□ 1400

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Ms. GARCIA of Texas) at 2 p.m.

PRAYER

The Chaplain, the Reverend Margaret Grun Kibben, offered the following prayer:

Holy God, You see us as we are—our strengths, our weaknesses, our accomplishments, and our shortcomings—and still You love us with a parent's heart.

God, we give You thanks for the patience You show us time and again. Despite our inclination to take things into our own hands, to fool ourselves to think that our way is the only way, to turn from Your guidance and walk away from Your loving arms, nonetheless, You stand beside, behind, and before us, ready to right us when we stumble and to reassure us when we fail.

Like a hen that broods over her nest, You gather us under Your wings and tend to our every need. Open our eyes to Your gracious care over us. Call us to seek shelter in Your encouraging embrace and to trust Your steadying hand.

We ask that You give us this day reminders of Your abiding faithfulness and enduring mercy. As we stand in the light of Your grace, may we see both our guilt and our acquittal.

Then may we find restoration and renewal to serve You as those who have been given a new chance to bask in Your love and proclaim Your compassion for all people.

In Your merciful name we pray.

Amen.

THE JOURNAL

The SPEAKER pro tempore. Pursuant to section 11(a) of House Resolution 188, the Journal of the last day's proceedings is approved.

PLEDGE OF ALLEGIANCE

The SPEAKER pro tempore. Will the gentleman from Michigan (Mr. BERGMAN) come forward and lead the House in the Pledge of Allegiance.

Mr. BERGMAN led the Pledge of Allegiance as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

MESSAGE FROM THE SENATE

A message from the Senate by Ms. Byrd, one of its clerks, announced that the Senate has agreed to without amendment a concurrent resolution of the House of the following title:

H. Con. Res. 88. Concurrent Resolution authorizing the use of the Capitol Grounds for the Greater Washington Soap Box Derby.

The message also announced that the Senate has passed bills of the following titles in which the concurrence of the House is requested:

S. 2129. An act to promote freedom of information and counter censorship and surveillance in North Korea, and for other purposes.

S. 2280. An act to provide PreCheck to certain severely injured or disabled veterans, and for other purposes.

S. 3309. An act to require SelectUSA to coordinate with State-level economic development organizations to increase foreign direct investment in semiconductor-related manufacturing and production.

RETURN TO FISCAL RESTRAINT

(Mr. JOYCE of Pennsylvania asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. JOYCE of Pennsylvania. Madam Speaker, last week, a report from Moody's found that the average American is now spending an extra $460 a month on everyday items like gas and groceries. Because of this staggering inflation caused by President Biden's failed policies, the average American family is being impacted.

The burden of this out-of-control inflation has fallen on working families, who can least afford to pay for the skyrocketing price of goods.

Now, instead of addressing the root causes of inflation, President Biden and Vice President HARRIS are once again championing their build back broken agenda, an agenda that would pour gasoline on a fire that is already far out of control.

Americans cannot afford this reckless spending, and we cannot afford to allow radical socialist policies to further destroy our Nation's economy.

It is time to return to fiscal restraint. It is time to stop spending money that we don't have. It is time to stop spending money on things that we do not need.

STOP THE SPENDING

(Mr. BERGMAN asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. BERGMAN. Madam Speaker, I have spoken before about President Biden's and House Democrats' flawed economic record. I continue to hear from constituents from across Michigan's First District who feel cast aside by the policies of this administration.

Inflation has hit a high of 8.6 percent, and this President continues to blame everyone but himself. High inflation isn't an act of God. High inflation isn't solely an act of the Federal Reserve. High inflation certainly isn't an act of Putin, either.

President Biden said the buck stops with him, but maybe he has changed his mind. Don't be deceived; his stated plan to address inflation is a farce.

The President and his advisers told the American people inflation was transitory, all while passing trillions in new spending. Instead of taking responsibility, this President continues to push tax-and-spend legislation that worsens inflation while leaving working families to pick up the tab.

I am asking the President and my colleagues to listen to the American people, stop the spending, and confront inflation head-on.

DON'T PROSECUTE BORDER PATROL AGENTS

(Mr. LAMALFA asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. LAMALFA. Madam Speaker, for months, the Democrats and the liberal media have been intentionally falsely accusing Border Patrol agents of whipping illegal immigrants coming across our southern border. The media falsely mislabeled the agents' long reins, which they use to control their horses, as whips.

Of course, where are all the fact checkers about this information? I guess they are absent over at The Washington Post and CNN.

Yet, the Biden administration's Department of Homeland Security isn't interested in the truth, either. They want to punish these Border Patrol agents who are doing their job and arresting illegal immigrants. Following a false narrative and special interest pressure, the DHS has announced plans to discipline these folks on horseback involved in the so-called incidents.

Prosecuting these law enforcement officers will do nothing but lower the already-low morale at the CBP.

The Biden administration's open-border and soft-on-crime policies have incentivized 2 million illegal immigrants to come across our southern border and have stripped Border Patrol agents from having the authority to stop it. Instead, they have become Welcome Wagon workers.

There is a caravan of illegal immigrants, nearly 20,000 strong, awaiting the day Biden fulfills his destructive promise of ending the border protections under title 42.

We need a true border policy that protects Americans.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which the yeas and nays are ordered.

The House will resume proceedings on postponed questions at a later time.

INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING ACT

Mr. SWALWELL. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 7777) to amend the Homeland

Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency to establish an industrial control systems cybersecurity training initiative, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 7777

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 ''Industrial Control Systems Cybersecurity Training Act''.

SEC. 2. ESTABLISHMENT OF THE INDUSTRIAL CONTROL SYSTEMS TRAINING INITIATIVE.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following new section:

''SEC. 2220D. INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING INITIATIVE.

''(a) ESTABLISHMENT.—

''(1) IN GENERAL.—The Industrial Control Systems Cybersecurity Training Initiative (in this section referred to as the 'Initiative') is established within the Agency.

''(2) PURPOSE.—The purpose of the Initiative is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

''(b) REQUIREMENTS.—In carrying out the Initiative, the Director shall—

''(1) ensure the Initiative includes—

''(A) virtual and in-person trainings and courses provided at no cost to participants;

''(B) trainings and courses available at different skill levels, including introductory level courses;

''(C) trainings and courses that cover cyber defense strategies for industrial control systems, including an understanding of the unique cyber threats facing industrial control systems and the mitigation of security vulnerabilities in industrial control systems technology; and

''(D) appropriate consideration regarding the availability of trainings and courses in different regions of the United States; and

''(2) engage in—

''(A) collaboration with the National Laboratories of the Department of Energy in accordance with section 309;

''(B) consultation with Sector Risk Management Agencies; and

''(C) as appropriate, consultation with private sector entities with relevant expertise, such as vendors of industrial control systems technologies.

''(c) REPORTS.—

''(1) IN GENERAL.—Not later than one year after the date of the enactment of this section and annually thereafter, the Director 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 the Initiative.

''(2) CONTENTS.—Each report under paragraph (1) shall include the following:

''(A) A description of the courses provided under the Initiative.

''(B) A description of outreach efforts to raise awareness of the availability of such courses.

''(C) Information on the number and demographics of participants in such courses, including by gender, race, and place of residence.

''(D) Information on the participation in such courses of workers from each critical infrastructure sector.

''(E) Plans for expanding access to industrial control systems education and training, including expanding access to women and underrepresented populations, and expanding access to different regions of the United States.

''(F) Recommendations on how to strengthen the state of industrial control systems cybersecurity education and training.''.

(b) 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 2220C the following new item:

''Sec. 2220D. Industrial Control Systems Cybersecurity Training Initiative.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. SWALWELL) and the gentlewoman from Iowa (Mrs. MILLER-MEEKS) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. SWALWELL. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on this measure.

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

There was no objection.

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

Madam Speaker, I thank the chairman and ranking member of the Committee on Homeland Security for their support for moving my bill, H.R. 7777, the Industrial Control Systems Cybersecurity Training Act, through committee. I thank the Speaker and majority leader for bringing this measure to the floor today.

Madam Speaker, H.R. 7777 is not only a winning number on a slot machine; it is a winning formula for bringing cyber hygiene to our industrial control systems across America.

Every day, we rely on critical infrastructure to power our homes, fuel our cars, and connect us online. One essential component of critical infrastructure is industrial control systems, also known as ICS, which digitally manage operations of these vital systems.

As Congress considers legislation to address cybersecurity threats to America's interests, my legislation would help to secure vulnerable ICS at every level of our economy and our government. H.R. 7777 would make permanent an existing education initiative within the Cybersecurity and Infrastructure Security Agency, also known as CISA.

This initiative, the ICS training initiative, provides free virtual and in-person cybersecurity training to public and private security entities, including critical infrastructure administrators, national laboratories, and even small businesses.

This training equips technology professionals across all levels with the tools and expertise necessary to secure themselves against advanced persistent threats.

When threats turn into successful attacks, it impacts the daily lives of every American, including sowing discord into our electoral processes, as we have seen election after election; shutting down our pipelines; or breaking down supply chains that provide essential food and other materials.

That means virtually everything that is connected to a network has a potential vulnerability, or what we would refer to as a left-of-boom vulnerability, the vulnerability that exists before the attack occurs. Every person, small business, or government database is a potential target.

In 2021 alone, cybercrimes inflicted approximately $6 trillion in damages across the world. Attacks on industrial networks account for a significant portion of that number, and it is only going to get worse in the future.

These threats often emerge from sophisticated state actors, like Russia and China, that have the ability to exploit vulnerabilities to disrupt and destroy the systems that make our way of life possible.

As Putin and his regime become increasingly isolated because of a successful sanctions regime and the effort that we are prosecuting to help keep Ukraine in the fight, we should expect the Kremlin to progressively target the United States and our allies with unconventional cyberattacks on our election systems and critical infrastructure. Any success that Russia has in exploiting vulnerabilities will inevitably be closely watched by other countries, particularly China.

In sum, we know this threat is real and that malignant actors will persistently probe our systems to find additional weaknesses to exploit, which would cause real harms, harms to Americans that would blunt innovation, steal American secrets, and destroy America's small businesses.

In my district, cybersecurity professionals deal with threats to ICS every single day. I specifically note two major Federal research centers, Sandia and Lawrence Livermore National Laboratories, which play a critical role in protecting against worldwide cyber threats. They are in the heart of my district in Livermore, California.

This support is leveraged every day by numerous Federal agencies, including CISA, which sit on the front lines of protecting our infrastructure from bad actors. We in Congress must do everything we can to equip our security protectors with the resources they need to continue the fight, and that is what this legislation does.

Resources must include proactive ways to help cybersecurity-focused entities retain a competitive workforce. The training programs in my legislation will equip technology professionals with the skills, expertise, and resources they need to build resilience against threats to some of our most sensitive facilities.

I applaud CISA for increasing these trainings, which H.R. 7777—which I love saying—would make permanent. This commonsense program is an easy solution to build resilience against cyberattacks for our most vulnerable systems.

Madam Speaker, I urge my House colleagues to support this legislation, and I reserve the balance of my time.

Mrs. MILLER-MEEKS. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 7777, the Industrial Control Systems Cybersecurity Training Act.

In policy discussions following recent cyber incidents, like SolarWinds and Colonial Pipeline, one constant area of concern to Congress and our cyber defenders, like the Cybersecurity and Infrastructure Security Agency, CISA, has been improving the Nation's workforce pipeline for cybersecurity and other STEM-related fields.

As the interconnectivity of our daily lives continues to grow, the estimated worldwide cost of cybercrime has risen to $6 trillion annually. Despite this alarming and growing threat, some estimates say that the cybersecurity workforce is currently short about 1 to 3 million qualified professionals.

A recent Center for Strategic and International Studies, CSIS, study of IT decisionmakers across eight countries found that 82 percent of employers report a shortage of cybersecurity skills, and 71 percent believe this talent gap causes direct and measurable damage to their organization.

□ 1415

Federal agencies have been working to bridge the gap in skills required to prepare a future cyber workforce.

CISA is collaborating closely with organizations like the National Institute of Standards and Technology, NIST, to identify cyber knowledge deficits on a sector-by-sector basis. One example is the National Initiative for Cybersecurity Education framework, which serves as a useful precursor for directing Federal resources into education and research priorities.

H.R. 7777 would require that CISA provide resources for the purpose of training cyber operators that are fluent across multiple segments of the cyber domain, not only information technology but also operational technology, like manufacturing systems and industrial control systems, which are commonplace within critical infrastructure sectors and are increasingly exposed to cyber risk.

We must continue to do all we can to improve our Nation's cyber posture and focus on policy that can help make our government and private sector critical infrastructure operations more resilient and prepared for future events.

Madam Speaker, I urge Members to join me in supporting H.R. 7777, and I yield back the balance of my time.

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

I appreciate the bipartisan, cooperative effort here to make sure that our cyber professionals across America are ready to meet the growing threats from Russia, China, and even nonstate cyber actors. That is exactly what H.R. 7777 seeks to do, by authorizing CISA's ICS cybersecurity training program and directing CISA to report to Congress annually about the initiative.

Improving the state of our cybersecurity workforce will be an ongoing effort, and these reports will help Congress continue to strengthen this program in the future.

Passing this bill will help us continue to move forward in developing the cybersecurity workforce we need to defend against the growing cyber threats that we face. In particular, this will help strengthen small businesses, particularly those in critical infrastructure, who do not yet today have cybersecurity defense forces receiving that training.

Madam Speaker, I urge my colleagues to support H.R. 7777, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. SWALWELL) that the House suspend the rules and pass the bill, H.R. 7777, as amended.

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. ROY. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

NATIONAL COMPUTER FORENSICS INSTITUTE REAUTHORIZATION ACT OF 2022

Mr. SWALWELL. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 7174) to amend the Homeland Security Act of 2002 to reauthorize the National Computer Forensics Institute of the United States Secret Service, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 7174

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 ''National Computer Forensics Institute Reauthorization Act of 2022''.

SEC. 2. REAUTHORIZATION OF THE NATIONAL COMPUTER FORENSICS INSTITUTE OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383) is amended—

(1) in subsection (a)—

(A) in the subsection heading, by striking ''IN GENERAL'' and inserting ''IN GENERAL; MISSION'';

(B) by striking ''2022'' and inserting ''2032''; and

(C) by striking the second sentence and inserting ''The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, judges, participants in the United States Secret Service's network of cyber fraud task forces, and other appropriate individuals regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Department guidance regarding privacy, civil rights, and civil liberties protections.'';

(2) by redesignating subsections (c) through (f) as subsections (d) through (g), respectively;

(3) by striking subsection (b) and inserting the following new subsections:

''(b) CURRICULUM.—In furtherance of subsection (a), all education and training of the Institute shall be conducted in accordance with relevant Federal law and policy regarding privacy, civil rights, and civil liberties protections, including best practices for safeguarding data privacy and fair information practice principles. Education and training provided pursuant to subsection (a) shall relate to the following:

''(1) Investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, including relating to instances involving illicit use of digital assets and emerging trends in cybersecurity and electronic crime.

''(2) Conducting forensic examinations of computers, mobile devices, and other information systems.

''(3) Prosecutorial and judicial considerations related to cybersecurity incidents, electronic crimes, related cybersecurity threats, and forensic examinations of computers, mobile devices, and other information systems.

''(4) Methods to obtain, process, store, and admit digital evidence in court.

''(c) RESEARCH AND DEVELOPMENT.—In furtherance of subsection (a), the Institute shall research, develop, and share information relating to investigating cybersecurity incidents, electronic crimes, and related cybersecurity threats that prioritize best practices for forensic examinations of computers, mobile devices, and other information systems. Such information may include training on methods to investigate ransomware and other threats involving the use of digital assets.'';

(4) in subsection (d), as so redesignated—

(A) by striking ''cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers and prosecutors'' and inserting ''cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a)''; and

(B) by adding at the end the following new sentence: ''The Institute shall prioritize providing education and training to individuals from geographically-diverse jurisdictions throughout the United States.'';

(5) in subsection (e), as so redesignated—

(A) by striking ''State, local, tribal, and territorial law enforcement officers'' and inserting ''recipients of education and training provided pursuant to subsection (a)''; and

(B) by striking ''necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations'' and inserting ''for investigating and preventing cybersecurity incidents, electronic crimes, related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems'';

(6) in subsection (f), as so redesignated—

(A) by amending the heading to read as follows: ''CYBER FRAUD TASK FORCES'';

(B) by striking ''Electronic Crime'' and inserting ''Cyber Fraud'';

(C) by striking ''State, local, tribal, and territorial law enforcement officers'' and inserting