the gentlewoman from New York (Ms. CLARKE) that the House suspend the rules and pass the bill, H.R. 3138, 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. BISHOP of North Carolina. 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.

DHS INDUSTRIAL CONTROL SYSTEMS CAPABILITIES ENHANCEMENT ACT OF 2021

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 1833) to amend the Homeland Security Act of 2002 to provide for the responsibility of the Cybersecurity and Infrastructure Security Agency to maintain capabilities to identify threats to industrial control systems, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1833

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 ''DHS Industrial Control Systems Capabilities Enhancement Act of 2021''.

SEC. 2. CAPABILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS.

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (e)(1)—

(A) in subparagraph (G), by striking ''and'' after the semicolon;

(B) in subparagraph (H), by inserting ''and'' after the semicolon; and

(C) by adding at the end the following new subparagraph:

''(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;''; and

(2) by adding at the end the following new subsection:

''(p) INDUSTRIAL CONTROL SYSTEMS.—The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

''(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

''(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

''(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;

''(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and

''(5) conduct such other efforts and assistance as the Secretary determines appropriate.''.

(b) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act and every six months thereafter during the subsequent 4-year period, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the industrial control systems capabilities of the Agency under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a).

(c) GAO REVIEW.—Not later than two years after the date of the enactment of this Act, the Comptroller General of the United States shall review implementation of the requirements of subsections (e)(1)(I) and (p) of section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a), and submit to the Committee on Homeland Security in the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate a report containing findings and recommendations relating to such implementation. Such report shall include information on the following:

(1) Any interagency coordination challenges to the ability of the Director of the Cybersecurity and Infrastructure Agency of the Department of Homeland Security to lead Federal efforts to identify and mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(1) of such section.

(2) The degree to which the Agency has adequate capacity, expertise, and resources to carry out threat hunting and incident response capabilities to mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(2) of such section, as well as additional resources that would be needed to close any operational gaps in such capabilities.

(3) The extent to which industrial control system stakeholders sought cybersecurity technical assistance from the Agency pursuant to subsection (p)(3) of such section, and the utility and effectiveness of such technical assistance.

(4) The degree to which the Agency works with security researchers and other industrial control systems stakeholders, pursuant to subsection (p)(4) of such section, to provide vulnerability information to the industrial control systems community.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New York (Ms. CLARKE) and the gentleman from New York (Mr. KATKO) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

GENERAL LEAVE

Ms. CLARKE of New York. 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 gentlewoman from New York?

There was no objection.

Ms. CLARKE of New York. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in support of H.R. 1833, the DHS Industrial Control Systems Capabilities Enhancement Act.

This bill seeks to give the Cybersecurity and Infrastructure Security Agency, or CISA, a stronger hand in securing industrial control systems and would help to clarify its central coordination role across the Federal Government.

□ 1315

The importance of securing industrial control systems cannot be overstated. We rely on these systems to provide vital services, like water treatment, energy distribution, and critical manufacturing.

As control systems have grown more and more connected to business and IT networks that rely on the internet, we have seen systems become more vulnerable to cyberattacks.

Industrial control systems have been targeted by groups closely aligned with nation-states like China and Russia who seek to undermine the United States and advance their own geopolitical interests.

We have also seen criminal groups, like the perpetrators of the ransomware attack on the Colonial Pipeline, create great economic disruption while extorting companies.

It doesn't take a criminal mastermind to infiltrate an industrial environment, either. Earlier this year, an unsophisticated, unknown perpetrator was able to breach a water treatment plant in Oldsmar, Florida, and manipulate chemical levels in ways that could have poisoned nearby residents.

H.R. 1833 will strengthen CISA's authority as the lead Federal coordinator for securing industrial control systems and empower CISA to hunt for threats, respond to incidents, and to promote strong cybersecurity for critical infrastructure.

The Department of Homeland Security has been working on control system security since 2004. H.R. 1833 recognizes that role at a pivotal time as cyber threats to critical infrastructure reach new heights.

Importantly, this bill also includes a GAO review of whether CISA has the resources, staffing, and authorities it needs to effectively implement these provisions. Such oversight will be key, given that these systems are complex, diverse, and there are a limited number of skilled cyber experts capable of securing them.

Madam Speaker, I urge my colleagues to support H.R. 1833, and I reserve the balance of my time.

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

I want to thank my colleague from New York for supporting my bill, H.R.

1833, the DHS Industrial Control Systems Capabilities Enhancement Act of 2021.

As I have said from day one as ranking member of this committee, we need to continue to bolster cybersecurity capabilities at CISA to defend our Federal networks and the Nation's critical infrastructure from cyber threats.

The volume of cyberattacks and ransomware attacks in 2021 alone shows that no one is immune from nation-state cyber actors or cyber criminals. Cyber threats, particularly ransomware, are the preeminent national security threat facing our Nation today. From Colonial Pipeline to a local water facility in Florida, we have witnessed the real-world consequences cyberattacks can have on our critical infrastructure.

In the cyberattack against a water treatment plant in Florida, hackers were able to gain access to industrial control systems, or ICS for short, and attempted to alter the mixture of water chemicals to what could have been catastrophic fatal levels.

Cyber incidents are very rarely sector specific. CISA is a central agency that can quickly connect the dots when a malicious cyber campaign spans multiple sectors. It is vital that we continue to enhance its visibility across the critical infrastructure ecosystem.

This bill requires the CISA director to maintain capabilities to detect and mitigate threats and vulnerabilities affecting automated control of critical infrastructure, particularly industrial control systems.

This includes maintaining cross-sector incident response capabilities to respond to cybersecurity incidents and providing cybersecurity technical assistance to stakeholders.

We must continue to solidify CISA's lead role in protecting our Nation's critical infrastructure from cyber threats, particularly the industrial control systems that underpin vital components of our daily lives.

This bill is one step in the committee's continued efforts to build up CISA's authorities and resources to effectively carry out its mission, and it is a resounding statement to have such heavy-hitting, bipartisan support.

Madam Speaker, I urge all Members to join me in supporting H.R. 1833, and I reserve the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I have no further speakers, and I am prepared to close after the gentleman from New York closes. I reserve the balance of my time.

Mr. KATKO. Madam Speaker, I have no further speakers. I urge Members to support this bill. I yield back the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I yield myself the balance of my time to close.

I would like to start by thanking the gentleman from New York for his outstanding leadership in this regard.

Industrial control systems are a rich target for cyber adversaries looking to disrupt, extort, and simply wreak havoc. These systems underpin the functions and services we rely on for our day-to-day lives, and the threats they face have never been higher.

Successful disruption of one of these systems could have dire consequences for public health and safety, public confidence, and even the national and economic security of the United States.

CISA is well-positioned to help owners and operators better understand risks to operational technology and work with them to close security gaps.

I again want to congratulate the gentleman from New York (Mr. KATKO), my committee colleague and ranking member, on authoring this bill to codify the role that CISA plays in leading Federal efforts to secure industrial control systems.

Enactment of H.R. 1833 will help to raise our cybersecurity posture across the board.

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

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New York (Ms. CLARKE) that the House suspend the rules and pass the bill, H.R. 1833, 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. BISHOP of North Carolina. 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.

CYBERSECURITY VULNERABILITY REMEDIATION ACT

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 2980) to amend the Homeland Security Act of 2002 to provide for the remediation of cybersecurity vulnerabilities, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2980

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 ''Cybersecurity Vulnerability Remediation Act''.

SEC. 2. CYBERSECURITY VULNERABILITIES.

Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''and'' after the semicolon at the end;

(B) by redesignating paragraph (6) as paragraph (7); and

(C) by inserting after paragraph (5) the following new paragraph:

''(6) the term 'cybersecurity vulnerability' has the meaning given the term 'security vulnerability' in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and''.

(2) in subsection (c)—

(A) in paragraph (5)—

(i) in subparagraph (A), by striking ''and'' after the semicolon at the end;

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting after subparagraph (A) the following new subparagraph:

''(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and''; and

(iv) in subparagraph (C), as so redesignated, by inserting ''and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)'' before ''with Federal'';

(B) in paragraph (7)(C), by striking ''sharing'' and inserting ''share''; and

(C) in paragraph (9), by inserting ''mitigation protocols to counter cybersecurity vulnerabilities,'' after ''measures,'';

(3) in subsection (e)(1)(G), by striking the semicolon after ''and'' at the end;

(4) by redesignating subsection (o) as subsection (p); and

(5) by inserting after subsection (n) following new subsection:

''(o) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.''.

SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.

(a) REPORT.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security 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 how the Agency carries out subsection (n) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (o) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, that includes the following:

(1) A description of the policies and procedures relating to the coordination of vulnerability disclosures.

(2) A description of the levels of activity in furtherance of such subsections (n) and (o) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in such section 2209) between the Department and industry and other stakeholders.

(4) Any available information on the degree to which such information was acted upon by industry and other stakeholders.

(5) A description of how privacy and civil liberties are preserved in the collection, retention, use, and sharing of vulnerability disclosures.

(b) FORM.—The report required under subsection (b) shall be submitted in unclassified form but may contain a classified annex.

SEC. 4. COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES.

The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the