last year to discuss homeland security and cybersecurity issues, Mr. LANGEVIN and I worked closely to champion two important pieces of legislation.

Last year, I introduced H.R. 5877, the United States-Israeli Advanced Part-

nership Act of 2016, which was signed into law on December 16 with Mr. LANGEVIN's help and support. That legislation expanded a current cooperative research program between the two countries by adding cybersecurity to a program that had previously focused only on border security, explosives detection, and emergency services.

Today, Mr. Speaker, I am pleased to have H.R. 612, the United States-Israel Cybersecurity Cooperation Enhancement Act of 2017 come before the House. This bill would expand the memorandum of agreement already in place between our Department of Homeland Security and the State of Israel by authorizing the Secretary to carry out a grant program at DHS to support cybersecurity research and development as well as the demonstration and commercialization of cybersecurity technologies.

During our congressional delegation, Mr. LANGEVIN and I were able to meet with top Israeli officials, including Prime Minister Benjamin Netanyahu, to discuss how the United States and Israel can better cooperate in these vital areas. We also had the opportunity to meet with many of Israel's cybersecurity companies and technology startups.

Over the past several years, Israel has become a leader in cybersecurity and has developed a deep and talented cyber workforce, something we need greater focus on here in the United States. To that end, much of our discussion with Israeli officials and private companies revolved around how the United States and Israel can work more closely together and learn from each other as we combat growing cybersecurity threats. This legislation is a product of those successful discussions.

Mr. Speaker, the United States and Israel are both under constant threat from nation-state and other actors that wish to do our countries harm, so it is vitally important that the United States and Israel work hand-in-hand to build our cyber defenses to combat these cyber threats together.

Mr. Speaker, it is also vital that in the House both parties work hand-in-hand on America's national security vulnerabilities. Given the current political environment, I would like to commend and thank my colleague, Mr. LANGEVIN, for his willingness to do just that, as demonstrated by his partnership on this issue. I very much look forward to continuing to work with him on more cybersecurity issues during the 115th Congress.

I urge all my colleagues to support this legislation.

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

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

I rise in strong support of H.R. 612, the United States-Israel Cybersecurity Cooperation Enhancement Act of 2017.

Mr. Speaker, let me start by thanking Chairman RATCLIFFE for his leader-

ship on the subcommittee and, in particular, on the issue of cybersecurity. I have greatly enjoyed our partnership on this and many issues. I appreciate his due diligence and his hard work on many national security issues.

Let me also start by expressing my deep gratitude to Chairman MCCAUL and Ranking Member THOMPSON in acting so quickly to bring this bill to the floor. Both the chairman and ranking member led a very productive committee last Congress, and I am very pleased that their commitment to protect our national security has extended to swift action this year as well. That urgency is particularly relevant to this bill, the United States-Israel Cybersecurity Cooperation Enhancement Act.

As Chairman RATCLIFFE mentioned, last May, he and I traveled to Israel to meet with public and private cybersecurity officials. I think I can speak for my friend when I say that we were very impressed by the Israeli's efforts in this space. Israel was one of the first countries to recognize the potential threat posed by interconnected computer systems, and they have been leaders in cybersecurity now for decades.

For instance, the first stateful firewall technology was first developed by an Israeli firm. Today, these firewalls are ubiquitous across the information security landscape. In fact, despite its size, Israel is the second largest exporter of cybersecurity goods and services, behind only the United States. U.S. companies have certainly taken notice. Mr. RATCLIFFE and I, as he mentioned, met with some of their representatives during our trip.

Just last week, Reuters reported that one of the components of Microsoft's \$1 billion per year cybersecurity strategy is acquisition of three Israeli corporations.

Collaboration with our closest Middle East ally only makes sense from a national security perspective. Preserving Israeli security is essential to stability in the region.

We clearly have a lot to learn from each other as well, which is why I have championed government-to-government interaction on cybersecurity, such as the recent letter of intent for more information-sharing between DHS and Israel that was championed by former Deputy Secretary Mayorkas.

Beyond our governments working together, Chairman RATCLIFFE and I also believe the government can do more to encourage collaboration between our private sector and nonprofit entities on issues directly relevant to homeland security. That is why, upon our return, we worked in close collaboration to develop two bills to enhance these cooperative relationships.

I could not have asked for a better partnership in this effort. I was thrilled that our first bill, the United States-Israel Advanced Research Partnership Act, was signed into law last month. It is our second bill, which passed the House in November, but failed to make

it through the Senate before Congress adjourned last year, that we are discussing today.

Specifically, this bill creates a cybersecurity grant program for joint research and development ventures between Israeli and American entities. Projects would be selected after a merit review process and would have to address requirements in cybersecurity determined by the Secretary of Homeland Security. The grants would also be subject to a cost-sharing requirement, with at least 50 percent of project funds coming from a non-Federal source.

Importantly, H.R. 612 leverages existing United States-Israel R&D infrastructure, specifically the Binational Industrial Research and Development, or BIRD Foundation, and the Binational Science Foundation, or BSF. Both organizations have a proven track record of encouraging joint research ventures.

□ 1645

BIRD, for instance, has financed R&D and commercialization projects that have led to a cumulative \$8 billion in commercial sales since its founding, while BSF regularly funds collaborations between the top scientists in our respective countries as 45 Nobel laureates have received support from the Foundation.

Now, using the existing infrastructure, as was done in 2007 when Congress passed the Energy Independence and Security Act that led to the creation of BIRD Energy, also allows us to capitalize on both foundations' robust networks of United States and Israeli entities to help seed these joint ventures. All of these factors are particularly critical in the fast-moving cybersecurity domain where offensive and defensive tactics and techniques change on a monthly or even weekly basis.

As such, advances in the discipline require a near constant reexamining of assumptions, and having people from different backgrounds and security cultures working together engenders an environment where such reexamination is encouraged. While both the U.S. and Israel have robust cybersecurity communities, further collaboration will spur more advances to combat the threats that we face.

Although some of these advances are technological in nature, basic cybersecurity research, such as investigations into the psychology of secure interface design and social engineering, is also supported by the bill. All told, the programs authorized in H.R. 612 will both address urgent homeland security needs and build capacity for further transnational collaboration on cybersecurity, all while matching Federal investment with private sector dollars and funds from the Israeli Government.

Mr. Speaker, I normally preface my remarks on cybersecurity with an explanation of the threat our country faces. I would hope that, given recent events, I don't have to remind my col-

leagues of the dangers that we face in this sphere which, as I see it, is one of the key national security challenges of the 21st century.

I would hope that incidents like the recent attack on the Ukrainian power grid demonstrate the power of a computer keyboard to affect our critical infrastructure. I would hope that the breach of hundreds of millions of accounts at Yahoo, which affected around 10 percent of the world's population, demonstrates how pervasive data collection is and its vulnerabilities. I would certainly hope that the Russian information warfare operations targeting the very foundations of our democracy, our elections, demonstrate the stakes that we face.

In the face of these threats, we must join together with our allies to protect a free and open internet and ensure that the amazing benefits of technology are not overshadowed by the new vulnerabilities that they open up. Mr. Speaker, H.R. 612 is an important step to driving the innovation we need in the security space to meet these two goals.

As with any bills that make it to the floor, this bill owes much to the dedicated staff on both sides of the aisle who spent countless hours behind the scenes reviewing this legislation. I thank them for their extraordinary and exceptional work.

I am also very grateful, again, to Chairman MCCAUL, Ranking Member THOMPSON, and Subcommittee Ranking Member RICHMOND for their continued leadership on cybersecurity and, in particular, Chairman RATCLIFFE for his work and for their assistance in quickly actualizing the lessons that we have learned on our trip to Israel.

Finally, in closing, I owe, once again, a debt of gratitude to my friend across the aisle, Chairman RATCLIFFE, who, in his first term, immediately had a substantial impact on our Nation's cybersecurity and with whom it has been a great pleasure to work. I look forward to our continued work in this Congress and beyond.

Mr. Speaker, H.R. 612 does three things: it encourages innovative approaches to address top priorities in homeland security R&D; it strengthens ties with Israel, one of our closest allies; and it does so in a public-private partnership that matches Federal investment.

Mr. Speaker, if you indulge me for a moment, I would like to read something the Saudi Arabian Computer Emergency Response Team put out last week: "Following a recent cyberattack which targeted several national organizations, this is an urgent call for your cybersecurity team to be on the alert for Shamoon 2 and ransomware attacks that could possibly cripple your organization's systems."

For those of my colleagues who are not aware, the Shamoon attacks of 2012 took down tens of thousands of computers at the Saudi state oil company, Saudi Aramco. The Shamoon 2 variant

has been targeting Saudi Government agencies and private industry since November.

I bring this up, Mr. Speaker, because open source intelligence reports point to Iran as being responsible for the original Shamoon attack. I believe there is a good chance that Iranian-aligned actors are behind the recent incidents as well. Our Israeli partners live under this threat every day, and, to be frank, so do we.

Last year, the Justice Department indicted seven Iranian hackers for attacks on the U.S. financial sector and for probing the networks of a New York dam. The same threats that leave me unable to sleep keep my friend Dr. Matania, head of the Israel National Cyber Bureau, up at night as well.

Closing our aperture of vulnerability will be difficult, Mr. Speaker, but it is possible if we work together to bring our countries' unique perspectives to bear on the problem. I know my colleagues in the Senate share these sentiments, and I hope they will move quickly to take this bill up and start fostering further collaboration as soon as possible.

Let me again thank Chairman RATCLIFFE for his leadership and his outstanding work on this bill. I urge my colleagues to support H.R. 612.

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

Mr. RATCLIFFE. Mr. Speaker, I thank the gentleman from Rhode Island for his kind words. I also thank him and commend him for his leadership on cybersecurity issues for many years in this House. I look forward to working with him for many years, hopefully, to come. I thank him for his friendship and collaboration in helping to make America safer.

Mr. Speaker, I again urge all my colleagues to support H.R. 612.

I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. RATCLIFFE) that the House suspend the rules and pass the bill, H.R. 612.

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.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, proceedings will resume on questions previously postponed.

Votes will be taken in the following order:

Ordering the previous question on House Resolution 70; and adoption of House Resolution 70, if ordered.

The first electronic vote will be conducted as a 15-minute vote. The remaining electronic vote will be conducted as a 5-minute vote.