The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. PALLONE) that the House suspend the rules and pass the bill, H.R. 5313, 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. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

REPORTING ATTACKS FROM NATIONS SELECTED FOR OVERSIGHT AND MONITORING WEB ATTACKS AND RANSOMWARE FROM ENEMIES ACT

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4551) to amend the U.S. SAFE WEB Act of 2006 to provide for reporting with respect to cross-border complaints involving ransomware or other cyber-related attacks, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4551

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 ''Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act'' or the ''RANSOMWARE Act''.

SEC. 2. RANSOMWARE AND OTHER CYBER-RELATED ATTACKS.

Section 14 of the U.S. SAFE WEB Act of 2006 (Public Law 109–455; 120 Stat. 3382) is amended—

(1) in the matter preceding paragraph (1)—

(A) by striking ''Not later than 3 years after the date of enactment of this Act,'' and inserting ''Not later than 1 year after the date of enactment of the Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act, and every 2 years thereafter,''; and

(B) by inserting '', with respect to the 2-year period preceding the date of the report (or, in the case of the first report transmitted under this section after the date of the enactment of the Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act, the 1-year period preceding the date of the report)'' after ''include'';

(2) in paragraph (8), by striking ''; and'' and inserting a semicolon;

(3) in paragraph (9), by striking the period at the end and inserting ''; and''; and

(4) by adding at the end the following:

''(10) the number and details of cross-border complaints received by the Commission that involve ransomware or other cyber-related attacks—

''(A) that were committed by individuals located in foreign countries or with ties to foreign countries; and

''(B) that were committed by companies located in foreign countries or with ties to foreign countries.''.

SEC. 3. REPORT ON RANSOMWARE AND OTHER CYBER-RELATED ATTACKS BY CERTAIN FOREIGN INDIVIDUALS, COMPANIES, AND GOVERNMENTS.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and every 2 years thereafter, the Federal Trade Commission shall transmit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report describing its use of and experience with the authority granted by the U.S. SAFE WEB Act of 2006 (Public Law 109–455) and the amendments made by such Act. The report shall include the following:

(1) The number and details of cross-border complaints received by the Commission (including which such complaints were acted upon and which such complaints were not acted upon) that relate to incidents that were committed by individuals, companies, or governments described in subsection (b), broken down by each type of individual, type of company, or government described in a paragraph of such subsection.

(2) The number and details of cross-border complaints received by the Commission (including which such complaints were acted upon and which such complaints were not acted upon) that involve ransomware or other cyber-related attacks that were committed by individuals, companies, or governments described in subsection (b), broken down by each type of individual, type of company, or government described in a paragraph of such subsection.

(3) A description of trends in the number of cross-border complaints received by the Commission that relate to incidents that were committed by individuals, companies, or governments described in subsection (b), broken down by each type of individual, type of company, or government described in a paragraph of such subsection.

(4) Identification and details of foreign agencies (including foreign law enforcement agencies (as defined in section 4 of the Federal Trade Commission Act (15 U.S.C. 44))) located in Russia, China, North Korea, or Iran with which the Commission has cooperated and the results of such cooperation, including any foreign agency enforcement action or lack thereof.

(5) A description of Commission litigation, in relation to cross-border complaints described in paragraphs (1) and (2), brought in foreign courts and the results of such litigation.

(6) Any recommendations for legislation that may advance the mission of the Commission in carrying out the U.S. SAFE WEB Act of 2006 and the amendments made by such Act.

(7) Any recommendations for legislation that may advance the security of the United States and United States companies against ransomware and other cyber-related attacks.

(8) Any recommendations for United States citizens and United States businesses to implement best practices on mitigating ransomware and other cyber-related attacks.

(b) INDIVIDUALS, COMPANIES, AND GOVERNMENTS DESCRIBED.—The individuals, companies, and governments described in this subsection are the following:

(1) An individual located within Russia or with direct or indirect ties to the Government of the Russian Federation.

(2) A company located within Russia or with direct or indirect ties to the Government of the Russian Federation.

(3) The Government of the Russian Federation.

(4) An individual located within China or with direct or indirect ties to the Government of the People's Republic of China.

(5) A company located within China or with direct or indirect ties to the Government of the People's Republic of China.

(6) The Government of the People's Republic of China.

(7) An individual located within North Korea or with direct or indirect ties to the Government of the Democratic People's Republic of Korea.

(8) A company located within North Korea or with direct or indirect ties to the Government of the Democratic People's Republic of Korea.

(9) The Government of the Democratic People's Republic of Korea.

(10) An individual located within Iran or with direct or indirect ties to the Government of the Islamic Republic of Iran.

(11) A company located within Iran or with direct or indirect ties to the Government of the Islamic Republic of Iran.

(12) The Government of the Islamic Republic of Iran.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Georgia (Mr. CARTER) each will control 20 minutes.

The Chair recognizes the gentleman from New Jersey.

GENERAL LEAVE

Mr. PALLONE. 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 H.R. 4551.

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

There was no objection.

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

Mr. Speaker, I rise in strong support of H.R. 4551, the RANSOMWARE Act.

Ransomware and cyberattacks by foreign actors are an unfortunate reality of the modern world, and the United States must be as prepared as possible to address them.

In 2006, Congress passed the SAFE WEB Act to bolster the Federal Trade Commission's authority to receive information from its foreign counterparts and take investigative action in response.

FTC action is critical since the number of consumer complaints against foreign businesses is staggering, with over 255,000 complaints submitted to the FTC's database between 2015 and 2019. The estimated dollar value of losses from just these submitted complaints is in the hundreds of millions of dollars.

H.R. 4551 amends the SAFE WEB Act by adding important new FTC reporting requirements. The legislation requires the FTC to provide regular reports to Congress describing cross-border complaints it receives that involve ransomware and other cyberattacks by foreign individuals, companies, and governments with ties to specific countries.

This bill also boosts the FTC's role in protecting consumers from ransomware and cyberattacks by helping the FTC and Congress better understand these attacks and how to combat them. It also requires the FTC to submit any legislative recommendations

to advance our Nation's security against these types of attacks. This information is crucial in our continued efforts to address this serious issue.

Mr. Speaker, protecting Americans and our businesses against cyberattacks from malicious foreign actors is not a partisan issue, and that is why members of the Energy and Commerce Committee unanimously supported this bill, and why I strongly support it today.

I thank Consumer Protection and Commerce Subcommittee Ranking Member BILIRAKIS for his tireless efforts on this legislation, and I urge everyone to support this important bill.

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

Mr. CARTER of Georgia. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of this legislation by Representative BILIRAKIS, the RANSOMWARE Act.

H.R. 4551 amends the U.S. SAFE WEB Act, a tool the Federal Trade Commission uses to protect consumers with an international dimension, which includes increasing cooperation with foreign law enforcement.

This bill quite simply requires the FTC to report on cross-border complaints they receive involving ransomware or other cybersecurity-related incidents committed by our foreign adversaries, China, Russia, North Korea and Iran.

I am sure we all have stories from our districts. For example, a researcher recently located a host in Georgia that could possibly be connected to a Russian host with exploitation tools that are connected to ransomware.

With the increase in these attacks, I am glad to see this legislation under consideration today, which will help Congress, the Federal Trade Commission, and other law enforcement entities better understand these attacks and learn how to better combat them.

Mr. Speaker, I urge all my colleagues to vote in favor, and I reserve the balance of my time.

□ 1630

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

Mr. CARTER of Georgia. Mr. Speaker, I yield such time as she may consume to the gentlewoman from Washington (Mrs. RODGERS), a member of the Energy and Commerce Committee.

Mrs. RODGERS of Washington. Mr. Speaker, I rise today in support of H.R. 4551, the RANSOMWARE Act.

Every sector of our economy can be targeted by bad actors seeking to exploit vulnerabilities in software and networks. Last year, we saw a significant increase in ransomware attacks from groups operating out of and affiliated with foreign countries like China and Russia.

This legislation builds on my SAFE WEB Extension Act, which was enacted last Congress, and amends it to include ransomware in its international reporting and cooperation. This will help protect Americans from ransomware and other cyberattacks from foreign actors.

Just a few months ago, the U.S. learned that hackers for the Chinese Communist Party had breached major telecommunications companies and network service providers to steal credentials and harvest data. What the CCP will do with this information, no one knows. If their intent is ransom or to use it to extort Americans, this bill will help us better understand and combat these attacks.

We will achieve this by requiring the FTC to report on cross-border complaints involving ransomware, or other cybersecurity-related incidents, committed by foreign adversaries. This will help safeguard critical industries from countries like China, Russia, North Korea, Iran, and others that may wish to harm us.

Mr. Speaker, I thank the ranking member of the Subcommittee on Consumer Protection and Commerce (Mr. BILIRAKIS) for his work on H.R. 4551, and I urge my colleagues to vote in favor of this legislation.

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

Mr. CARTER of Georgia. Mr. Speaker, I yield such time as she may consume to the gentlewoman from Iowa (Mrs. MILLER-MEEKS).

Mrs. MILLER-MEEKS. Mr. Speaker, I thank the gentleman from Georgia (Mr. CARTER) for yielding me time.

Mr. Speaker, I rise in support of H.R. 4551, the RANSOMWARE Act. This important legislation will help protect consumers and businesses from ransomware and cyberattacks.

Almost every day, there are reports of foreign bad actors using ransomware to attack companies, hospital systems, law enforcement agencies, schools, and municipalities.

Last year, the largest meat processing company in the world, JBS, which has a meat processing plant in my district, was hacked by a Russian-led cybercriminal organization. These hackers threatened to delete the company's internal files unless a ransom was paid. JBS was forced to halt processing operations at over a dozen plants, causing the price of meat to rise and impacting economies across the globe.

We have also seen this in our municipalities and schools in Iowa, prompting us in the State legislature to enact legislation addressing ransomware attacks.

This particular legislation will help avoid attacks like these by focusing resources to better understand the threat posed by attacks from our foreign adversaries in China, Russia, North Korea, and Iran.

Mr. Speaker, I am proud to support this bill, and I urge my colleagues to do the same.

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

Mr. PALLONE. Mr. Speaker, I just want to stress how important this bill is. We have heard from the speakers on the Republican side, and I certainly agree with everything they have said about the increased ransomware and cyberattacks by foreign actors and bad actors like Beijing and Russia and some of the others that have been mentioned. It is really important that we pass this bill to protect the United States.

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

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. PALLONE) that the House suspend the rules and pass the bill, H.R. 4551.

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. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

SECURING AND ENABLING COMMERCE USING REMOTE AND ELECTRONIC NOTARIZATION ACT OF 2022

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3962) to authorize notaries public to perform, and to establish minimum standards for, electronic notarizations and remote notarizations that occur in or affect interstate commerce, to require any Federal court to recognize notarizations performed by a notarial officer of any State, to require any State to recognize notarizations performed by a notarial officer of any other State when the notarization was performed under or relates to a public Act, record, or judicial proceeding of the notarial officer's State or when the notarization occurs in or affects interstate commerce, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3962

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 ''Securing and Enabling Commerce Using Remote and Electronic Notarization Act of 2022'' or the ''SECURE Notarization Act of 2022''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COMMUNICATION TECHNOLOGY.—The term ''communication technology'', with respect to a notarization, means an electronic device or process that allows the notary public performing the notarization, a remotely located individual, and (if applicable) a credible witness to communicate with each other simultaneously by sight and sound during the notarization.

(2) ELECTRONIC; ELECTRONIC RECORD; ELECTRONIC SIGNATURE; INFORMATION; PERSON; RECORD.—The terms ''electronic'', ''electronic record'', ''electronic signature'', ''information'', ''person'', and ''record'' have the meanings given those terms in section 106 of the Electronic