incredibly intimidating, and I want to thank my colleague, Mr. DELGADO, for his leadership on this issue.

Small businesses account for 99.6 percent of the businesses in the Commonwealth of Pennsylvania. These businesses are truly the backbone of the American economy, which is why I was proud to introduce this legislation with my colleague from New York. This legislation takes a simple, yet important, step to reduce the strain that the Federal regulations place on small businesses and provide much-needed transparency.

Any time a Federal agency is required to produce a final regulatory flexibility analysis on a rule, the agency is also required by section 212 of the Small Business Regulatory Enforcement Fairness Act to publish one or more guides to assist small entities in complying with the rule.

This legislation makes already available information more easily accessible to small businesses by requiring the Small Business and Agriculture Regulatory Enforcement Ombudsman to create a public website to publish these compliance guides and list contact information for persons who can help small entities comply with these rules. Making this information publicly available on a centralized website is a commonsense way to ease the regulatory burden on small firms that are looking for assistance to comply with the Federal regulations.

I again would like to thank Mr. DELGADO for bringing this issue to my attention and the chairwoman and Ranking Member CHABOT from Ohio for their commitment to advancing this bipartisan solution.

I ask each of my colleagues to support this measure.

Mr. CHABOT. Mr. Speaker, this is yet another example of how our committee continues to work across the aisle for the benefit of America's small businesses. We do it in a bipartisan manner, and I want to thank Mr. DELGADO and the doctor, as well, for their leadership on this.

I urge the bill's adoption, and I yield back the balance of my time.

Mr. DELGADO. Mr. Speaker, we know that small business owners don't necessarily have the resources and time to navigate multiple websites to fully understand their responsibilities with Federal laws. My bill is an important step toward reversing these problems. H.R. 2142 will make it easier, not harder, to comply with Federal regulations by providing them one location for compliance assistance.

The ombudsman already maintains a site for guidance, but this bill goes one step further by requiring that they not just provide agency contacts, but also keep a regular, updated page of compliance guides readily accessible to the public. My legislation renews our commitment towards small business growth and success by creating transparency and accountability of Federal agencies.

Again, I want to thank Dr. JOYCE for cosponsoring this bill and putting our small businesses first.

I urge my colleagues to support this bill, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. DELGADO) that the House suspend the rules and pass the bill, H.R. 2142.

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

A motion to reconsider was laid on the table.

SBA CYBER AWARENESS ACT

Mr. DELGADO. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2331) to require an annual report on the cybersecurity of the Small Business Administration, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2331

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 ''SBA Cyber Awareness Act''.

SEC. 2. CYBERSECURITY AWARENESS REPORTING.

Section 10 of the Small Business Act (15 U.S.C. 639) is amended by inserting after subsection (a) the following:

''(b) CYBERSECURITY REPORTS.—

''(1) ANNUAL REPORT.—Not later than 180 days after the date of enactment of this subsection, and every year thereafter, the Administrator shall submit a report to the appropriate congressional committees that includes—

''(A) an assessment of the information technology (as defined in section 11101 of title 40, United States Code) and cybersecurity infrastructure of the Administration;

''(B) a strategy to increase the cybersecurity infrastructure of the Administration;

''(C) a detailed account of any information technology equipment or interconnected system or subsystem of equipment of the Administration that was manufactured by an entity that has its principal place of business located in the People's Republic of China; and

''(D) an account of any cybersecurity risk or incident that occurred at the Administration during the 2-year period preceding the date on which the report is submitted, and any action taken by the Administrator to respond to or remediate any such cybersecurity risk or incident.

''(2) ADDITIONAL REPORTS.—If the Administrator determines that there is a reasonable basis to conclude that a cybersecurity risk or incident occurred at the Administration, the Administrator shall—

''(A) not later than 7 days after the date on which the Administrator makes that determination, notify the appropriate congressional committees of the cybersecurity risk or incident; and

''(B) not later than 30 days after the date on which the Administrator makes a determination under subparagraph (A)—

''(i) provide notice to individuals and small business concerns affected by the cybersecurity risk or incident; and

''(ii) submit to the appropriate congressional committees a report, based on information available to the Administrator as of the date which the Administrator submits the report, that includes—

''(I) a summary of information about the cybersecurity risk or incident, including how the cybersecurity risk or incident occurred; and

''(II) an estimate of the number of individuals and small business concerns affected by the cybersecurity risk or incident, including an assessment of the risk of harm to affected individuals and small business concerns.

''(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to affect the reporting requirements of the Administrator under chapter 35 of title 44, United States Code, in particular the requirement to notify the Federal information security incident center under section 3554(b)(7)(C)(ii) of such title, or any other provision of law.

''(4) DEFINITIONS.—In this subsection:

''(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(i) the Committee on Small Business and Entrepreneurship of the Senate; and

''(ii) the Committee on Small Business of the House of Representatives.

''(B) CYBERSECURITY RISK; INCIDENT.—The terms 'cybersecurity risk' and 'incident' have the meanings given such terms, respectively, under section 2209(a) of the Homeland Security Act of 2002.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. DELGADO) and the gentleman from Ohio (Mr. CHABOT) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. DELGADO. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on the measure under consideration.

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

There was no objection.

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

I rise in support of H.R. 2331, the SBA Cyber Awareness Act of 2019, which strengthens the Small Business Administration's cybersecurity infrastructure to handle and report cyber threats that affect small businesses.

The Small Business Administration processes a significant amount of small business data, and protecting these businesses is essential to its mission. That is why they must protect its precious digital networks from cyberattacks. But after the massive data breach at the U.S. Office of Personnel Management, 75 percent of Americans are doubtful that the government can protect their personal information.

With 28 million small business owners in the U.S. that provide 64 percent of new private-sector jobs, America cannot afford for small businesses to lose faith in the SBA. Today, we take an important step to restore American confidence in the SBA's cybersecurity protections and prevent the harmful results of cyberattacks.

H.R. 2331 ensures that the SBA has an effective cyber strategy and requires timely reporting of cyber incidents to Congress and affected individuals. Through these measures, the SBA will better serve the American small businesses that support the U.S. economy.

I thank Congressman CROW and Congressman BALDERSON for working so diligently to strengthen the agency we oversee and protect the Nation's small business community that utilizes its services.

I ask my fellow Members to support this bill, and I reserve the balance of my time.

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

Mr. Speaker, I rise in support of H.R. 2331, the SBA Cyber Awareness Act.

In June 2015, the Office of Personnel Management, or OPM, discovered that background investigation records of current, former, and prospective Federal employees and contractors had been stolen from their system. That data breach affected 21.5 million individuals. Earlier in 2015, OPM discovered that the personal data of 4.2 million current and former Federal Government employees had also been stolen. This is absolutely unacceptable, and we must hold agencies accountable to secure their networks.

While a much smaller agency, the SBA maintains important and sensitive data about loan recipients, government contractor information, and various other forms of personally identifiable information that hackers covet. That is why I am happy to support Mr. CROW's and Mr. BALDERSON's legislation, H.R. 2331, the SBA Cyber Awareness Act. This legislation mirrors legislation introduced in the last Congress by Senators RUBIO and CARDIN.

The bill directs the SBA to issue reports that assess its cybersecurity infrastructure, including determining the country of origin of its IT components, and report cyber threats, breaches, and cyberattacks.

This is a commonsense, bipartisan bill, and I urge my colleagues to support the measure.

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

Mr. DELGADO. Mr. Speaker, I yield 5 minutes to the gentleman from Colorado (Mr. CROW), the sponsor of the bill.

Mr. CROW. Mr. Speaker, I want to thank the gentleman from New York (Mr. DELGADO) for yielding, and I want to thank Chairwoman VELÁZQUEZ for prioritizing this critical issue and bringing our bill to the floor. I also want to thank my friend and colead on H.R. 2331, the gentleman from Ohio (Mr. BALDERSON), for his leadership on cybersecurity and small business issues and this bill in particular. I value his input and expertise on all of these issues.

Mr. Speaker, I rise in strong support of this bipartisan legislation I introduced with Ranking Member BALDERSON, the SBA Cyber Awareness Act.

The Small Business Administration houses vital information for small business owners and lenders. We must do everything we can to help the SBA protect its systems and the data of our Nation's small businesses.

Our bill would require the SBA to be more proactive in protecting its data and more transparent in the event of a cyber breach.

First, our bill requires the SBA to issue a report detailing its cybersecurity efforts within 6 months of enactment. This report must include an assessment of the SBA's existing IT and cybersecurity infrastructure and its strategy to address vulnerabilities.

Notably, this bill ensures we are protecting ourselves against China by requiring an audit of any SBA system or IT equipment manufactured by a company headquartered in China.

The report must detail every cybersecurity risk or incident in the last 2 years and the SBA's strategy to address them going forward.

Second, our bill provides a framework for the SBA to follow in the event of future breaches, requiring timely notifications to Congress as well as the people in the small businesses affected. The bill also requires the SBA to submit a full report to both committees on how the cybersecurity risk or incident occurred and how many parties were affected.

The goal of this bill is to put the SBA and the small businesses that it interacts with and that depend on it on the best footing possible to combat the rising threat of cyberattacks.

I am very excited that this bill is up for a vote in the House today and has such strong bipartisan support.

Mr. Speaker, I urge my colleagues to vote in support of our bipartisan legislation and thank everyone who had a hand in bringing it to the floor. It is an exciting day when we can focus on our Nation's small businesses and cyber infrastructure, and I am hopeful for this bill's quick consideration by the Senate.

Mr. CHABOT. Mr. Speaker, in closing, I just want to thank Mr. BALDERSON and Mr. CROW for working together in a bipartisan manner on this very important legislation.

I know Mr. BALDERSON wanted to be here today to speak on this. Unfortunately, I believe he had some airline issues, but I believe he will be submitting a statement for the RECORD.

But again, we appreciate both Mr. BALDERSON and Mr. CROW's leadership on this.

□ 1700

We have seen a large increase in cybersecurity threats against not only the private sector, but also the public sector. We must remain vigilant to ensure the public's data does not end up in the wrong hands.

This bipartisan legislation ensures that the SBA is better equipped to protect American citizens' data.

Mr. Speaker, I urge my colleagues to support this, and I yield back the balance of my time.

Mr. DELGADO. Mr. Speaker, the Small Business Administration fuels the U.S. economy, and through its lending and contracting programs, helps Americans start, build, and grow small businesses, but in doing so, the agency is tasked with handling vital information.

As we all know, cyberattacks are very real, and nobody, not even the Federal Government, is immune.

That is why this piece of legislation, H.R. 2331, is fundamental to the health of our national cyber infrastructure as it relates to small firms.

The SBA must protect its digital networks from cyberattacks and collaborate more with Congress. Modernizing the agency's IT infrastructure and implementing an effective cyber strategy is the key component of this bill. Doing so guarantees the SBA can adequately and effectively defend its digital network.

This bill also requires timely reporting of cyber incidents to Congress and affected individuals in the unfortunate event of a breach. The sharing of this information allows us to collaborate with the SBA to better address vulnerabilities in the system.

Mr. Speaker, H.R. 2331 has bipartisan support, so I once again want to urge my colleagues to support the measure. I yield back the balance of my time.

Mr. BALDERSON. Mr. Speaker, I rise today in support of H.R. 2331, the SBA Cyber Awareness Act of 2019. This bill has had my full support since its introduction and I am happy to support its passage today.

I want to first thank my good friend, the gentleman from Colorado, for his leadership on this effort. It is nice to see Congress attempt to solve problems not only in a bipartisan manner, but also proactively before problems occur, rather than waiting until something goes wrong.

This bill addresses a potential weakness within the Small Business Administration's cybersecurity infrastructure. By passing this bill, we will proactively guard against harmful and widespread cyberattacks by bringing the Small Business Administration's cybersecurity defenses into the 21st Century. This bill will protect the sensitive business and personal information of millions of small business owners across the country.

In a rapidly-developing digital age, strong cybersecurity protections and reinforcements are of the utmost importance. Many small businesses don't have the defensive infrastructure to deal with cyberattacks, A threat to cybersecurity is a threat to small businesses' vitality. that's why this bill is so important.

We, as Congress, must lift up the small businesses of America and ensure they have the support they need to address this ever-changing online environment. And this bill is a bipartisan example of that.

Once again, I thank my colleague from Colorado for his proactive leadership, and I urge the passage of H.R. 2331.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr.

DELGADO) that the House suspend the rules and pass the bill, H.R. 2331.

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

A motion to reconsider was laid on the table.

SMALL BUSINESS DEVELOPMENT CENTER CYBER TRAINING ACT OF 2019

Mr. DELGADO. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1649) to amend the Small Business Act to require cyber certification for small business development center counselors, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1649

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 ''Small Business Development Center Cyber Training Act of 2019''.

SEC. 2. DUTIES OF SMALL BUSINESS DEVELOPMENT CENTER COUNSELORS.

Section 21 of the Small Business Act (15 U.S.C. 648) is amended by adding at the end the following:

''(o) CYBER STRATEGY TRAINING FOR SMALL BUSINESS DEVELOPMENT CENTERS.—

''(1) DEFINITIONS.—In this subsection—

''(A) the term 'cyber strategy' means resources and tactics to assist in planning for cybersecurity and defending against cyber risks and cyber attacks; and

''(B) the term 'lead small business development center' means a small business development center that has received a grant from the Administration.

''(2) CERTIFICATION PROGRAM.—The Administrator shall establish a cyber counseling certification program, or approve a similar existing program, to certify the employees of lead small business development centers to provide cyber planning assistance to small business concerns.

''(3) NUMBER OF CERTIFIED EMPLOYEES.—The Administrator shall ensure that the number of employees of each lead small business development center who are certified in providing cyber planning assistance under this subsection is not fewer than the lesser of—

''(A) 5; or

''(B) 10 percent of the total number of employees of the lead small business development center.

''(4) CONSIDERATION OF SMALL BUSINESS DEVELOPMENT CENTER CYBER STRATEGY.—In carrying out this subsection, the Administrator, to the extent practicable, shall consider any cyber strategy methods included in the Small Business Development Center Cyber Strategy developed under section 1841(a) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 130 Stat. 2662).

''(5) REIMBURSEMENT FOR CERTIFICATION.—

''(A) IN GENERAL.—Subject to the availability of appropriations and subparagraph (B), the Administrator shall reimburse a lead small business development center for costs relating to the certification of an employee of the lead small business development center under the program established under paragraph (2).

''(B) LIMITATION.—The total amount reimbursed by the Administrator under subparagraph (A) may not exceed $350,000 in any fiscal year.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. DELGADO) and the gentleman from Ohio (Mr. CHABOT) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. DELGADO. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on the measure under consideration.

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

There was no objection.

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

Mr. Speaker, I rise in support of H.R. 1649, the Small Business Development Center Cyber Training Act of 2019, which helps Small Business Development Centers, or SBDCs, become better equipped to assist small entities with their cybersecurity needs.

Small businesses have increasingly become the targets of cyberattacks, and because of the complexity and cost associated with identifying, monitoring, and sharing information with appropriate agencies, only 31 percent of small firms have cybersecurity plans in place.

Besides access to capital, cybersecurity is one of the main impediments to entrepreneurial success. Our committee has heard many heartbreaking stories about how it took just one attack to shutter a business.

We have also heard time and time again the frustration business owners feel as they attempt to protect against ever-changing threats and navigate cyber regulations to win government contracts.

This legislation ensures that our Nation's most vulnerable businesses are prepared to combat the imminent threat from cyberattacks.

Leveraging the vast network of SBDCs and their expertise in assisting entrepreneurs from all over the country is a step in the right direction to provide education and training to business owners seeking to implement safeguards to their networks.

Mr. Speaker, I commend Ranking Member CHABOT and Congressman EVANS for working together on this important issue, and I ask my fellow Members to support this bill.

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

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

Mr. Speaker, I rise in support of H.R. 1649, the Small Business Development Center Cyber Training Act of 2019.

Information technology is a necessity for small businesses, because it arms them with the tools they need to be competitive in the global economy.

Unfortunately, small businesses are increasingly popular targets for cybercriminals. The average cost of a cyberattack on a small business is over $30,000, which can destroy, literally, a small business.

That is exactly why Ms. VELÁZQUEZ, Mr. EVANS, and I introduced H.R. 1649, the Small Business Development Center Cyber Training Act of 2019.

This bipartisan legislation establishes a cyber counseling certification program in lead SBDCs to better assist small businesses with planning and implementing cybersecurity measures to defend against cyberattacks.

The cyber assistance offered by trained staff at SBDCs would be provided at no or low cost to small businesses.

Cyber planning assistance will encourage small businesses to take a more proactive approach to defending themselves from cyberattacks by leveraging the expertise from SBDCs and their partner agencies and institutions. This bill utilizes existing Federal resources to cover the reimbursement costs.

We recognize cyber threats are ever-evolving and will continue to work with industry to ensure that appropriate staffing needs are met.

Mr. Speaker, I urge my colleagues to support this measure, and I reserve the balance of my time.

Mr. DELGADO. Mr. Speaker, I yield 5 minutes to the gentleman from Pennsylvania (Mr. EVANS).

Mr. EVANS. Mr. Speaker, I thank my colleague from New York (Mr. DELGADO) for the introduction.

Mr. Speaker, I rise to offer my support for H.R. 1649, the Small Business Development Center Cyber Training Act.

As vice chair of the Small Business Committee, I was proudly joined by fellow colleagues in the committee, Ranking Member CHABOT and Chairwoman VELÁZQUEZ, in introducing this important bipartisan legislation.

I consider small business to be the foundation of our communities. They are the engines that drive innovativeness, investments, and economic development, and they are the pillars that prop up our neighborhoods.

Both in my home State of Pennsylvania and across the U.S., small businesses account for more than 99 percent of all businesses. Nationally, they support almost 59 million jobs.

Over the past decade, as we have seen immense growth in technology and innovativeness, we have also seen an increase in incidents involving the theft of valuable information from businesses and governments.

In 2014, it was discovered that the Office of Personnel Management was hacked, resulting in the theft of over 20 million records.

In 2013, criminals broke into Target's databases, with the credit and debit information from almost 40 million consumers being compromised.

Breaches have also been reported at Home Depot, JPMorgan Chase, and Sony.