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

(F) the major duties and functions of the position; and

(2) shall be used to support the rotational cyber workforce program.

(c) DISTRIBUTION OF LIST.—Not less frequently than annually, the Director shall distribute an updated list developed under subsection (b) to the head of each agency and other appropriate entities.

SEC. 4. ROTATIONAL CYBER WORKFORCE PROGRAM.

(a) OPERATION PLAN.—

(1) IN GENERAL.—Not later than 270 days after the date of enactment of this Act, and in consultation with the Councils, the Secretary, representatives of other agencies, and any other entity as the Director determines appropriate, the Director shall develop and issue a Federal Rotational Cyber Workforce Program operation plan providing policies, processes, and procedures for a program for the detailing of employees among rotational cyber workforce positions at agencies, which may be incorporated into and implemented through mechanisms in existence on the date of enactment of this Act.

(2) UPDATING.—The Director may, in consultation with the Councils, the Secretary, and other entities as the Director determines appropriate, periodically update the operation plan developed and issued under paragraph (1).

(b) REQUIREMENTS.—The operation plan developed and issued under subsection (a) shall, at a minimum—

(1) identify agencies for participation in the rotational cyber workforce program;

(2) establish procedures for the rotational cyber workforce program, including—

(A) any training, education, or career development requirements associated with participation in the rotational cyber workforce program;

(B) any prerequisites or requirements for participation in the rotational cyber workforce program; and

(C) appropriate rotational cyber workforce program performance measures, reporting requirements, employee exit surveys, and other accountability devices for the evaluation of the program;

(3) provide that participation in the rotational cyber workforce program by an employee shall be voluntary;

(4) provide that an employee shall be eligible to participate in the rotational cyber workforce program if the head of the employing agency of the employee, or a designee of the head of the employing agency of the employee, approves of the participation of the employee;

(5) provide that the detail of an employee to a rotational cyber workforce position under the rotational cyber workforce program shall be on a nonreimbursable basis;

(6) provide that agencies may agree to partner to ensure that the employing agency of an employee that participates in the rotational cyber workforce program is able to fill the position vacated by the employee;

(7) require that an employee detailed to a rotational cyber workforce position under the rotational cyber workforce program, upon the end of the period of service with respect to the detail, shall be entitled to return to the position held by the employee, or an equivalent position, in the employing agency of the employee without loss of pay, seniority, or other rights or benefits to which the employee would have been entitled had the employee not been detailed;

(8) provide that discretion with respect to the assignment of an employee under the rotational cyber workforce program shall remain with the employing agency of the employee;

(9) require that an employee detailed to a rotational cyber workforce position under the rotational cyber workforce program in an agency that is not the employing agency of the employee shall have all the rights that would be available to the employee if the employee were detailed under a provision of law other than this Act from the employing agency to the agency in which the rotational cyber workforce position is located;

(10) provide that participation by an employee in the rotational cyber workforce program shall not constitute a change in the conditions of the employment of the employee; and

(11) provide that an employee participating in the rotational cyber workforce program shall receive performance evaluations relating to service in the rotational cyber workforce program in a participating agency that are—

(A) prepared by an appropriate officer, supervisor, or management official of the employing agency, acting in coordination with the supervisor at the agency in which the employee is performing service in the rotational cyber workforce position;

(B) based on objectives identified in the operation plan with respect to the employee; and

(C) based in whole or in part on the contribution of the employee to the agency in which the employee performed such service, as communicated from that agency to the employing agency of the employee.

(c) PROGRAM REQUIREMENTS FOR ROTATIONAL SERVICE.—

(1) IN GENERAL.—An employee serving in a cyber workforce position in an agency may, with the approval of the head of the agency, submit an application for detail to a rotational cyber workforce position that appears on the list developed under section 3(b).

(2) OPM APPROVAL FOR CERTAIN POSITIONS.—An employee serving in a position in the excepted service may only be selected for a rotational cyber workforce position that is in the competitive service with the prior approval of the Office of Personnel Management, in accordance with section 300.301 of title 5, Code of Federal Regulations, or any successor thereto.

(3) SELECTION AND TERM.—

(A) SELECTION.—The head of an agency shall select an employee for a rotational cyber workforce position under the rotational cyber workforce program in a manner that is consistent with the merit system principles under section 2301(b) of title 5, United States Code.

(B) TERM.—Except as provided in subparagraph (C), and notwithstanding section 3341(b) of title 5, United States Code, a detail to a rotational cyber workforce position shall be for a period of not less than 180 days and not more than 1 year.

(C) EXTENSION.—The Chief Human Capital Officer of the agency to which an employee is detailed under the rotational cyber workforce program may extend the period of a detail described in subparagraph (B) for a period of 60 days unless the Chief Human Capital Officer of the employing agency of the employee objects to that extension.

(4) WRITTEN SERVICE AGREEMENTS.—

(A) IN GENERAL.—The detail of an employee to a rotational cyber workforce position shall be contingent upon the employee entering into a written service agreement with the employing agency under which the employee is required to complete a period of employment with the employing agency following the conclusion of the detail that is equal in length to the period of the detail.

(B) OTHER AGREEMENTS AND OBLIGATIONS.—A written service agreement under subparagraph (A) shall not supersede or modify the terms or conditions of any other service agreement entered into by the employee under any other authority or relieve the obligations between the employee and the employing agency under such a service agreement. Nothing in this subparagraph prevents an employing agency from terminating a service agreement entered into under any other authority under the terms of such agreement or as required by law or regulation.

SEC. 5. REPORTING BY GAO.

Not later than the end of the third fiscal year after the fiscal year in which the operation plan under section 4(a) is issued, the Comptroller General of the United States shall submit to Congress a report assessing the operation and effectiveness of the rotational cyber workforce program, which shall address, at a minimum—

(1) the extent to which agencies have participated in the rotational cyber workforce program, including whether the head of each such participating agency has—

(A) identified positions within the agency that are rotational cyber workforce positions;

(B) had employees from other participating agencies serve in positions described in subparagraph (A); and

(C) had employees of the agency request to serve in rotational cyber workforce positions under the rotational cyber workforce program in participating agencies, including a description of how many such requests were approved; and

(2) the experiences of employees serving in rotational cyber workforce positions under the rotational cyber workforce program, including an assessment of—

(A) the period of service;

(B) the positions (including grade level and occupational series or work level) held by employees before completing service in a rotational cyber workforce position under the rotational cyber workforce program;

(C) the extent to which each employee who completed service in a rotational cyber workforce position under the rotational cyber workforce program achieved a higher skill level, or attained a skill level in a different area, with respect to information technology, cybersecurity, or other cyber-related functions; and

(D) the extent to which service in rotational cyber workforce positions has affected intra-agency and interagency integration and coordination of cyber practices, functions, and personnel management.

SEC. 6. SUNSET.

Effective 5 years after the date of enactment of this Act, this Act is repealed.

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 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. 1097, the Federal Rotational Cyber Workforce Program Act. The bill was introduced by Senator PETERS with bipartisan support here in the House

with the companion legislation introduced by Representatives RO KHANNA and NANCY MACE.

The Federal Rotational Cyber Workforce Program Act enables cybersecurity professionals in the Federal Government to rotate through assignments outside of their regular position or agency on a voluntary basis.

The Office of Personnel Management would establish guidelines for the implementation of the program. The program would be authorized for 5 years, and after 3 years, the Government Accountability Office would assess its operation and effectiveness.

Achieving cybersecurity in response to the threats the Nation faces was identified in GAO's latest ''High Risk List'' as an area where the government is actually regressing. GAO reported that Federal agencies are struggling to ensure that staff have the skills required to address the critical cybersecurity risks that continue to intensify.

The program this bill creates allows the government to have its security employees to further develop their skills and agencies across the government to benefit from the employees' expertise.

Recent cyberattacks in both the private and public sectors have demonstrated the dire consequences of failing to improve the Federal Government's cybersecurity operations.

We know that adversaries in Russia, China, and other malign actors, state and nonstate, are consistently working to breach the U.S. Government's communications and data. Unfortunately, at times, they have been all too successful. In the 2020 SolarWinds breach, for example, Russian hackers infiltrated the networks of nine Federal agencies and went undetected for months.

This bill goes a long way toward improving Federal agencies' capacity to strengthen cybersecurity operations, help them retain top talent in that field, and facilitate the exchange of expertise in this critical area.

The security of Federal information technology systems and data is a national security priority, and it ought to be. It is essential to preserving public trust in government institutions and ensuring that agencies are better equipped to meet their missions in serving the American people.

I strongly support the bill, and I urge my colleagues to do the same. I reserve the balance of my time.

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

Mr. Speaker, the U.S. Government is under constant attack. We watch news story after news story of private companies being attacked by hackers across the country and, quite frankly, across the world. But our Federal agencies are also vulnerable.

Malicious hackers try to steal sensitive public information and disrupt the missions of our Federal agencies. In fact, in 2020, there were 11 Federal agencies that were hacked by actors aligned with countries like China and—you guessed it—Russia. And all too often, these malicious actors are successful.

My colleague, Representative RO KHANNA, and I recognized this reality and crafted the House companion bill legislation to the Senate bill we are considering today. That companion bill is H.R. 3599.

The Federal Rotational Cyber Workforce Program Act continues the Trump administration's efforts as laid out in the ''America's Cybersecurity Workforce'' executive order. This executive order promoted cyber rotational details at the Department of Homeland Security. Such programs help Federal cyber experts gain more diverse professional experiences and continue to sharpen their skills.

Our Nation's cyber readiness depends on maintaining a skilled Federal workforce to defend against constant attacks. Specifically, this bill establishes an additional governmentwide rotational opportunity for cyber-focused professionals.

The bill has necessary congressional oversight mechanisms, such as a requirement for a detailed operational plan and a future Government Accountability Office review. This will help Congress understand if the program is running as intended. Additionally, a 5-year sunset will provide Congress an opportunity to evaluate the program and decide whether to renew it for future years.

I thank my House and Senate colleagues for their work on this bipartisan bill, which builds upon the cyber workforce efforts of the prior administration, and I encourage my colleagues to support S. 1097 and send this necessary bill to the President's desk.

To any teenager who loves to code out there today, I encourage all of you to look at cybersecurity jobs and opportunities in your near future because we will need you in our workforce.

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

Mr. CONNOLLY. Mr. Speaker, I inform the House I have no further speakers, and I reserve the balance of my time.

Ms. MACE. Mr. Speaker, now more than ever, the cyber workforce of our Federal agencies needs to be well equipped to address the constant threats we face.

By expanding cyber rotation programs under this bill, we will help Federal agencies gain valuable experience and share best practices across the government.

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

Mr. CONNOLLY. Mr. Speaker, I congratulate my colleague from South Carolina for her leadership on a very important matter, and I urge passage of this important piece of legislation.

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. 1097.

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.

TARGETING RESOURCES TO COMMUNITIES IN NEED ACT OF 2022

Mr. CONNOLLY. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6531) to provide an increased allocation of funding under certain programs for assistance in areas of persistent poverty, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6531

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 ''Targeting Resources to Communities in Need Act of 2022''.

SEC. 2. INCREASING SHARE OF FEDERAL RESOURCES TO AREAS OF PERSISTENT POVERTY AND OTHER HIGH-POVERTY AREAS.

(a) INCREASING SHARE OF FEDERAL RESOURCES.—

(1) GUIDANCE AND MEASURES TO INCREASE FEDERAL INVESTMENTS.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with Federal agencies, shall implement guidance to increase the share of Federal investments targeted to—

(A) areas of persistent poverty; and

(B) other areas of high and persistent poverty that the Director, in consultation with Federal agencies, determines to be appropriate.

(2) GUIDANCE FOR AGENCIES.—Not later than 120 days after the date of enactment of this Act, the Director shall issue guidance to Federal agencies identifying—

(A) the scope and type of programs subject to the guidance and measures required by paragraph (1);

(B) the share of Federal investments to be targeted to the areas described under paragraph (1);

(C) the manner in which Federal investments are to be targeted to the areas described under paragraph (1); and

(D) measures to track the Federal investments targeted to the areas described under paragraph (1) over time.

(3) INVESTMENT AMOUNT.—In developing the guidance and measures under paragraph (1), the Director shall include a minimum goal that Federal investments targeted to areas of persistent poverty or other areas with high and persistent poverty be in an amount that is greater than the amount that is proportional to the population of such areas in the United States relative to the population of the United States as a whole.

(4) REPORTS TO CONGRESS.—The Director, in consultation with Federal agencies, shall submit each fiscal year to the appropriate committees of Congress a report that includes—

(A) a list of the programs, by agency, under which the amount of Federal funds targeted to areas described under paragraph (1) were increased in the previous fiscal year, in accordance with such paragraph; and