

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from the District of Columbia (Ms. NORTON) that the House suspend the rules and pass the bill, H.R. 3533, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the yeas have it.

Mrs. GREENE of Georgia. Mr. 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.

# FEDERAL ROTATIONAL CYBER WORKFORCE PROGRAM ACT OF 2021

Ms. NORTON. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3599) to establish a Federal rotational cyber workforce program for the Federal cyber workforce, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3599

*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 par-

ticipation 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 expected 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.

**SEC. 7. DETERMINATION OF BUDGETARY EFFECTS.**

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled “Budgetary Effects of PAYGO Legislation” for this Act, submitted for printing in the Congressional Record by the Chairman of the House Budget Committee, provided that such statement has been submitted prior to the vote on passage.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from the District of Columbia (Ms. NORTON) and the gentleman from Pennsylvania (Mr. KELLER) each will control 20 minutes.

The Chair recognizes the gentlewoman from the District of Columbia.

**GENERAL LEAVE**

Ms. NORTON. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days within which to revise and extend their remarks and insert extraneous material on H.R. 3599.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from the District of Columbia? There was no objection.

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

Mr. Speaker, I rise to support H.R. 3599, the Federal Rotational Cyber Workforce Program Act. This bill is the product of bipartisan cooperation of our Oversight and Reform Committee members, Representatives RO KHANNA and NANCY MACE, and I want to thank them for their work on this bill.

Earlier this year, our committee held a hearing on the Government Accountability Office’s 2021 High-Risk Report, which details the areas of government operations at greatest risk of failing to meet the considerable challenges they face.

Cybersecurity was near the top of the list, along with the cyber skills gap that persists across the Federal workforce. As the Government Accountability Office report described, Federal agencies are struggling to ensure that staff have the skills required to address the critical cybersecurity risks and challenges that our government faces.

Recent cyberattacks have demonstrated the dire consequences of failing to improve the Federal Government’s cybersecurity operations. These include the SolarWinds breach, in

which Russian hackers infiltrated the networks of nine Federal agencies and went undetected for months.

Around the same time, cyberattacks linked to the Chinese government targeted Microsoft’s enterprise email software and threatened the internal data of Federal agencies. In addition, Russian hackers successfully breached the servers of the U.S. Department of State and stole thousands of emails.

The Federal Rotational Cyber Workforce Program Act, as it is called, would enable cybersecurity professionals in the Federal Government to rotate through assignments outside of their regular position. This would allow more agencies to benefit from their enterprise and give program participants the opportunities for professional development. The program would be authorized for 5 years and, after 3 years, the Government Accountability Office would assess the operation and effectiveness of the program.

This legislation would go a long way toward improving Federal agencies’ capacity to strengthen cybersecurity operations, help retain top talent, and facilitate the exchange of expertise in this critical field.

The security of Federal information technology systems and data is essential to national security, to preserving public trust in government institutions, and to ensuring that agencies meet their missions in serving the American people.

I strongly support this bill, and I urge my colleagues to do the same.

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

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

Mr. Speaker, the Federal Government has significant work to do on the cybersecurity front. My colleagues, Representatives KHANNA and MACE, recognized this harsh reality when crafting their bill to improve our Federal workforce’s cybersecurity and IT expertise.

We face many challenges, including adequately securing IT infrastructure from cyber intrusions, supply chain hacks, and ransomware, each the subject of recent front-page news.

Our cyber readiness depends, in part, upon our ability to maintain a prepared and capable Federal workforce to defend our Nation’s government from a relentless onslaught of cyberattacks.

Toward that end, the Federal Rotational Cyber Workforce Program Act continues efforts created and implemented during the Trump administration to promote cyber rotational details throughout Federal agencies so that our valuable Federal cyber experts continue to sharpen their skills.

This bill seeks to codify an additional rotational opportunity for cyber-focused professionals throughout the Federal Government.

Former President Trump’s executive order, “America’s Cybersecurity Workforce,” established a mechanism for Federal employees to be detailed to

other agencies through a cybersecurity rotational assignment program. The Federal Rotational Cyber Workforce Program Act places management of a similar type of program under the Office of Personnel Management.

Importantly, for oversight purposes, the bill establishes requirements for a detailed operational plan and a report from the Government Accountability Office to enable congressional oversight. This will help Congress evaluate whether the rotational program is running as intended and meaningfully addressing both personnel and agency needs.

If this new rotational program is not providing the intended value to the Federal Government, then Congress will have the opportunity to decline reauthorizing the program after it sunsets in 5 years. This is a valuable safety valve to the expansion of the Federal Government, which I am glad to see included in this bill.

I thank my colleagues for their work on this bipartisan bill, which builds upon the cyber workforce efforts of the prior administration.

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

Ms. NORTON. Mr. Speaker, I yield 2 minutes to the gentleman from California (Mr. KHANNA).

Mr. KHANNA. Mr. Speaker, I thank Delegate NORTON for her leadership, and I thank Ranking Member COMER for his leadership on the bill and, of course, Representative MACE, who has been a colleague and helped craft this.

Everyone recognizes that our country faces cyberattacks. In the private sector, we don't silo cybersecurity officials. You don't say, "You just work in one department." They rotate through a company. We shouldn't have separate silos in the Federal Government.

This bill is just common sense. It says that we need to have a rotational system in the Federal Government so that you can have expertise from all the different agencies, and we can have a comprehensive response. It helps us get talent. And it is bipartisan.

We should give credit to the previous administration for having, as was pointed out, the executive order. I worked with Matt Lira at the previous White House. There is nothing that is partisan about making sure that America isn't attacked with cybercrimes and cyberattacks. That is a bipartisan initiative, and this does build on the work they did. It makes it stronger, and we put, ultimately, resources toward it.

But I am proud of the work. I am proud of working with Representative MACE on it. Frankly, I think we ought to be doing more things in this body in a bipartisan way that strengthen American security.

Mr. KELLER. Mr. Speaker, I yield such time as she may consume to the gentlewoman from South Carolina (Ms. MACE).

Ms. MACE. Mr. Speaker, today, I rise in support of H.R. 3599, the Federal Ro-

tational Cyber Workforce Program Act. It is a long title, but it is a very good bill. I thank my colleague, Ro KHANNA, for his leadership.

Cybersecurity is national security, and this is one area where it is not Democrat or Republican. When 11 Federal agencies were hacked last year by an organization affiliated with Russia, they didn't care if you had an R or a D by your name.

Imagine if, in the Federal Government, or at least a portion of the Federal Government, we could work and operate more like a business than a bureaucracy. Well, we can do that right here today with H.R. 3599.

I thank, again, Ro KHANNA for his leadership and for allowing me the opportunity to work together with him on this. This is the third bill I have worked on that I hope will pass on the floor of the House tonight.

We have an opportunity to show tremendous leadership here today. I have heard a number of my colleagues here this afternoon, Republicans and Democrats, working together for the American people, putting the American people first, and that is what we are doing.

Every day, criminal elements are attempting to steal our secrets, disrupt our infrastructure, and damage our economy by extorting money from businesses and organizations across the United States.

Most recently, in the State of South Carolina, we saw the high-profile Colonial Pipeline hacking and attack. It is a reminder that America's adversaries are creative and cunning and that our government must be the same to combat this growing threat.

It is imperative that our government be able to obtain, train, and retain the cyber and technology talent needed to counter these sophisticated hackers across the globe. The Federal Rotational Cyber Workforce Program Act will allow Federal employees to collaborate and broaden their work experiences, their knowledge, and their skill sets across Federal agencies, much in the same way their counterparts do in the private sector.

I thank my colleagues today, Republicans and Democrats, and I urge each and every one of them to vote in favor of this legislation this evening.

Mr. KELLER. Mr. Speaker, I have no further speakers, and I am prepared to close.

Mr. Speaker, it is important to improve the readiness of our Nation's cyber workforce through the expansion of cyber rotations between our Federal agencies. I encourage my colleagues to support this important legislation.

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

Ms. NORTON. Mr. Speaker, I urge passage of H.R. 3599, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from the District of Columbia (Ms. NORTON) that the House suspend the rules and pass the bill, H.R. 3599, 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.

Mrs. GREENE of Georgia. Mr. 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.

□ 1630

# DISTRICT OF COLUMBIA CHIEF FINANCIAL OFFICER SALARY HOME RULE ACT

Ms. NORTON. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1204) to amend the District of Columbia Home Rule Act to permit the District of Columbia to establish the rate of pay of the Chief Financial Officer of the District of Columbia.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1204

*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 "District of Columbia Chief Financial Officer Salary Home Rule Act".

## SEC. 2. PERMITTING DISTRICT OF COLUMBIA TO ESTABLISH RATE OF PAY OF CHIEF FINANCIAL OFFICER OF DISTRICT OF COLUMBIA.

Section 424(b)(2)(E) of the District of Columbia Home Rule Act (sec. 1-204.24b(b)(5), D.C. Official Code) is amended to read as follows:

"(E) PAY.—The Chief Financial Officer shall be paid at the greater of—

"(i) a rate such that the total amount of compensation paid during any calendar year is equal to the limit on total pay which is applicable during the year under section 5307 of title 5, United States Code, to an employee described in section 5307(d) of such title; or

"(ii) a rate established in law by the District of Columbia, except that any rate established under this clause which is applicable to any individual serving as the Chief Financial Officer shall not be reduced during any period of the individual's service as Chief Financial Officer."

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from the District of Columbia (Ms. NORTON) and the gentleman from Pennsylvania (Mr. KELLER) each will control 20 minutes.

The Chair recognizes the gentlewoman from the District of Columbia.

## GENERAL LEAVE

Ms. NORTON. 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 the measure before us.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from the District of Columbia?

There was no objection.

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