The Cybersecurity Vulnerability Remediation Act was introduced and passed the House during the 115th and 116th Congresses and has been updated again in the 117th Congress to meet the ever-evolving nature of cyber threats faced by federal and private sector information systems and our nation's critical infrastructure.

This bill goes significantly further than the first Cybersecurity Vulnerability bill that I introduced in the 115th Congress, to address the instance of Zero Day Events that can lead to catastrophic cybersecurity failures of information and computing systems.

It is estimated that eighty-five percent of critical infrastructure is owned by the private sector and for far too long this fact has hampered efforts to establish stronger requirements for cybersecurity by owners and operators.

Private sector critical infrastructure failure due to a cyberattack is no longer a private matter when it can have massive impacts on the public such as the disruption of gasoline flowing to filling stations.

The Jackson Lee Cybersecurity Vulnerability Remediation Act will:

Expand the definition of security vulnerability to include cybersecurity vulnerability;

Adds sharing mitigation protocols to counter cybersecurity vulnerabilities;

Establish protocols to counter cybersecurity vulnerabilities involving information systems and industrial control systems, which will include vulnerabilities related to software, or hardware that is no longer supported by a vendor;

Direct the Under Secretary for the DHS Office of Science and Technology to standup a competition to find solutions to known cybersecurity vulnerabilities; and

Provide greater transparency on how the Department of Homeland Security's Cybersecurity and Information Security Agency (CISA) is coordinating cybersecurity vulnerability disclosures through the sharing of actionable protocols to mitigate cybersecurity vulnerabilities with information systems and industrial control systems owners and operators.

H.R. 2890 bolsters the efforts to engage critical infrastructure owners and operators in communicating cybersecurity threats; and lays the foundation for greater transparency on the real threats posed by cyberterrorist to private and government sector critical infrastructure and information systems.

The legislation allows the Science the Technology Directorate in consultation with CISA to establish an incentive based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities to information systems and industrial control systems including supervisory control and data acquisition systems.

This bill when it becomes law would put our nation's best minds to work on closing the vulnerabilities that cyber-thieves and terrorists to use them to access, disrupt, corrupt, or take control of critical infrastructure and information systems.

In addition to these changes, the bill requires a report to Congress that may contain a classified annex.

The report will provide information on how DHS:

Coordinates cybersecurity vulnerability disclosures; and

Disseminates actionable protocols to mitigate cybersecurity vulnerabilities involving information system and industrial systems.

Congress needs to know how prevalent and persistent cybersecurity threats targeting critical infrastructure and information systems might be, especially if those threats result in a payment of ransom.

Paying a ransom for ransomware emboldens and encourages bad cyber actors and places everyone at greater risk for the financial and societal costs of increases in threats as other seek payouts.

As long as there is silence about cyber-attacks like ransomware the criminals and terrorists will remain out of reach and continue to feel safe in carrying out these attacks often from the soil of our enemies or peer competitors.

A company cannot stand up to Russia or China, but the United States can and has done so to protect our national interest.

I applaud and thank the Biden Administration for its quick action to respond to the attack against Colonial Pipeline in issuing a new Executive Order.

Today, our nation is in a cybersecurity crisis.

My concern regarding the security of information networks began in 2015 when the Office of Personnel Management's data breach resulted in the theft of millions of sensitive personnel records on federal employees.

The attacks against federal, state, local, territorial, and tribal governments, as well as threats posed to private information systems, and critical infrastructure systems makes this bill necessary.

On May 13, 2021 it was reported that the DC Metropolitan Police Department had experienced the worst reported cyberattack against a police department in the United States.

The gang, known as the Babuk group, released thousands of the Metropolitan Police Department's sensitive documents on the dark web because the department would not pay.

Cyberthreats are not limited to information related to government employees.

In February 2021, a cyberattack on an Oldsmar, Florida water treatment facility involved increasing the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million in drinking water.

However, the levels of this chemical in the water produced by Oldsmar, Florida was increased to levels that would cause harm to people if they drank or used it.

This is just one example of how terrorists can attack critical infrastructure and cause threats to health, safety and life.

Cyber terrorists and cyber criminals are also motivated to attack information networks in exchange for money.

The sources of revenue from cyberattacks has moved from demands of payment for thieves not to release information—to the sale of stolen information on the dark web and now to a sophisticated denial of service attack in the form of ransomware that locks a system using encryption until the victim pays.

A list of known ransomware attacks in 2020 that are suspected of paying ransoms, included:

ISS World (Denmark) paid an estimated cost: $74 million;

Cognizant (US) paid an estimated $50 million;

Sopra Steria (French) paid estimated $50 million;

Redcar and Cleveland Council (UK) paid an estimated $14 million; and

University of California San Francisco (US) paid an estimated $1.14 million.

There are likely many other attacks that are not publicly known and this must change if we are to defeat this threat.

Ransomware is becoming the tool of choice for those seeking a payout because it can be carried out against anyone or any entity by perpetrators who are far from U.S. shores.

The Colonial Pipeline incident is just one in a long line of successful attacks or infiltrations carried out against domestic information systems and critical infrastructure with increasing consequences for the life, health, safety, and economic security of our citizens.

CEO Joseph Blount testified before the U.S. Senate that the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication.

In other words, hackers were able to gain access to this critical infrastructure as a result of a single compromised password.

There would be no need for the Cybersecurity Vulnerability Remediation Act if owners and operators were succeeding in meeting the cybersecurity needs of critical infrastructure.

I know that there is more that should and ought to be done to address the issue of cybercrime and I will be pursuing this avenue under the jurisdiction of the House Judiciary Committee, as the chair of the Subcommittee on Crime, Terrorism and Homeland Security.

Madam Speaker, I ask that my colleagues vote in support of H.R. 2890.

Mr. KATKO. Madam Speaker, I have no further speakers, and 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.

Madam Speaker, our adversaries are showing no signs of slowing their efforts to undermine U.S. interests in cyberspace.

Most often, hackers exploit known vulnerabilities. The Federal Government can and should support efforts to address and mitigate known vulnerabilities.

H.R. 2980 would do just that.

I thank the gentlewoman from Texas for her foresight, and I urge my colleagues to support the bill.

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. 2980, 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.

CISA CYBER EXERCISE ACT

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules

and pass the bill (H.R. 3223) to amend the Homeland Security Act of 2002 to establish in the Cybersecurity and Infrastructure Security Agency the National Cyber Exercise Program, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3223

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 ''CISA Cyber Exercise Act''.

SEC. 2. NATIONAL CYBER EXERCISE PROGRAM.

(a)IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following new section:

''SEC. 2220A. NATIONAL CYBER EXERCISE PROGRAM.

''(a)ESTABLISHMENT OF PROGRAM.—

''(1)IN GENERAL.—There is established in the Agency the National Cyber Exercise Program (referred to in this section as the 'Exercise Program') to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

''(2)REQUIREMENTS.—

''(A)IN GENERAL.—The Exercise Program shall be—

''(i) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

''(ii) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident;

''(iii) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

''(iv) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

''(B)MODEL EXERCISE SELECTION.—The Exercise Program shall—

''(i) include a selection of model exercises that government and private entities can readily adapt for use; and—

''(ii) aid such governments and private entities with the design, implementation, and evaluation of exercises that—

''(I) conform to the requirements described in subparagraph (A);

''(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

''(III) provide for systematic evaluation of readiness.

''(3)CONSULTATION.—In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, cybersecurity research stakeholders, and Sector Coordinating Councils.

''(b)DEFINITIONS.—In this section:

''(1)STATE.—The term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

''(2)PRIVATE ENTITY.—The term 'private entity' has the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).''.

(b)TECHNICAL AMENDMENTS.—

(1)HOMELAND SECURITY ACT OF 2002.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(A) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

''SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.'';

(B) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

''SEC. 2216. JOINT CYBER PLANNING OFFICE.'';

(C) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

''SEC. 2217. CYBERSECURITY STATE COORDINATOR.'';

(D) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management Agencies), by amending the section enumerator and heading to read as follows:

''SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.'';

(E) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

''SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.'';

and

(F) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

''SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.''.

(2)CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting ''of 2002'' after ''Homeland Security Act''.

(c)CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following new items:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint cyber planning office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity Education and Training Programs.
''Sec. 2220A. National Cyber Exercise Program.''.

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 to revise and extend their remarks and to 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, as Americans prepared for their 4th of July holiday weekends, a Russian-based cybercrime crime group launched a ransomware attack that would affect up to 1,500 small- and medium-sized businesses and local governments.

The Kaseya ransomware attacks followed a series of cyberattacks, including one that resulted in the shutdown of 5,500 miles of pipeline on the East Coast.

The unfortunate reality is that the rate and ferocity of cyberattacks show no signs of ebbing.

State actors and cybercriminals alike use cyber tools to advance their goals, regardless of whether they are driven by geopolitical considerations or profiteering.

Together, the Federal Government and its State, local, and private sector partners must do everything in their power to defend our networks while deterring and raising the cost of cyberattacks.

At the same time, we must have tested, exercised cyber-incident response plans in place in the event a malicious hacker successfully gains access to a victim network.

Last year's National Defense Authorization Act included language directing DHS, in coordination with interagency partners, to conduct four exercises over the next 12 years to test the resiliency, response, and recovery of the U.S. to a significant cyber incident impacting critical infrastructure.

Such exercises are critical to understanding our national resilience to cyberattacks and where we need to invest in improving capability.

H.R. 3223 would complement the capstone exercise program authorized last year.

It directs the Cybersecurity and Infrastructure Security Agency, or CISA, together with sector risk management agencies, to develop an exercise program that is designed to more regularly test and assess systemic preparedness and resilience to cyberattacks against critical infrastructure.

The authorization includes requirements for the development of model exercises that State and local governments or private sector entities could readily adapt.

Our collective resilience to cyberattacks demands that we regularly assess and improve our ability to respond to cyberattacks.

The exercise program authorized by H.R. 3223 will help State and local governments and private sector critical infrastructure entities to do just that.

So I urge my colleagues to support H.R. 3223, and I reserve the balance of my time

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

I rise today in support of H.R. 3223, the CISA Cyber Exercise Act. I thank my friend and colleague, Ms. SLOTKIN, for her leadership on this bill, which establishes a cyber exercise program

within CISA to elevate the National Cyber Incident Response Plan.

As cyberattacks affecting our Nation's critical infrastructure continue to rise, it is imperative that State and local governments and the private sector leverage the free services CISA offers to help prevent and mitigate the scourge of ransomware and other cyberattacks facing our Nation.

I am pleased that this legislation will authorize another vital tool in CISA's arsenal.

I urge Members to join me in supporting H.R. 3223, and I reserve the balance of my time.

Ms. CLARKE of New York. Madam Speaker, I yield 2 minutes to the gentlewoman from Michigan (Ms. SLOTKIN).

Ms. SLOTKIN. Madam Speaker, I rise to urge my colleagues to support the CISA Cyber Exercise Act, a bipartisan bill to strengthen our preparation for cyber threats, which I introduced following the ransomware attacks on the Colonial Pipeline.

Last month, I happened to have the Secretary of Agriculture, Mr. Vilsack join me in Ingham County in my district to talk to farmers about protecting family farms, a very important topic in a rural community like mine. And when we went to open Q and A what I think shocked everybody was that the first man to stand up, the first farmer that stood up in his John Deere hat and his overalls wanted to know about cybersecurity. That was the first thing on his mind.

I never imagined that, as a Member of Congress, I would find myself standing in a barn talking with local farmers about ransomware, cyberattacks, and how we are going to protect ourselves but, in fact, I have been having that conversation over and over again in my community. And that is because the last few months have made clear to all Americans that cybersecurity is not just a tech issue, it has gone mainstream. It is at the very heart of protecting our critical infrastructure, energy, food, water, and healthcare that drives our daily lives, and it affects every single one of us. That is why just a week after a ransomware attack struck the world's largest meat processor, these Ingham County farmers wanted to know how cyberattacks would affect their family farms, their livelihood.

What would happen if we were struck by ransomware in Michigan? Who could they turn to to call for help? And above all, what is our government doing to protect citizens who are on the front lines of this threat?

I introduced the CISA Cyber Exercise Act to help answer exactly those questions.

This bill will make sure that our government is preparing for the full range of cyber threats and that we are giving our communities and businesses the tools they need to be secure and resilient.

It strengthens CISA, which is literally America's 911 call for cybersecurity, by formally establishing a National Cyber Exercise Program to test our Nation's response plans for major cyberattacks.

It also directs CISA to build and expand a set of model cyber exercises that can be used by our State and local governments.

By passing this legislation today, we are helping to ensure our Nation and our communities are protected.

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

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

Madam Speaker, the country is experiencing an unprecedented number of significant cyberattacks.

From hospitals to schools to pipelines and a meat processing plant, nothing is immune.

The key to ensuring we are resilient to cyberattacks is to ensure that we have trained and tested cyber incident response plans.

H.R. 3223, the CISA Cyber Exercise Act, is critical in that effort.

I urge my colleagues to support H.R. 3223, and 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. 3223.

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.

DOMAINS CRITICAL TO HOMELAND SECURITY ACT

Ms. CLARKE of New York. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 3264) to amend the Homeland Security Act of 2002 to require research and development to identify and evaluate the extent to which critical domain risks within the United States supply chain pose a substantial threat to homeland security, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3264

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 ''Domains Critical to Homeland Security Act''.

SEC. 2. CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—Subtitle H of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 451 et seq.) is amended by adding at the end the following new section:

''SEC. 890B. HOMELAND SECURITY CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

''(a) IN GENERAL.—

''(1) RESEARCH AND DEVELOPMENT.—The Secretary is authorized to conduct research and development to—

''(A) identify United States critical domains for economic security and homeland security; and

''(B) evaluate the extent to which disruption, corruption, exploitation, or dysfunction of any of such domain poses a substantial threat to homeland security.

''(2) REQUIREMENTS.—

''(A) RISK ANALYSIS OF CRITICAL DOMAINS.—The research under paragraph (1) shall include a risk analysis of each identified United States critical domain for economic security to determine the degree to which there exists a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to such domain. Such research shall consider, to the extent possible, the following:

''(i) The vulnerability and resilience of relevant supply chains.

''(ii) Foreign production, processing, and manufacturing methods.

''(iii) Influence of malign economic actors.

''(iv) Asset ownership.

''(v) Relationships within the supply chains of such domains.

''(vi) The degree to which the conditions referred to in clauses (i) through (v) would place such a domain at risk of disruption, corruption, exploitation, or dysfunction.

''(B) ADDITIONAL RESEARCH INTO HIGH-RISK CRITICAL DOMAINS.—Based on the identification and risk analysis of United States critical domains for economic security pursuant to paragraph (1) and subparagraph (A) of this paragraph, respectively, the Secretary may conduct additional research into those critical domains, or specific elements thereof, with respect to which there exists the highest degree of a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to such a domain. For each such high-risk domain, or element thereof, such research shall—

''(i) describe the underlying infrastructure and processes;

''(ii) analyze present and projected performance of industries that comprise or support such domain;

''(iii) examine the extent to which the supply chain of a product or service necessary to such domain is concentrated, either through a small number of sources, or if multiple sources are concentrated in one geographic area;

''(iv) examine the extent to which the demand for supplies of goods and services of such industries can be fulfilled by present and projected performance of other industries, identify strategies, plans, and potential barriers to expand the supplier industrial base, and identify the barriers to the participation of such other industries;

''(v) consider each such domain's performance capacities in stable economic environments, adversarial supply conditions, and under crisis economic constraints;

''(vi) identify and define needs and requirements to establish supply resiliency within each such domain; and

''(vii) consider the effects of sector consolidation, including foreign consolidation, either through mergers or acquisitions, or due to recent geographic realignment, on such industries' performances.

''(3) CONSULTATION.—In conducting the research under paragraph (1) and subparagraph