Finally, during this Jewish History Month, it is a privilege to recognize a Jew who served his country and his people with distinction, honor, and success. Mr. Ferencz was the embodiment of the Biblical instruction: Justice, justice you shall pursue.

Mr. Speaker, I thank my colleague, Ms. FRANKEL, for her effort to make sure this Gold Medal is awarded to such a deserving recipient.

Mr. HILL. Mr. Speaker, I yield myself such time as I may consume, and I am prepared to close.

Mr. Speaker, let me thank Ms. FRANKEL for her leadership, Congresswoman MANNING for her testimony there, and we all, on both sides of the aisle, stand in recognition of Ben Ferencz' pioneering efforts of his and his colleagues in the Nuremberg trials for laying out the protection of evidence, the careful documentation of it, preserving a way to convict the perpetrators of the Holocaust.

Those lessons and Ben Ferencz' legacy live on today, as just a few months ago we received one of our first convictions in a court in Germany of an Assad henchman for murder and mayhem in Syria. There is no doubt in my mind that the chain of evidence and the actions of this Congress, the actions of the United Nations, to promptly set up an evidence protection and evidence documentation effort for Ukraine will bear fruit in coming days. Those are all efforts standing on the shoulders of Ben Ferencz and his colleagues in Nuremburg.

I urge all my colleagues to support this recognition of his efforts.

Mr. Speaker, I urge a ''yes'' vote, and I yield back the balance of my time.

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

Mr. Speaker, I thank my colleagues, the gentlewoman from Florida, Congresswoman FRANKEL, for her leadership in sponsoring H.R. 6015, and for working so hard to ensure that Mr. Ferencz receives the recognition that he so clearly deserves.

Through his prosecutorial work, his teaching, his written works and his advocacy, for the establishment of the International Criminal Court, he has directly and indirectly brought countless criminals to justice and left a lasting humanitarian legacy.

The recent reports of Russian atrocities being committed against the people of Ukraine are a reminder that war crimes are far from being a relic of a past.

Now more than ever, we must act to honor and uplift those who have dedicated their lives to advancing justice, peace, and giving a voice to the voiceless.

Mr. Speaker, I urge my colleagues to vote ''yes'' on H.R. 6015, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Illinois (Mr. GARCÍA) that the House suspend the rules and pass the bill, H.R. 6015, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

□ 1730

SUPPLY CHAIN SECURITY TRAINING ACT OF 2021

Mr. CONNOLLY. Mr. Speaker, I move to suspend the rules and pass the bill (S. 2201) to manage supply chain risk through counterintelligence training, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 2201

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 ''Supply Chain Security Training Act of 2021''.

SEC. 2. TRAINING PROGRAM TO MANAGE SUPPLY CHAIN RISK.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of General Services, through the Federal Acquisition Institute, shall develop a training program for officials with supply chain risk management responsibilities at Federal agencies.

(b) CONTENT.—The training program shall be designed to prepare such personnel to perform supply chain risk management activities and identify and mitigate supply chain security risks that arise throughout the acquisition lifecycle, including for the acquisition of information and communications technology. The training program shall—

(1) include, considering the protection of classified and other sensitive information, information on current, specific supply chain security threats and vulnerabilities; and

(2) be updated as determined to be necessary by the Administrator.

(c) COORDINATION AND CONSULTATION.—In developing and determining updates to the training program, the Administrator shall—

(1) coordinate with the Federal Acquisition Security Council, the Secretary of Homeland Security, and the Director of the Office of Personnel Management; and

(2) consult with the Director of the Department of Defense's Defense Acquisition University, the Director of National Intelligence, and the Director of the National Institute of Standards and Technology.

(d) GUIDANCE.—

(1) IN GENERAL.—Not later than 180 days after the training program is developed under subsection (a), the Director of the Office of Management and Budget shall promulgate guidance to Federal agencies requiring executive agency adoption and use of the training program. Such guidance shall—

(A) allow executive agencies to incorporate the training program into existing agency training programs; and

(B) provide guidance on how to identify executive agency officials with supply chain risk management responsibilities.

(2) AVAILABILITY.—The Director of the Office of Management and Budget shall make the guidance promulgated under paragraph (1) available to Federal agencies of the legislative and judicial branches.

SEC. 3. REPORTS ON IMPLEMENTATION OF PROGRAM.

Not later than 180 days after the completion of the first course, and annually thereafter for the next three years, the Administrator of General Services shall submit to the appropriate congressional committees and leadership a report on implementation of the training program required under section 2.

SEC. 4. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate; and

(B) the Committee on Oversight and Reform and the Committee on Armed Services of the House of Representatives.

(2) INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term ''information and communications technology'' has the meaning given the term in section 4713(k) of title 41, United States Code.

(3) EXECUTIVE AGENCY.—The term ''executive agency'' has the meaning given the term in section 133 of title 41, United States Code.

(4) FEDERAL AGENCY.—The term ''Federal agency'' means any agency, committee, commission, office, or other establishment in the executive, legislative, or judicial branch of the Federal Government.

(5) TRAINING PROGRAM.—The term ''training program'' means the training program developed pursuant to section 2(a).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Virginia (Mr. CONNOLLY) and the gentlewoman from South Carolina (Ms. MACE) each will control 20 minutes.

The Chair recognizes the gentleman from Virginia.

GENERAL LEAVE

Mr. CONNOLLY. Mr. 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 Virginia?

There was no objection.

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

Mr. Speaker, I rise in support of S. 2201, the Supply Chain Security Training Act, led by Chairman GARY PETERS of the Committee on Homeland Security and Governmental Affairs and Senator RON JOHNSON of Wisconsin.

I thank Representatives JOE NEGUSE and SCOTT FRANKLIN, who did excellent bipartisan work here to lead the House companion, H.R. 5962, which was reported by the Oversight and Reform Committee on February 4 without opposition.

This important bill to defend our Nation's information and communications technology supply chains cannot be enacted soon enough.

In December 2020, a Government Accountability Office report revealed that Federal agencies had failed to fully implement supply chain and risk management standards for information and communications technology.

That same month, the discovery of the SolarWinds breach made urgently clear how dangerous supply chain vulnerabilities can be. The networks of at least nine Federal agencies were compromised by Russian actors, allowing

them access to Federal systems for months before they were even discovered.

To help address these concerns, the Supply Chain Security Training Act establishes a training program for agency employees with responsibilities related to supply chain risk management, better preparing them to identify and mitigate supply chain threats associated with the acquisition of products and services.

The training requirements created by this bill will ensure that the acquisition workforce has the capability to identify items in the supply chain that could be used to exploit Federal information systems.

As the largest purchaser of goods and services in the world, the Federal Government relies on a complex supply chain that spans continents and is continuously targeted by foreign adversaries and cybercriminals scheming to breach Federal information systems.

To protect our national security interests and guard against these attacks, we must equip our Federal acquisition officials with the expertise and skills they need to reinforce our cybersecurity defenses through purchasing decisions.

I encourage my colleagues to support this bill, and I reserve the balance of my time.

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

Mr. Speaker, recent cyberattacks on the U.S. Government continue to reveal weaknesses in our Federal information technology systems. One such weakness resides in the software products Federal agencies purchase from the private sector.

IT and software products, like most goods and services, now rely on global supply chains for their development, and this means increased vulnerabilities to threats from malicious and criminal actors, as well as our foreign enemies, as my colleague, Mr. CONNOLLY, just recognized.

Congress must ensure Federal agencies proactively address supply chain security risks. The Supply Chain Security Training Act will ensure the Federal workforce properly understands these supply chain risks and the appropriate policies to implement to address the risks.

Specifically, the bill tasks the General Services Administration with developing, and the Office of Management and Budget, OMB, with implementing a governmentwide supply chain security training program. This training will prepare the Federal workforce to better identify and mitigate the security risks throughout the acquisition lifecycle of information and communications technology products and services. For instance, Federal agency personnel would be better able to recognize and avoid purchasing software products with malware vulnerabilities.

This is smart legislation that builds on existing congressional reforms. For instance, the bill requires coordination with the existing Federal Acquisition Security Council, an interagency effort established by Congress in 2018 to develop policies and procedures addressing supply chain risks.

Despite these existing efforts, there are currently no Federal workforce training requirements in place to ensure supply chain security policies are properly and consistently implemented. The national security stakes are too high to leave such a strategic gap in our Federal defenses.

S. 2201 represents a practical policy reform to a very real threat. I appreciate my colleagues Representatives NEGUSE and FRANKLIN's leadership on championing the House companion bill, H.R. 5962.

I look forward to seeing the Supply Chain Security Training Act pass the House and advance to the President's desk.

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

Mr. CONNOLLY. Mr. Speaker, I have no further speakers on this side. I reserve the balance of my time.

Ms. MACE. Mr. Speaker, I also want to again recognize my colleagues, Representatives NEGUSE and FRANKLIN, who crafted the House companion legislation, H.R. 5962.

I encourage my colleagues to support this bill, and I yield back the balance of my time.

Mr. CONNOLLY. Mr. Speaker, I thank my friend from South Carolina for her leadership and support on this important piece of legislation, which will help guard Federal assets.

I urge passage of the bill, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Virginia (Mr. CONNOLLY) that the House suspend the rules and pass the bill, S. 2201.

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.

FEDERAL ROTATIONAL CYBER WORKFORCE PROGRAM ACT OF 2021

Mr. CONNOLLY. Mr. Speaker, I move to suspend the rules and pass the bill (S. 1097) to establish a Federal rotational cyber workforce program for the Federal cyber workforce.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 1097

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 ''Federal Rotational Cyber Workforce Program Act of 2021''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given the term ''Executive agency'' in section 105 of title 5, United States Code, except that the term does not include the Government Accountability Office.

(2) COMPETITIVE SERVICE.—The term ''competitive service'' has the meaning given that term in section 2102 of title 5, United States Code.

(3) COUNCILS.—The term ''Councils'' means—

(A) the Chief Human Capital Officers Council established under section 1303 of the Chief Human Capital Officers Act of 2002 (5 U.S.C. 1401 note); and

(B) the Chief Information Officers Council established under section 3603 of title 44, United States Code.

(4) CYBER WORKFORCE POSITION.—The term ''cyber workforce position'' means a position identified as having information technology, cybersecurity, or other cyber-related functions under section 303 of the Federal Cybersecurity Workforce Assessment Act of 2015 (5 U.S.C. 301 note).

(5) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(6) EMPLOYEE.—The term ''employee'' has the meaning given the term in section 2105 of title 5, United States Code.

(7) EMPLOYING AGENCY.—The term ''employing agency'' means the agency from which an employee is detailed to a rotational cyber workforce position.

(8) EXCEPTED SERVICE.—The term ''excepted service'' has the meaning given that term in section 2103 of title 5, United States Code.

(9) ROTATIONAL CYBER WORKFORCE POSITION.—The term ''rotational cyber workforce position'' means a cyber workforce position with respect to which a determination has been made under section 3(a)(1).

(10) ROTATIONAL CYBER WORKFORCE PROGRAM.—The term ''rotational cyber workforce program'' means the program for the detail of employees among rotational cyber workforce positions at agencies.

(11) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

SEC. 3. ROTATIONAL CYBER WORKFORCE POSITIONS.

(a) DETERMINATION WITH RESPECT TO ROTATIONAL SERVICE.—

(1) IN GENERAL.—The head of each agency may determine that a cyber workforce position in that agency is eligible for the rotational cyber workforce program, which shall not be construed to modify the requirement under section 4(b)(3) that participation in the rotational cyber workforce program by an employee shall be voluntary.

(2) NOTICE PROVIDED.—The head of an agency shall submit to the Director—

(A) notice regarding any determination made by the head of the agency under paragraph (1); and

(B) for each position with respect to which the head of the agency makes a determination under paragraph (1), the information required under subsection (b)(1).

(b) PREPARATION OF LIST.—The Director, with assistance from the Councils and the Secretary, shall develop a list of rotational cyber workforce positions that—

(1) with respect to each such position, to the extent that the information does not disclose sensitive national security information, includes—

(A) the title of the position;

(B) the occupational series with respect to the position;

(C) the grade level or work level with respect to the position;

(D) the agency in which the position is located;

(E) the duty location with respect to the position; and