As an added benefit, according to the Congressional Budget Office, this new policy will not cost the American taxpayers anything to implement.

Further, this new flexibility for the Federal Government and its employees to utilize electric vehicles could help bolster the American market for electric vehicles.

As we have learned throughout the coronavirus pandemic, American manufacturing is vitally important to our success as a Nation. By allowing the increased use of electric vehicles in America, we can secure all the American ingenuity and innovation that comes with the vehicles of the future.

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

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I urge passage of S. 2193, 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 (Mrs. CAROLYN B. MALONEY) that the House suspend the rules and pass the bill, S. 2193.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3 of House Resolution 965, the yeas and nays are ordered.

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

INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1668) to leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1668

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 ''Internet of Things Cybersecurity Improvement Act of 2020'' or the ''IoT Cybersecurity Improvement Act of 2020''.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) ensuring the highest level of cybersecurity at agencies in the executive branch is the responsibility of the President, followed by the Director of the Office of Management and Budget, the Secretary of Homeland Security, and the head of each such agency;

(2) this responsibility is to be carried out by working collaboratively within and among agencies in the executive branch, industry, and academia;

(3) the strength of the cybersecurity of the Federal Government and the positive benefits of digital technology transformation depend on proactively addressing cybersecurity throughout the acquisition and operation of Internet of Things devices by the Federal Government; and

(4) consistent with the second draft National Institute for Standards and Technology Interagency or Internal Report 8259 titled ''Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline'', published in January 2020, Internet of Things devices are devices that—

(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and

(B) can function on their own and are not only able to function when acting as a component of another device, such as a processor.

SEC. 3. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 3502 of title 44, United States Code.

(2) DIRECTOR OF OMB.—The term ''Director of OMB'' means the Director of the Office of Management and Budget.

(3) DIRECTOR OF THE INSTITUTE.—The term ''Director of the Institute'' means the Director of the National Institute of Standards and Technology.

(4) INFORMATION SYSTEM.—The term ''information system'' has the meaning given that term in section 3502 of title 44, United States Code.

(5) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given that term in section 3552(b)(6) of title 44, United States Code.

(6) OPERATIONAL TECHNOLOGY.—The term ''operational technology'' means hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise.

(7) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(8) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)).

SEC. 4. SECURITY STANDARDS AND GUIDELINES FOR AGENCIES ON USE AND MANAGEMENT OF INTERNET OF THINGS DEVICES.

(a) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY DEVELOPMENT OF STANDARDS AND GUIDELINES FOR USE OF INTERNET OF THINGS DEVICES BY AGENCIES.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Institute shall develop and publish under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) standards and guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices.

(2) CONSISTENCY WITH ONGOING EFFORTS.—The Director of the Institute shall ensure that the standards and guidelines developed under paragraph (1) are consistent with the efforts of the National Institute of Standards and Technology in effect on the date of the enactment of this Act—

(A) regarding—

(i) examples of possible security vulnerabilities of Internet of Things devices; and

(ii) considerations for managing the security vulnerabilities of Internet of Things devices; and

(B) with respect to the following considerations for Internet of Things devices:

(i) Secure Development.

(ii) Identity management.

(iii) Patching.

(iv) Configuration management.

(3) CONSIDERING RELEVANT STANDARDS.—In developing the standards and guidelines under paragraph (1), the Director of the Institute shall consider relevant standards, guidelines, and best practices developed by the private sector, agencies, and public-private partnerships.

(b) REVIEW OF AGENCY INFORMATION SECURITY POLICIES AND PRINCIPLES.—

(1) REQUIREMENT.—Not later than 180 days after the date on which the Director of the Institute completes the development of the standards and guidelines required under subsection (a), the Director of OMB shall review agency information security policies and principles on the basis of the standards and guidelines published under subsection (a) pertaining to Internet of Things devices owned or controlled by agencies (excluding agency information security policies and principles pertaining to Internet of Things of devices owned or controlled by agencies that are or comprise a national security system) for consistency with the standards and guidelines submitted under subsection (a) and issue such policies and principles as may be necessary to ensure those policies and principles are consistent with such standards and guidelines.

(2) REVIEW.—In reviewing agency information security policies and principles under paragraph (1) and issuing policies and principles under such paragraph, as may be necessary, the Director of OMB shall—

(A) consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security; and

(B) ensure such policies and principles are consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code.

(3) NATIONAL SECURITY SYSTEMS.—Any policy or principle issued by the Director of OMB under paragraph (1) shall not apply to national security systems.

(c) QUINQUENNIAL REVIEW AND REVISION.—

(1) REVIEW AND REVISION OF NIST STANDARDS AND GUIDELINES.—Not later than 5 years after the date on which the Director of the Institute publishes the standards and guidelines under subsection (a), and not less frequently than once every 5 years thereafter, the Director of the Institute, shall—

(A) review such standards and guidelines; and

(B) revise such standards and guidelines as appropriate.

(2) UPDATED OMB POLICIES AND PRINCIPLES FOR AGENCIES.—Not later than 180 days after the Director of the Institute makes a revision pursuant to paragraph (1), the Director of OMB, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall update any policy or principle issued under subsection (b)(1) as necessary to ensure those policies and principles are consistent with the review and any revision under paragraph (1) under this subsection and paragraphs (2) and (3) of subsection (b).

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement any standards and guidelines promulgated in this section.

SEC. 5. GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Institute, in consultation with such cybersecurity researchers and private sector industry experts as the Director considers appropriate, and in consultation with the Secretary, shall develop and publish under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) guidelines—

(1) for the reporting, coordinating, publishing, and receiving of information about—

(A) a security vulnerability relating to information systems owned or controlled by an agency (including Internet of Things devices owned or controlled by an agency); and

(B) the resolution of such security vulnerability; and

(2) for a contractor providing to an agency an information system (including an Internet of Things device) and any subcontractor thereof at any tier providing such information system to such contractor, on—

(A) receiving information about a potential security vulnerability relating to the information system; and

(B) disseminating information about the resolution of a security vulnerability relating to the information system.

(b) ELEMENTS.—The guidelines published under subsection (a) shall—

(1) to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely-used standard;

(2) incorporate guidelines on—

(A) receiving information about a potential security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device); and

(B) disseminating information about the resolution of a security vulnerability relating to an information system owned or controlled by an agency (including an Internet of Things device); and

(3) be consistent with the policies and procedures produced under section 2009(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m)).

(c) INFORMATION ITEMS.—The guidelines published under subsection (a) shall include example content, on the information items that should be reported, coordinated, published, or received pursuant to this section by a contractor, or any subcontractor thereof at any tier, providing an information system (including Internet of Things device) to the Federal Government.

(d) OVERSIGHT.—The Director of OMB shall oversee the implementation of the guidelines published under subsection (a).

(e) OPERATIONAL AND TECHNICAL ASSISTANCE.—The Secretary, in consultation with the Director of OMB, shall administer the implementation of the guidelines published under subsection (a) and provide operational and technical assistance in implementing such guidelines.

SEC. 6. IMPLEMENTATION OF COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.

(a) AGENCY GUIDELINES REQUIRED.—Not later than 2 years after the date of the enactment of this Act, the Director of OMB, in consultation with the Secretary, shall develop and oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including Internet of Things devices).

(b) OPERATIONAL AND TECHNICAL ASSISTANCE.—Consistent with section 3553(b) of title 44, United States Code, the Secretary, in consultation with the Director of OMB, shall provide operational and technical assistance to agencies on reporting, coordinating, publishing, and receiving information about security vulnerabilities of information systems (including Internet of Things devices).

(c) CONSISTENCY WITH GUIDELINES FROM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Secretary shall ensure that the assistance provided under subsection (b) is consistent with applicable standards and publications developed by the Director of the Institute.

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement the provisions under this section.

SEC. 7. CONTRACTOR COMPLIANCE WITH COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INTERNET OF THINGS DEVICES.

(a) PROHIBITION ON PROCUREMENT AND USE.—

(1) IN GENERAL.—The head of an agency is prohibited from procuring or obtaining, renewing a contract to procure or obtain, or using an Internet of Things device, if the Chief Information Officer of that agency determines during a review required by section 11319(b)(1)(C) of title 40, United States Code, of a contract for such device that the use of such device prevents compliance with the standards and guidelines developed under section 4 or the guidelines published under section 5 with respect to such device.

(2) SIMPLIFIED ACQUISITION THRESHOLD.—Notwithstanding section 1905 of title 41, United States Code, the requirements under paragraph (1) shall apply to a contract or subcontract in amounts not greater than the simplified acquisition threshold.

(b) WAIVER.—

(1) AUTHORITY.—The head of an agency may waive the prohibition under subsection (a)(1) with respect to an Internet of Things device if the Chief Information Officer of that agency determines that—

(A) the waiver is necessary in the interest of national security;

(B) procuring, obtaining, or using such device is necessary for research purposes; or

(C) such device is secured using alternative and effective methods appropriate to the function of such device.

(2) AGENCY PROCESS.—The Director of OMB shall establish a standardized process for the Chief Information Officer of each agency to follow in determining whether the waiver under paragraph (1) may be granted.

(c) REPORTS TO CONGRESS.—

(1) REPORT.—Every 2 years during the 6-year period beginning on the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report—

(A) on the effectiveness of the process established under subsection (b)(2);

(B) that contains recommended best practices for the procurement of Internet of Things devices; and

(C) that lists—

(i) the number and type of each Internet of Things device for which a waiver under subsection (b)(1) was granted during the 2-year period prior to the submission of the report; and

(ii) the legal authority under which each such waiver was granted, such as whether the waiver was granted pursuant to subparagraph (A), (B), or (C) of such subsection.

(2) CLASSIFICATION OF REPORT.—Each report submitted under this subsection shall be submitted in unclassified form, but may include a classified annex that contains the information described under paragraph (1)(C).

(d) EFFECTIVE DATE.—The prohibition under subsection (a)(1) shall take effect 2 years after the date of the enactment of this Act.

SEC. 8. GOVERNMENT ACCOUNTABILITY OFFICE REPORT ON CYBERSECURITY CONSIDERATIONS STEMMING FROM THE CONVERGENCE OF INFORMATION TECHNOLOGY, INTERNET OF THINGS, AND OPERATIONAL TECHNOLOGY DEVICES, NETWORKS, AND SYSTEMS.

(a) BRIEFING.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall provide a briefing to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate on broader Internet of Things efforts, including projects designed to assist in managing potential security vulnerabilities associated with the use of traditional information technology devices, networks, and systems with—

(1) Internet of Things devices, networks, and systems; and

(2) operational technology devices, networks, and systems.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General shall submit a report to the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate on broader Internet of Things efforts addressed in subsection (a).

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New York (Mrs. CAROLYN B. MALONEY) and the gentleman from Pennsylvania (Mr. KELLER) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

GENERAL LEAVE

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include extraneous material on the measure before us.

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

There was no objection.

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I yield myself as much time as I may consume.

Mr. Speaker, I thank Representatives KELLY and HURD for introducing the bill before us, which has garnered strong support from both sides of the aisle.

As technology evolves rapidly, this bill will help safeguard our Federal

workforce, systems, and data from the very real cyber threats posed by the commonplace, everyday devices and items that make up the Internet of Things.

Since 2014, there have been more devices connected to our networks and in use than there are people on this planet.

Our committee has conducted extensive work this Congress to address the silent war of cyberattacks that American governments, companies, and citizens face on a daily basis. Reports indicate that 25 percent of those attacks target these types of devices.

Without adequate standards and protections in place, these devices can be compromised, hijacked, and utilized for surveillance, disruption, denial-of-service, or ransomware attacks.

Currently, there are no national standards to ensure the security of these connected devices. H.R. 1668 would establish minimum cybersecurity standards for such devices that are owned by the Federal Government, based on guidelines set by the National Institute of Standards and Technology.

This bill will also require contractors or vendors to notify the Federal Government if devices in Federal use have a known or suspected security vulnerability.

H.R. 1668 recognizes that protecting our Nation from cyber threats is an ongoing interactive process that requires established baseline standards and constant vigilance.

Mr. Speaker, I support this bill, and I reserve the balance of my time.

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

I rise in support of H.R. 1668, the Internet of things, or IoT, Cybersecurity Improvement Act of 2019.

Our Nation's use of technology has shifted dramatically in recent years. Internet of Things, or IoT, devices have found a way into nearly every aspect of our lives, work, and now government.

A recent Congressional Research Service report cites market estimates that, by 2025, there will be more than 21.5 billion internet-connected devices.

IoT devices, such as smart TVs and appliances, home security systems, thermostats, and many other home and work devices, are now connected to the internet. This offers ever-increasing gateways into our most valuable networks through our weakest technology devices.

We traditionally think of computing devices such as computers, smartphones, and tablets as our primary interface with the internet. These computing devices have securely designed, mature, and powerful operating systems. However, IoT devices normally have less computing power and, therefore, security capabilities than traditional computing devices.

As our economy has embraced the convenience of IoT devices, we have also created more entry points to the internet and our networks for malicious actors to exploit. For example, building elevators, HVAC, lighting, audio-video, fire suppression, and even security systems are now capable of being monitored and updated remotely through networks.

IoT devices play an integral role with industrial and manufacturing infrastructure as well. These systems can be potentially manipulated in a manner that can put our security at risk.

With new technology capabilities come new cyber vulnerabilities that can be taken advantage of in unpredictable ways.

But why are we talking about IoT devices here in Congress? Well, Congress, and the House Oversight and Reform Committee, in particular, have the responsibility to ensure appropriate oversight of the technology that our Federal Government procures and the security of our Federal networks.

The IoT Cybersecurity Improvement Act will ensure that any security gaps in Internet of Things devices are properly and transparently identified by the National Institute of Standards and Technology.

It then requires that the Office of Management and Budget develop and the Department of Homeland Security implement policies requiring Federal agencies to only procure IoT devices that can be securely incorporated into an agency's information systems.

It does this while ensuring that leading private-sector security standards are adopted and improved upon by the Federal Government. Such government and private-sector partnership is key to developing widely useful and effective security standards.

Lastly, H.R. 1668 would ensure that proper disclosure mechanisms exist to report and fix newly discovered security vulnerabilities related to the government's use of IoT devices.

In summary, this bill will help improve the mechanisms protecting the Nation's valuable cybersecurity infrastructure as new technology devices are increasingly used by Federal agencies.

Mr. Speaker, I encourage my colleagues to support this bill. I reserve the balance of my time.

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I yield 5 minutes to the gentlewoman from Illinois (Ms. KELLY). Representative KELLY from Illinois is an outstanding member of our Committee on Oversight and Reform.

Ms. KELLY of Illinois. Mr. Speaker, I thank the chairwoman for yielding.

Mr. Speaker, in October 2017, the IT Subcommittee held a hearing on cybersecurity of the Internet of Things. This hearing was largely held in response to the Mirai botnet, a massive Distributed Denial of Service, or DDoS, attack, which left the internet inaccessible for much of the East Coast.

IoT devices have processing power and an internet connection, but often have little security and no built-in ability to be patched remotely. IoT devices can range from your home routers, security cameras, and baby monitors to smart appliances and industrial sensors.

During the Mirai attack, hackers attempted to log in to common devices using 61 username-password combos that are frequently used as a default for IoT devices and never changed. This tactic gave them access to hundreds of thousands of unsecured IoT devices.

This attack served as a wake-up call.

In 2018, Lieutenant General Robert Ashley, DIA Director, described the exploitation of insecure IoT devices as one of the two ''most important emerging cyber threats to our national security.'' This is why I urge my colleagues to support this bipartisan legislation.

During the hearing and subsequent process, we learned that the U.S. Government is purchasing these IoT devices without a standard for security to prevent them from being used in such an attack or used as an unauthorized access point to U.S. Government networks.

Bipartisan and bicameral conversations necessitated the introduction of this legislation.

H.R. 1668, the IoT Cybersecurity Improvement Act, aims to address supply chain risk to the Federal Government stemming from insecure IoT devices. By establishing light-touch, minimum security requirements for procurement of connected devices by the government, this bill has two main focuses: ensuring the government is purchasing secure devices and resolving critical vulnerabilities to existing devices.

Building upon the amazing work over at NIST, the bill has NIST-published guidelines on the appropriate use and management of Internet of Things devices owned or controlled by a government agency. At a minimum, it will address secure development, identity management, patching, and configuration management for IoT devices.

Following this, OMB will take these guidelines and issue policies and principles consistent with the current law.

To ensure these devices stay secure, this bill creates a coordinated vulnerability disclosure program to receive information about a device's related vulnerabilities.

To improve U.S. cybersecurity and the security of American citizens, agencies would be prohibited from purchasing devices that fail to comply with the minimum security policies and vulnerability disclosure guidance.

□ 1515

Throughout the entire process, I have worked hard to ensure that the requirements of this bill do not impede or conflict with the current and good efforts of NIST or CISA. Both agencies have been issuing excellent guidance on IoT devices and Coordinated Vulnerability Disclosures, and they should be commended for their proactive work and their engagement with me and my team during this process.

This bill offers Congress the opportunity to secure our Federal infrastructure from threats, both foreign

and domestic. We cannot wait as more devices are connected to government networks that could potentially become part of a botnet or an entryway for hackers.

I want to thank everyone: experts, industry leaders, civil society leaders, and my colleagues who made comments and helped us craft a bill that is bipartisan and solves a real problem.

Finally, I have been proud to have worked with my friend and colleague WILL HURD on this legislation. He has always been there when I needed a partner on IT legislation, and he has taught me a lot about technology. His absence from this Chamber will be sorely missed.

I also want to thank Senators WARREN and GARDNER for working with me on this legislation.

This is a strong bill that I believe can pass both Chambers and be signed into law. I hope my colleagues will join me in supporting this important bipartisan piece of legislation.

Mr. KELLER. Mr. Speaker, I yield 3 minutes to the gentleman from Texas (Mr. HURD).

Mr. HURD of Texas. Mr. Speaker, I rise today in support of securing the Internet of Things through the IoT Cybersecurity Improvement Act of 2020.

Every second of the day, more devices are connecting to the internet, and the amount of data we put online through these devices grows. The Internet of Things is the world in which all these devices and information live. The Internet of Things is the world where devices work together to make our lives easier. The Internet of Things is a world where we are always connected.

IoT devices are improving our society. IoT devices are improving our economy. IoT devices are improving healthcare systems, shopping experiences, and just about every other aspect of our lives. The Internet of Things is showing just how innovative humans can be.

But, like most innovations, IoT has the potential to be misused and abused by bad actors.

The Director of the Defense Intelligence Agency has called IoT devices one of ''the most important emerging cyber threats to our national security.''

If our security practices for using the Internet of Things does not evolve as our use of it grows, then we will find out how innovative criminals, hackers, and hostile foreign governments can be.

Securing the Internet of Things is something Congress can actually address, and we are doing just that with the IoT Cybersecurity Improvement Act. The bill reduces the risks associated with introducing new devices into the Federal Government's digital infrastructure. We achieve this goal by establishing minimum security requirements for the supply chain that is used to purchase devices that will be used on government systems.

The IoT Cybersecurity Improvement Act will ensure that taxpayer dollars are only being used to purchase IoT devices that meet basic minimum security requirements. We are taking simple steps to secure our supply chain and protect Americans' personal data and information.

We can take advantage of technology before it takes advantage of us, and one way we accomplish this feat is by passing this piece of legislation that will mitigate vulnerabilities that IoT devices might introduce into Federal networks.

What we are about to do today wouldn't have been possible without my friend and partner from the great State of Illinois, Representative ROBIN KELLY. We have had a lot of fun together and passed a lot of legislation together.

I want to also thank the Committee on Oversight and Reform staff for helping to perfect this legislation. If it weren't for you all, we couldn't have gotten to this point.

I hope all of our colleagues join us in supporting this legislation.

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, if the gentleman has no further speakers, I am prepared to close. I reserve the balance of my time.

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

We often talk about the need for government to be a responsible steward of taxpayer dollars. This responsibility of stewardship extends to safeguarding the public's data and government systems.

With H.R. 1668, we can take positive steps to secure the devices that connect to and interact with our valuable Federal Government networks. These same networks enable critical government missions and protect America's valuable information.

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

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I urge passage of H.R. 1668, as amended, 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 (Mrs. CAROLYN B. MALONEY) that the House suspend the rules and pass the bill, H.R. 1668, as amended.

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

The title of the bill was amended so as to read: ''A bill to establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes.''.

A motion to reconsider was laid on the table.

AI IN GOVERNMENT ACT OF 2020

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2575) to authorize an AI Center of Excellence within the General Services Administration, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2575

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 ''AI in Government Act of 2020''.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''Administrator'' means the Administrator of General Services;

(2) the term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code;

(3) the term ''AI CoE'' means the AI Center of Excellence described in section 3;

(4) the term ''artificial intelligence'' has the meaning given the term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note);

(5) the term ''Director'' means the Director of the Office of Management and Budget;

(6) the term ''institution of higher education'' has the meaning given the term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001); and

(7) the term ''nonprofit organization'' means an organization described in section 501(c)(3)of the Internal Revenue Code of 1986 and exempt from taxation under section 501(a) of that Code.

SEC. 3. AI CENTER OF EXCELLENCE.

(a) IN GENERAL.—There is created within the General Services Administration a program to be known as the ''AI Center of Excellence'', which shall—

(1) facilitate the adoption of artificial intelligence technologies in the Federal Government;

(2) improve cohesion and competency in the adoption and use of artificial intelligence within the Federal Government; and

(3) carry out paragraphs (1) and (2) for the purposes of benefitting the public and enhancing the productivity and efficiency of Federal Government operations.

(b) DUTIES.—The duties of the AI CoE shall include—

(1) regularly convening individuals from agencies, industry, Federal laboratories, nonprofit organizations, institutions of higher education, and other entities to discuss recent developments in artificial intelligence, including the dissemination of information regarding programs, pilots, and other initiatives at agencies, as well as recent trends and relevant information on the understanding, adoption, and use of artificial intelligence;

(2) collecting, aggregating, and publishing on a publicly available website information regarding programs, pilots, and other initiatives led by other agencies and any other information determined appropriate by the Administrator;

(3) advising the Administrator, the Director, and agencies on the acquisition and use of artificial intelligence through technical insight and expertise, as needed;

(4) assist agencies in applying Federal policies regarding the management and use of data in applications of artificial intelligence;

(5) consulting with agencies, including the Department of Defense, the Department of Commerce, the Department of Energy, the Department of Homeland Security, the Office of Management and Budget, the Office of the Director of National Intelligence, and