

these vouchers are distributed. With several communities around the country having made great strides to effectively end veteran homelessness, it is crucial that we use this information to better target the HUD-VASH voucher program in those communities that need them the most.

The bill would also expand the eligibility for the program, as Chairwoman WATERS described, to veterans who were discharged other than honorably, helping that vulnerable population have access to this crucial resource.

Since 2010, the number of homeless veterans has been cut in half. This Congress has made it a priority and the Obama administration and the Trump administration have made this a priority. These are positive signs, but there is more to do and this bill will help achieve the goal of ending veterans' homelessness.

I, again, would like to thank Mr. STIVERS, the ranking member of the Housing, Community Development and Insurance Subcommittee in the House and a cosponsor of the bill for his leadership on the issue and in working with Mr. PETERS.

Madam Speaker, I urge all my colleagues to support this bill, and I reserve the balance of my time.

Ms. WATERS. Madam Speaker, I yield such time as he may consume to the gentleman from California (Mr. PETERS), who is the sponsor of this legislation.

Mr. PETERS. Madam Speaker, San Diego County is home to over 230,000 veterans. Each year thousands of servicemembers exit the military and choose to stay in San Diego. It has been one of my greatest priorities in Congress to support those in the Armed Forces transitioning back into civilian life. The transition can be tougher for some people than for others. Many veterans struggle with mental health conditions like post-traumatic stress or traumatic brain injury, and they may turn to alcohol or drugs to deal with these mental health issues.

Studies have shown that the top two risk factors to becoming homeless are mental health issues and substance use disorders. The next biggest risk factor is economic insecurity. In expensive regions like ours, rising housing costs can exacerbate these risks and drive up the rate of homelessness. In our county we have over 1,000 veterans experiencing homelessness. We have made serious progress, as my colleague, Mr. HILL, said, here in Congress in reducing the number of veterans experiencing homelessness primarily due to the HUD-VA Supportive Housing, or HUD-VASH, voucher program, which aims to serve chronically homeless veterans. HUD-VASH recognizes housing first as the best way to end homelessness and couples rental assistance with case management services from the VA.

Since this partnership was forged between HUD and VA in 2019, the rate of veteran homelessness has been cut in half. HUD-VASH works, and I have

spent the past several years supporting the program and looking for ways to improve it.

□ 1745

One of those ways to improve this program is to expand eligibility for those who don't have access to the program.

Currently, veterans with other than honorable discharges are not eligible for HUD-VASH because, generally, they don't have access to VA healthcare. A veteran could receive, I think as Chairwoman WATERS mentioned, an other than honorable discharge for administrative or relatively minor reasons.

This eligibility gap prevents thousands of homeless veterans from being housed while receiving critical supportive services. Now, Congress has recognized the value of extending access to veterans for other VA homelessness service programs. Two years ago, we allowed other than honorable veterans to access the grant and per diem program for transitional housing and supportive services for veteran families for rapid rehousing.

This bill, my bill, the bipartisan Veteran HOUSE Act, closes this gap. The legislation expands eligibility for the HUD-VASH program to include veterans with other than honorable, but not dishonorable, discharges.

We know how to end veteran homelessness. Several cities across the country have already achieved functional zero. HUD-VASH is one of the most vital tools we have to accomplish this goal, and we must make sure more homeless veterans have access to this resource.

This bill will see that at least 1,300 additional veterans are eventually served by HUD-VASH and will stop more homeless veterans from falling through the cracks.

Madam Speaker, I thank the Financial Services Committee, particularly Chairwoman WATERS, Mr. HECK, and Mr. STIVERS, for moving this bill through their subcommittee. I also thank my colleagues on the House Committee on Veterans' Affairs, Chairman TAKANO and Chairman LEVIN, for taking swift action on this bill last year. Both committees passed this bill with unanimous support.

Finally, I thank all the local organizations in San Diego for supporting this bill, as well as the National Alliance to End Homelessness and many national veterans service organizations, including The American Legion, the VFW, Disabled American Veterans, and Paralyzed Veterans of America.

Madam Speaker, I urge all of my colleagues to support the Veterans HOUSE Act, and I call on the Senate to act on this bill to help more homeless veterans.

Mr. HILL of Arkansas. Madam Speaker, this is a good bill. This is a bill that will help move more people to shelter, particularly our veterans, who are so in need.

When I think about Jack Kemp and his inspiration for this so many years ago, he frequently quoted Theodore Roosevelt's great quote, which was: "Nobody cares how much you know, until they know how much you care."

Certainly, that is apropos here because Mr. PETERS and the Committee on Veterans' Affairs and the members, both Republicans and Democrats, on the House Financial Services Committee care about solving this crisis. We care about working with our local partners to make our communities a better place.

Madam Speaker, I thank Mr. STIVERS for his work and my friend Mr. PETERS. I urge a "yes" vote on this bill, and I yield back the balance of my time.

Ms. WATERS. Madam Speaker, I yield myself the balance of my time.

Madam Speaker, I again thank Representatives Peters and Heck for bringing forth this important legislation.

We were reminded only last week of the commitment of those who served in the United States armed services. We must continue to do all we can to ensure that those who have served receive the support they need. The reforms in H.R. 2398 will do exactly that.

Madam Speaker, I urge my colleagues to join me in supporting this important piece of legislation, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from California (Ms. WATERS) that the House suspend the rules and pass the bill, H.R. 2398, 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.

Ms. WATERS. Madam 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.

CYBERSECURITY AND FINANCIAL SYSTEM RESILIENCE ACT OF 2019

Ms. WATERS. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4458) to require the Board of Governors of the Federal Reserve System to issue reports on cybersecurity with respect to the functions of the Federal Reserve System, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4458

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 and Financial System Resilience Act of 2019".

SEC. 2. CYBERSECURITY AND FINANCIAL SYSTEM RESILIENCE REPORT.

(a) IN GENERAL.—Not later than the end of the 180-day period beginning on the date of

enactment of this Act, and annually thereafter, each banking regulator shall submit a report to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate that provides a detailed explanation of measures undertaken to strengthen cybersecurity with respect to the functions of the regulator, including the supervision and regulation of financial institutions and, where applicable, third-party service providers. Each such report shall specifically include a detailed analysis of—

(1) policies and procedures (including those described under section 3554(b) of title 44, United States Code) that guard against—

(A) efforts to deny access to or degrade, disrupt, or destroy any information and communications technology system or network, or exfiltrate information from such a system or network without authorization;

(B) destructive malware attacks;

(C) denial of service activities; and

(D) any other efforts that may threaten the functions of the banking regulator or entities overseen by the regulator by undermining cybersecurity and the resilience of the financial system;

(2) activities to ensure the effective implementation of policies and procedures described under paragraph (1), including—

(A) the appointment of qualified staff, the provision of staff training, the use of accountability measures to support staff performance, and the designation, if any, of senior appointed leadership to strengthen accountability for oversight of cybersecurity measures;

(B) deployment of adequate resources and technologies;

(C) efforts to respond to cybersecurity-related findings and recommendations of the Inspector General of the banking regulator or the independent evaluation described under section 3555 of title 42, United States Code; and

(D) as appropriate, efforts to strengthen cybersecurity in coordination with other Federal departments and agencies, domestic and foreign financial institutions, and other partners, including the development and dissemination of best practices regarding cybersecurity and the sharing of threat information; and

(3) any current or emerging threats that are likely to pose a risk to the resilience of the financial system.

(b) **FORM OF REPORT.**—The report required under subsection (a) shall be submitted in unclassified form, but may include a classified annex, if appropriate.

(c) **CONGRESSIONAL BRIEFING.**—Upon request, the head of each banking regulator shall provide a detailed briefing to the appropriate Members of Congress on each report submitted pursuant to subsection (a), except—

(1) the Chairman of the Board of Governors of the Federal Reserve System may designate another member of the Board of Governors of the Federal Reserve System to provide such briefing;

(2) the Chairperson of the Federal Deposit Insurance Corporation may designate another member of the Board of Directors of the Corporation to provide such briefing; and

(3) the Chairman of the National Credit Union Administration may designate another member of the National Credit Union Administration Board to provide such briefing.

(d) **DEFINITIONS.**—For the purposes of this Act:

(1) **APPROPRIATE MEMBERS OF CONGRESS.**—The term “appropriate Members of Congress” means the following:

(A) The Chairman and Ranking Member of the Committee on Financial Services of the House of Representatives.

(B) The Chairman and Ranking Member of the Committee on Banking, Housing, and Urban Affairs of the Senate.

(2) **BANKING REGULATOR.**—The term “banking regulator” means the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the National Credit Union Administration.

(3) **SENIOR APPOINTED LEADERSHIP.**—With respect to a banking regulator, the term “senior appointed leadership” means a position that requires Senate confirmation.

(e) **SUNSET.**—The provisions of this Act shall have no force or effect on or after the date that is 7 years after the date of enactment of this Act.

SEC. 3. 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 California (Ms. **WATERS**) and the gentleman from North Carolina (Mr. **MCHEHRY**) each will control 20 minutes.

The Chair recognizes the gentlewoman from California.

GENERAL LEAVE

Ms. **WATERS**. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks on this legislation and to insert extraneous material thereon.

The **SPEAKER** pro tempore. Is there objection to the request of the gentlewoman from California?

There was no objection.

Ms. **WATERS**. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in support of H.R. 4458, the Cybersecurity and Financial System Resilience Act, which is sponsored by the ranking member of the Financial Services Committee, Mr. **MCHEHRY**.

H.R. 4458 would require the prudential regulators, specifically the Federal Reserve, FDIC, OCC, NCUA, to each issue an annual report to Congress describing measures the respective agency has taken to strengthen cybersecurity. The report must include steps each agency is taking to address any cybersecurity concerns identified by the annual independent evaluations conducted under the Federal Information Security Modernization Act of 2014. The bill sunsets after 7 years.

A wide range of regulators, including the Financial Stability Oversight Council, as well as experts and industrial stakeholders, have recognized cybersecurity is a key risk to our financial system and broader economy.

As technology continues to rapidly change how financial products and

services are delivered, it is important that regulators are ensuring financial institutions, including their third-party service providers, such as cloud service providers, have in place robust cyber policies and practices to help protect against cybersecurity incidents that could compromise sensitive consumer data.

In addition, it is equally important that regulators themselves have their houses in order and that they are protecting their own information systems from cyberattacks. Indeed, many of our regulatory agencies already conduct ongoing cyber exercises to assess their cybersecurity systems. But as the threat of cyberattacks increase, there is an opportunity for Congress, as well as the public, to better understand how their personal data is being protected.

Furthermore, these agencies also must have well-qualified cybersecurity experts on the job to help thwart potential cyberattacks that may be directed at these Federal agencies or the institutions they oversee.

I appreciate that the ranking member worked with our side of the aisle to make important improvements to the bill before the committee marked it up. These changes include expanding the bill from the Federal Reserve to apply it to all Federal depository institution regulators, including the FDIC, OCC, and NCUA.

The bill was also clarified so that the annual reporting includes how regulators supervise banks and credit unions, as well as their third-party service providers, to mitigate cybersecurity risks.

Madam Speaker, I urge Members to support this important legislation, and I reserve the balance of my time.

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

Madam Speaker, today, I begin by thanking Chairwoman **WATERS** and her staff for working with my staff and me to bring this bill to the floor today and, indeed, making it a bipartisan outcome.

It is a nice way to start a year. We started last year on the floor passing bipartisan bills, and from time to time, we have been able to do that over the last year. So I thank Chairwoman **WATERS** for working with me where we can, but when we disagree in our committee, we are able to disagree and still have the capacity to talk to one another. I think that is a very special thing. Now, the rest of our politics, they are what they are, but it is good to celebrate when we have our bipartisan victories.

Madam Speaker, the bill we have before us will ensure the government regulators are taking seriously the systemic risk that cybersecurity attacks pose to the global economy.

For the first time, this legislation will require U.S. bank regulators—the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation,

and the National Credit Union Administration—to provide Congress with a detailed analysis of what they are doing to protect against cyberattacks, both internally and in the entities they oversee.

This includes the regulators' technical procedures, their operational policies to ensure accountability for cybersecurity at the highest management levels, their cooperation with domestic and foreign financial institutions, as well as their forecasts on emerging threats to the resilience of the financial system—important stuff.

The need for this bill is clear. We have witnessed nearly half a billion data records exposed as a result of breaches in the private sector.

We know that the world is digitizing. Our government is trying to keep pace, but the private sector is moving very quickly as we, as consumers, drive this move to greater digitization.

Not surprisingly, one recent survey found that no less than two-thirds of our large financial institutions had experienced an increase in cyberattacks over the previous year, with 79 percent of them concluding that hackers were becoming more sophisticated. Certainly, they are.

At an April 2019 hearing of the Financial Services Committee, CEOs from five of America's seven largest banks cited cyberattacks as the foremost risk they face. Now, that is not productivity growth. It is not political upheaval overseas. It is not an economic slowdown in China or Europe. They ranked their highest concern as cybersecurity threats.

In the private sector, they are not alone in this exposure. Last year, we saw ransomware attacks against Baltimore and three towns in Florida that forced local government operations to be suspended, in some cases jeopardizing basic public services.

What would happen if hackers had that same success in a large attack that has systemic implications? Here is just one example.

The Federal Reserve settles \$35 billion in global payments in just the first hour of operations each business day. A cyberattack on the Fed that could be just partially successful would have and could have disastrous consequences. It is precisely the scale and interconnectedness of the financial sector that makes such scenarios so alarming.

As the 2019 annual report of the Financial Stability Oversight Council explains: "The increasing reliance of financial firms on information technology increases the risk that a cybersecurity event could have severe negative consequences for the U.S. economy, potentially impacting financial stability." True.

The FSOC report goes on to say: "The unique and complex threats posed by cyber risks require the public and private sectors to cooperate to identify, understand, and protect against these risks."

It is a new threat. It is a complex one. While I appreciate our regulators' growing sensitivity to cyber-related risks, we can and must do more.

As the Fed acknowledged in its most recent financial stability report, cyber resiliency is a potential risk for financial stability that doesn't fit neatly into existing risk frameworks.

□ 1800

This bill will help our regulators, including the Fed, incorporate cybersecurity into those risk assessments more effectively.

To be clear, Madam Speaker, the answer to cyber threats is not to return to some bygone, less technologically sophisticated age, something we can't do. On the contrary, ensuring the resiliency of the financial system means increasing vigilance and innovation. That means we need to have the best and brightest protecting our important institutions of government and the best and brightest protecting our important institutions in the private sector.

It is a lack of technological sophistication in the public and private sectors that will offer an opening to attackers if we don't take this action, and that is why Congress needs to hold our regulators to the highest standards of accountability so that they will remain a step ahead of tomorrow's threats.

Again, I want to thank my Democratic colleagues for working with us on this important measure, and I urge all Members to support its passage.

Madam Speaker, I reserve the balance of my time.

Ms. WATERS. Madam Speaker, I reserve the balance of my time.

Mr. MCHENRY. Madam Speaker, I yield myself the balance of my time.

I include in the RECORD a letter from the Credit Union National Association in support of H.R. 4458 and a blog post by the International Monetary Fund which highlights the global threat of cybersecurity attacks and the need for better preparation and risk assessments.

CREDIT UNION NATIONAL ASSOCIATION,
Washington, DC, October 29, 2019.

Hon. MAXINE WATERS,
Chairwoman, Committee on Financial Services,
House of Representatives, Washington, DC.

Hon. PATRICK MCHENRY,
Ranking Member, Committee on Financial Services,
House of Representatives, Washington, DC.

DEAR CHAIRWOMAN WATERS AND RANKING MEMBER MCHENRY: On behalf of America's credit unions, I am writing regarding the House Financial Services Committee's markup of H.R. 4458, "the Cybersecurity and Financial System Resilience Act." The Credit Union National Association (CUNA) represents America's credit unions and their 115 million members.

National Cybersecurity Awareness Month is an important reminder to assess cyber dangers and consider what can be done to help protect Americans and American businesses from cyber-attacks. For credit unions, protecting American's financial and other personal information no matter what business or entity possess or handle it is of the

utmost importance. Theft and misuse of members' information from other businesses and entities cost credit unions and by extension their member-owners significant money while lining the pockets of criminals and criminal nation states who use the money to hurt the United States.

CUNA supports H.R. 4458, the "Cybersecurity and Financial System Resilience Act." America's credit unions support efforts to ensure that the entire financial services sector has proper cyber safeguards in place and this effort should extend to the sectors' regulators. H.R. 4458 would require the sectors' regulators to each issue an annual report to Congress describing measures the respective agency has taken to strengthen cybersecurity with respect to its functions as a regulator, including the supervision and regulation of financial institutions and, where applicable, third-party service providers.

The Federal Information Security Modernization Act (FISMA) requires the sectors' regulators to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency. It appears that H.R. 4458 would enhance FISMA through reporting requirements while also requiring the regulators to ensure robust oversight of their regulated entities, which is already a primary duty of the regulators.

The regulators should be given wide latitude to decide the information reported publicly on the status of their regulated entities. Any information that details cyber vulnerabilities at financial institutions should not be reported publicly as it could harm the sector as bad actors could use reports as a roadmap for future attacks. Furthermore, the regulators should coordinate publicly reporting their regulated financial institutions for the same reason.

Lastly, we commend the National Credit Union Administration (NCUA) Chairman Rodney Hood for recently appointing a cybersecurity advisor. We believe this is a critical step to ensure the agency stays focused on important cyber issues. We appreciate that NCUA has taken proactive efforts to work to secure the cyber security framework for credit unions and their members.

On behalf of America's credit unions and their 115 million members, thank you for the opportunity to share our views. We look forward to continuing to work with the Committee on safeguarding the financial services sector against cyber-attacks.

Sincerely,

JIM NUSSLE,
President & CEO.

[From IMF, Jan. 13, 2020]

CYBERSECURITY THREATS CALL FOR A
GLOBAL RESPONSE

(By David Lipton)

Last March, Operation Taiex led to the arrest of the gang leader behind the Carbanak and Cobalt malware attacks on over 100 financial institutions worldwide. This law enforcement operation included the Spanish national police, Europol, FBI, the Romanian, Moldovan, Belarusian, and Taiwanese authorities, as well as private cybersecurity companies. Investigators found out that hackers were operating in at least 15 countries.

We all know that money moves quickly around the world. As Operation Taiex shows, cybercrime is doing the same, becoming increasingly able to collaborate rapidly across borders.

To create a cyber-secure world, we must be as fast and globally integrated as the criminals. Facing a global threat with local resources will not be enough. Countries need to

do more internally and internationally to coordinate their efforts.

HOW TO BEST WORK TOGETHER

To begin, the private sector offers many good examples of cooperation. The industry deserves credit for taking the lead in many areas—developing technical and risk management standards, convening information-sharing forums, and spending considerable resources. International bodies, including the Group of 7 Cyber Experts group and the Basel Committee, are creating awareness and identifying sound practices for financial sector supervisors. This is important work.

But there is more to be done, especially if we take a global perspective. There are four areas where the international community can come together and boost the work being done at the national level:

First, we need to develop a greater understanding of the risks: the source and nature of threats and how they might impact financial stability. We need more data on threats and on the impact of successful attacks to better understand the risks.

Second, we need to improve collaboration on threat intelligence, incident reporting and best practices in resilience and response. Information sharing between the private and public sector needs to be improved—for example, by reducing barriers to banks reporting issues to financial supervisors and law enforcement.

Different public agencies within a country need to communicate seamlessly. And most challenging, information sharing between countries must improve.

Third, and related, regulatory approaches need to achieve greater consistency. Today, countries have different standards, regulations, and terminology. Reducing this inconsistency will facilitate more communication.

Finally, knowing that attacks will come, countries need to be ready for them. Crisis preparation and response protocols should be developed at both the national and cross-border level, so as to be able to respond and recover operations as soon as possible. Crisis exercises have become crucial in building resilience and the ability to respond, by revealing gaps and weaknesses in processes and decision making.

CONNECTING THE GLOBAL DOTS

Because a cyberattack can come from anywhere in the world, or many places at once, crisis response protocols must be articulated within regions and globally.

That means the relevant authorities need to know “whom to call” during a crisis, in nearby and, ideally, also in faraway countries. For small or developing countries, this is a challenge that needs international attention. Many rely on financial services or correspondent lines provided by global banks for financial connection. Developing cross-border response protocols will help countries understand their respective roles in a crisis and ensure a coordinated response in the event of a crisis.

The Group of 7 countries has made an excellent start at building collaboration on cybersecurity, but this effort needs to be broadened to each and every country.

Here the IMF can play an important role. With a much broader representation than most of the standard-setting institutions, the IMF has the ability to raise the concerns of emerging-market and developing countries to a global level. Because any place is a good place to start an attack, it is in the ultimate interest of advanced economies to work with other countries to share information, coordinate actions, and build capacity.

At the IMF, we work with countries that need to build this capacity, developing the skills and expertise needed to recognize and effectively counter cybersecurity threats.

Our international partners are doing the same, and we work regularly with an array of stakeholders in the public and private sector.

Successful cyberattacks have the potential to hamper financial development by creating distrust, especially if personal and financial data are compromised.

If we want to reap the benefits of new technologies that can develop markets and expand financial inclusion, we have to preserve trust, and ensure the security of information and communications technologies. With cybersecurity, there is always more to be done simply because the pace of change is breathtakingly fast.

Mr. MCHENRY. Madam Speaker, I urge adoption of this measure, and I yield back the balance of my time.

Ms. WATERS. Madam Speaker, I yield myself the balance of my time.

In closing, cybersecurity is a major issue facing all aspects of our economy, including the financial sector. It is an important issue for both private companies and government agencies.

H.R. 4458 will enhance congressional oversight of our banking regulators to ensure that they are maintaining strong cyber defenses of their own systems, as well as the banks and credit unions they regulate. I urge Members to support this important legislation.

I thank the ranking member for his leadership and for the way that he reached across the aisle in working with us.

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 California (Ms. WATERS) that the House suspend the rules and pass the bill, H.R. 4458, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

PRESIDENT GEORGE H.W. BUSH AND FIRST SPOUSE BARBARA BUSH COIN ACT

Ms. WATERS. Madam Speaker, I move to suspend the rules and pass the bill (S. 457) to require that \$1 coins issued during 2019 honor President George H.W. Bush and to direct the Secretary of the Treasury to issue bullion coins during 2019 in honor of Barbara Bush.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 457

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 “President George H.W. Bush and First Spouse Barbara Bush Coin Act”.

SEC. 2. COINS HONORING PRESIDENT GEORGE H.W. BUSH AND FIRST SPOUSE BARBARA BUSH.

(a) CIRCULATING \$1 COINS HONORING PRESIDENT GEORGE H.W. BUSH.—Notwithstanding subsections (d), (n)(2)(E), (n)(3), (n)(4), and

(n)(8) of section 5112 of title 31, United States Code, in addition to the coins to be issued under subsections (r) and (w) of such section 5112, and in accordance with the other provisions of subsection (n) of such section 5112, the Secretary of the Treasury, beginning on January 1, 2020, shall mint and issue \$1 coins that bear—

(1) the image of President George H.W. Bush; and

(2) an inscription of the year “2020”.

(b) BULLION COINS HONORING FIRST SPOUSE BARBARA BUSH.—Notwithstanding paragraphs (1) and (5)(C) of section 5112(o) of title 31, United States Code, and in accordance with the other provisions of such section 5112(o), the Secretary of the Treasury, beginning on January 1, 2020, shall mint and issue bullion coins that bear—

(1) the image of First Spouse Barbara Bush; and

(2) an inscription of the year “2020”.

SEC. 3. FINANCIAL ASSURANCES.

The Secretary of the Treasury shall take such actions as may be necessary to ensure that the minting and issuing of coins under this Act will not result in any net cost to the United States Government.

The SPEAKER pro tempore (Mrs. WATSON COLEMAN). Pursuant to the rule, the gentlewoman from California (Ms. WATERS) and the gentleman from North Carolina (Mr. MCHENRY) each will control 20 minutes.

The Chair recognizes the gentlewoman from California.

GENERAL LEAVE

Ms. WATERS. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks on this legislation and to insert extraneous material thereon.

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

There was no objection.

Ms. WATERS. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in strong support of S. 457, the President George H.W. Bush and First Spouse Barbara Bush Coin Act. This bill directs the Treasury to issue \$1 coins honoring the life and legacy of President George Herbert Walker Bush as well as a bullion coin commemorating his wife, former First Lady Barbara Bush.

The dollar coin was one of the first silver coins minted in the United States. Since the first dollar coins were struck in 1794, the dollar coin has, on occasion, been minted with the images of various individuals whose leadership, actions, and deeds have played an integral role at key moments in our Nation's history. These include President Dwight D. Eisenhower, suffragist Susan B. Anthony, and, most recently, Lemhi Shoshone guide and interpreter for the Lewis and Clark expedition, Sacagawea.

Beginning in 2007, the Mint sought to honor our Nation's Presidents by issuing \$1 coins, featuring their images in the order that they served. The last President to be honored under this program was President Ronald Reagan in 2016.

This bill reauthorizes the Treasury to mint a \$1 coin in honor of the late