UNITED STATES OF AMERICA

CYBERSPACE SOLARIUM COMMISSION

CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)

AUGUST 2020

CYBERSECURITY LESSONS FROM THE PANDEMIC: LEGISLATIVE PROPOSALS

LETTER FROM THE EXECUTIVE DIRECTOR

Less than one week after the Cyberspace Solarium Commission launched its March 2020 final report on Capitol Hill, the COVID-19 pandemic forced millions of Americans into lockdown and called into question the ability of our political, economic, public health, and national security institutions and infrastructure to protect our American way of life. Tragically, we were not fully prepared to respond to a crisis of this magnitude. But this country has faced tragedy before, and each time we have been challenged, we have learned from our mistakes and crafted new institutions to better prepare ourselves to withstand the next crisis.

Our Commission witnessed this unfolding non-traditional national security crisis and saw striking parallels to our continued vulnerability in cyberspace. In a May 2020 white paper, "Cybersecurity Lessons from the Pandemic," the Commission identified (1) existing cybersecurity challenges made more pressing by the pandemic response and associated social distancing protocols, and (2) key similarities between our response to the COVID-19 pandemic and our continued vulnerability to cyberattacks of significant consequence. In addition to highlighting the renewed importance of a significant number of the Commission's original recommendations, the white paper included four new recommendations to further bolster our ability to respond to and recover from significant cyber incidents.

This document contains legislative language for those four new proposals, which we hope will lead to their speedy implementation. As with our original legislative proposals, this document was produced by the staff of the Commission, in coordination with our general counsel and trusted legal advisors. Although the staff regularly consulted the Commissioners during this process, these proposals were not edited or approved by the Commissioners themselves and should be taken as the product of the staff alone.

As we have learned the hard way, our government must take significant action to better prepare itself to act with speed and agility in the face of sudden, catastrophic threats to public health, cybersecurity, and our American way of life.

Mark Montgomery
Executive Director
Cyberspace Solarium Commission

CONTENTS

Cybersecurity Lessons from the Pandemic: Legislative Proposals

PAN 1.1 State, Local, and Tribal Information Technology Stimulus and Government Service Modernization Grants Act

This proposal authorizes making grants to State, localities, and tribes to support investments in Information Technology (IT) maintenance and modernization projects to bolster the ability of State, local, and tribal governments to respond to and mitigate effects stemming from the public health emergency with respect to the COVID-19 pandemic.

A BILL

To authorize making grants to States, localities, and tribes to support investment in Information Technology (IT) maintenance and modernization projects, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. SHORT TITLE.

This Act may be cited as the "IT Stimulus and Government Service Modernization Grants Act".

SEC. 2. DEFINITIONS.

In this Act:

(1) FISCAL YEAR.—The term "fiscal year" has the meaning given the term under the State, local, or tribal law of the relevant grant recipient.

(2) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(3) STATE.—The term "State" means each of the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico.

SEC. 3. STATE AND TRIBAL GENERAL INFORMATION TECHNOLOGY MODERNIZATION GRANTS.

(a) AUTHORITY TO PROVIDE ASSISTANCE.—

(1) IN GENERAL.—Not later than 180 days following the enactment of this Act, from amounts made available to carry out this section, the Secretary of Homeland Security shall make grants to States and tribes for the purpose of

funding or procuring, for use by the State, local governments within the State, or tribes—

(A) enterprise email solutions;

(B) enterprise productivity tools (such as word processing and spreadsheets);

(C) cybersecurity services and tools;

(D) customer relationship management;

(E) payroll for State, local or tribal information technology staff; or

(F) any other class of information technology product or service that the Cybersecurity and Infrastructure Security Agency approves.

(2) LIMITATIONS.—

(A) SINGLE GRANT.—A State or tribe may only receive one grant under this section.

(B) SECURITY REQUIRED .—No grant funds awarded pursuant to this section may be used to procure information technology products or services that do not adhere to commonly accepted security standards, as identified by the Secretary pursuant to subsection (j).

(b) APPLICATION.—

(1) APPLICATION REQUIRED.—To be eligible to receive a grant under subsection (a), a State or tribe shall submit an application to the Secretary, at such time and in such manner as the Secretary may require.

(2) APPLICATION NOTICE.—Not later than 90 days following the date of the enactment of this Act, the Secretary shall issue a notice inviting applications for grants pursuant to this section.

(3) APPLICATION ELEMENTS.—The Secretary shall require each application submitted pursuant to this subsection to include—

(A) baseline data that demonstrates the State or tribe's current funding of information technology support and modernization; and

(B) such other information as the Secretary determines appropriate or necessary to carry out or oversee the grant program established under this section.

(c) ELIGIBILITY.—To be eligible for a grant under subsection (a), a State or tribe shall—

(1) commit to maintain its percent of total spending on information technology support and modernization in fiscal year 2019 for fiscal years 2020, 2021, and 2022; and

(2) agree to designate the State or tribal Chief Information Officer, or an equivalent official, as the primary official for the management and allocation of grant funds awarded pursuant to this section.

(d) ALLOCATION OF FUNDS.—Of the amounts made available pursuant to carry out this section, the Secretary—

(1) shall reserve $X0,000,000 for grants to tribes;

(2) may reserve up to $X,000,000 for administration and oversight of activities necessary to carry out this section; and

(3) shall allocate the funds remaining after the application of paragraphs (1) and (2) to States that submit an application pursuant to subsection (b) on the basis of their relative population of individuals.

(e) GRANT AMOUNTS.—In carrying out subsection (d)(3), the Secretary shall not grant any State—

(1) less than $90,000,000; or

(2) more than $500,000,000.

(f) SUBGRANTS.—Each State that receives a grant pursuant to this section shall reserve 30 percent of any funds received for the purpose of—

(1) making subgrants to local governments within the State to procure information technology products and services, consistent with the requirements of this section; or

(2) purchase licenses and products on behalf of local governments under existing State programs and consistent with the requirements of this section.

(g) RETURN OF FUNDS.—A State or tribe shall return to the Secretary any funds received pursuant to this section that the State or tribe does not expend for a

permissible purpose and consistent with the requirements of this section within two years of receiving such funds, and the Secretary shall return such funds to the Treasury.

(h) REPORT.—A State or tribe receiving grant funds pursuant to this section shall submit to the Secretary, at such time and in such manner as the Secretary may require, a report that—

(1) describes the use of the grant funds, including the use of funds made available as subgrants; and

(2) demonstrates the State or tribe's compliance with the requirements of this subsection.

(i) GUIDANCE.—Not later than 90 days following the date of enactment of this Act, the Cybersecurity and Infrastructure Security Agency shall issue guidance to—

(1) assist States and tribes with respect to the prioritization of information technology projects and procurements; and

(2) define any categories of information technology products and services that may be procured or funded pursuant to subsection (a)(1)(F).

(j) SECURITY STANDARDS.—Not later than 90 days of the date of enactment of this Act, the Secretary, in consultation with the Secretary of Commerce, shall select and publish commonly accepted security standards and certifications to which information technology products and services purchased with grant funds awarded pursuant to this section must adhere.

(k) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to carry out this section $XX,000,000,000, which shall remain available until September 30, 2022.

SEC. 4. STATE, LOCAL, AND TRIBAL CRITICAL SERVICES MODERNIZATION GRANTS.

(a) AUTHORITY TO PROVIDE ASSISTANCE.—

(1) IN GENERAL.—From amounts made available to carry out this section, the Secretary shall make grants to States, localities, and tribes for the purpose of securely digitizing critical state, local, and tribal government services.

(2) USE OF FUNDS.—Grant funds awarded pursuant to this section may be used only to procure technologies or information technology services that enable the remote delivery of the following critical government services:

(A) Emergency services.

(B) Government benefit and entitlement programs.

(C) Administrative services performed by a State, local, or tribal, government that the Cybersecurity and Infrastructure Security Agency approves.

(3) LIMITATIONS.—

(A) SINGLE GRANT.—A State, locality, or tribe may not receive more than one grant or subgrant pursuant to this section.

(B) SECURITY REQUIRED.—No grant funds awarded pursuant to this section may be used to procure information technology products or services that do not adhere to commonly accepted security standards, as identified by the Secretary pursuant to subsection (m).

(b) APPLICATION.—

(1) APPLICATION REQUIRED.—To be eligible to receive a grant under subsection (a), a State, locality, or tribe shall submit an application to the Secretary, at such time and in such manner as the Secretary may require.

(2) APPLICATION TIMING.—Not later than 1 year following the enactment of this Act, the Secretary shall issue a notice—

(A) inviting applications for grants pursuant to this section; and

(B) establishing an application submission period, which shall—

(i) commence not later than 1 year after the date of enactment of this Act; and

(ii) remain open for no less than one year.

(3) APPLICATION ELEMENTS.—The Secretary shall require each application submitted pursuant to this subsection to include—

(A) baseline data that demonstrates the State or tribe's current funding of information technology support and modernization; and

(B) such other information as the Secretary determines appropriate or necessary to carry out or oversee the grant program established under this section.

(c) ELIGIBILITY.—To be eligible for a grant under subsection (a), a State, locality, or tribe shall—

(1) commit to maintain its percent of total spending on information technology support and modernization in fiscal year 2019 for the duration of the grant period;

(2) provide matching funds equal to 10 percent of the amount of any grant received pursuant to this section; and

(3) agree to designate the State, locality, or tribal Chief Information Officer, or an equivalent official, as the primary official for the management and allocation of grant funds awarded pursuant to this section.

(d) GRANT AWARDS.

(1) IN GENERAL.— Following the close of the application submission period established pursuant to subsection (b)(2)(B), the Secretary shall—

(A) evaluate each application utilizing the criteria developed pursuant to paragraph (2) of this subsection; and

(B) competitively allocate grant funds based on the merits of the applications received.

(2) CRITERIA.— Not later than 1 year following the date of enactment of this Act, the Secretary shall develop and make available to the public the criteria by which grant applications will be evaluated.

(e) ADMINISTRATIVE COSTS.—Of the amounts made available pursuant to carry out this section, the Secretary may reserve up to $X,000,000 for administration and oversight of activities necessary to carry out this section.

(f) GRANT AMOUNTS.—In carrying out subsection (d)(3), the Secretary may not award any grant that is—

(1) less than $X00,000; or

(2) more than $X00,000,000.

(g) DISBURSEMENT OF FUNDS.—Grant funds awarded pursuant to this section shall be dispersed in structured payments over a period of five years, in such increments as the Secretary determines appropriate for the project or procurement to be carried out using the funds.

(h) CONTINUED MAINTENANCE FUND.—

(1) ESTABLISHMENT.—A State, locality, or tribe receiving a grant pursuant to this section shall establish a "Continued Maintenance Fund" which—

(A) may not be accessed during the grant period; and

(B) shall be used for the continued maintenance of programs and projects funded by a grant awarded pursuant to this section.

(2) FUNDS REQUIRED.—A State, locality, or tribe receiving a grant pursuant to this section shall deposit 10 percent of the amount of any grant received and 10 percent of the matching funds required pursuant to subsection (c)(2) into the "Continued Maintenance Fund" required by paragraph (1).

(i) SUBGRANTS.—The Secretary may—

(1) accept an application from a State for statewide or multi-jurisdiction projects; and

(2) permit the State to allocate grant funds awarded pursuant to such an application as subgrants, provided that the subgrantees are named in the State's initial grant application.

(j) RETURN OF FUNDS.—A State, locality, or tribe shall return to the Secretary any funds received pursuant to this section that the State, locality, or tribe does not expend for a permissible purpose and consistent with the requirements of this section within five years of receiving such funds, and the Secretary shall return such funds to the Treasury.

(k) REPORT.—A State, locality, or tribe receiving a grant pursuant to this section shall submit to the Secretary, at such time and in such manner as the Secretary may require, a report that—

(1) describes the use of the grant funds, including the use of funds made available as subgrants; and

(2) demonstrates the State, locality, or tribe's compliance with the requirements of this subsection.

(l) GUIDANCE.—Not later than 1 year following the enactment of this Act, the Cybersecurity and Infrastructure Security Agency shall issue guidance to—

(1) assist States, localities, and tribes in prioritizing projects and procurements for the purpose of digitizing critical government services; and

(2) define any additional categories of government administrative services for which grant funds awarded pursuant to this section may be expended pursuant to subsection (a)(2)(C).

(m) SECURITY STANDARDS.—Not later than 1 year following the date of enactment of this Act, the Secretary, in consultation with the Secretary of Commerce, shall select and publish commonly accepted security standards and certifications to which information technology products and services purchased with grant funds awarded pursuant to this section must adhere.

(n) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to carry out this section $XX,000,000,000, which shall remain available until September 30, 202X.

PAN 1.1.a State, Local, and Tribal General Information Technology Modernization Grant (Appropriation)

For making grants to States and tribes to support investment in IT maintenance and modernization projects to bolster the ability of State, local, and tribal governments to respond to and mitigate effects stemming from the public health emergency with respect to the Coronavirus Disease (COVID–19), $XX,000,000,000, to remain available until September 30, 2022: *Provided*, That the Secretary of Homeland Security (referred to under this heading as "Secretary") shall make grants to States and tribes for the purpose of procuring IT products and services for use by the State, local governments within the State, or tribes: *Provided further*, That the Secretary may reserve up to $X,000,000 for administration and oversight of the activities under this heading: *Provided further*, That of the amounts made available under this heading, the Secretary shall reserve $X0,000,000 for distribution to tribes for the purpose of procuring IT products and services: *Provided further*, That the Secretary shall allocate remaining funds made available to carry out this heading to the States on the basis of their relative population of individuals: *Provided further*, That each State grant shall not be less than $XX,000,000 and not more than $X00,000,000: *Provided further*, That States shall allocate X percent of the funds received under this heading as subgrants to local governments to procure IT products and services or purchase licenses and products on behalf of local governments under existing state programs and consistent with the requirements of this heading: *Provided further*, That a State or tribe shall return to the Secretary any funds received pursuant to this heading that the State or tribe does not expend for a permissible purpose within two years of receiving such funds, and the Secretary shall return such funds to the Treasury: *Provided further*, a State, tribe, or local government receiving funds pursuant to this heading may use the funds only to procure enterprise email solutions, enterprise productivity tools (such as word processing and spreadsheets), cybersecurity services and tools, customer relationship management, payroll for IT staff, or another class of IT product or service that the Cybersecurity and Infrastructure Security Agency approves: *Provided further*, That within 90 days of the date of enactment of this Act, the Cybersecurity and Infrastructure Security Agency shall issue guidance on the prioritization of IT projects and procurements by States and tribes, including further defining the categories of permissible IT products and services. *Provided further*, That a State or tribe desiring to receive an allocation under this heading shall submit an application at such time, in such manner, and containing such information as the Secretary may reasonably require: *Provided further*, That the Secretary shall issue a notice inviting applications not later than 90 days after the date of enactment of this Act: *Provided further*, That the Secretary shall distribute funding under this heading within 180 days of the date of enactment of this Act: *Provided further*, That any State or tribe receiving funding under this heading shall maintain its percent of total

spending on IT support and modernization in fiscal year 2019 for fiscal years 2020, 2021, and 2022: *Provided further*, That a State or tribe's application shall include baseline data that demonstrates the State or tribe's current funding of IT support and modernization: *Provided further*, That a State or tribe's application shall affirm the primary role of the State Chief Information Officer, or an equivalent official, in the management and allocation of funds received pursuant to this heading: *Provided further*, That a State or tribe receiving funds under this heading shall submit a report to the Secretary, at such time and in such manner as the Secretary may require, that describes the use of funds, including the use of funds made available as subgrants: *Provided further*, That no recipient of funds under this heading shall use the funds to procure IT products or services that do not adhere to commonly accepted security standards, as identified by the Secretary: *Provided further*, That within 90 days of the date of enactment of this Act, the Secretary, in consultation with the Secretary of Commerce, shall select and publish commonly accepted security standards and certifications to which IT products and services purchased with funds made available under this heading must adhere. *Provided further*, That the term "fiscal year" shall have the meaning given such term under State law: *Provided further*, That the term "State" means each of the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico: *Provided further*, That such amount is designated by the Congress as being for an emergency requirement pursuant to section 251(b)(2)(A)(i) of the Balanced Budget and Emergency Deficit Control Act of 1985.

PAN 1.1.b State, Local, and Tribal Critical Services Modernization Fund (Appropriation)

For making grants to States, localities, and tribes to support investment in IT maintenance and modernization projects to bolster the ability of State and local governments to respond to and mitigate effects stemming from the public health emergency with respect to the Coronavirus Disease (COVID–19), $XX,000,000,000, to remain available until September 30, 202X: *Provided*, That the Secretary of Homeland Security (referred to under this heading as "Secretary") shall make grants to States, localities, and tribes for the purpose of securely digitizing critical state, local, and tribal government services: *Provided further*, That the Secretary may reserve up to $X,000,000 for administration and oversight of the activities under this heading: *Provided further*, That each grant shall not be less than $X00,000 and not more than $X00,000,000: *Provided further*, That an individual State, local, or tribal government may receive no more than one grant under this fund: *Provided further*, That a State, locality, or tribe shall return to the Secretary any funds received pursuant to this heading that the State, locality, or tribe does not expend for a permissible purpose within five years of receiving such funds, and the Secretary shall return such funds to the Treasury: *Provided further*, That a State, local, or tribal government receiving funds pursuant to this heading may use the funds only to procure technologies or information technology services that enable the remote delivery of critical government services, including emergency services, government benefit and entitlement programs, and other administrative services performed by a State, local, or tribal, government, that the Cybersecurity and Infrastructure Security Agency approves: *Provided further*, That any State, locality, or tribe receiving funding under this heading shall maintain its percent of total spending on IT support and modernization in fiscal year 2019 for the duration of the grant: *Provided further*, That within one year of the date of enactment of this Act, the Cybersecurity and Infrastructure Security Agency shall issue guidance on the prioritization of IT projects and procurements by States, localities, and tribes, including further defining the categories of permissible IT products and services: *Provided further*, That within one year of the enactment of this Act, the Secretary of Homeland Security shall issue requirements and procedures for applications for grant funding and guidance on criteria by which grant applications will be evaluated: *Provided further,* That the Secretary shall issue a notice inviting applications not later than one year after the date of enactment of this Act: *Provided further*, That a a State, locality, or tribe desiring to receive a grant under this heading shall submit an application at such time, in such manner, and containing such information as the Secretary may reasonably require: *Provided further*, That the window for grant application submission shall begin no later than one year after the date of enactment of this Act and remain open for no less than one year: *Provided further*, That, following the end of application window, the grant funds shall be awarded competitively

based on the merits of projects and program proposals: *Provided further*, That awarded funds shall be disbursed in structured payments over a five-year period: *Provided further*, That any State, local, or tribal government receiving funding under this heading shall provide ten percent matching funds: *Provided further*, That any State, local, or tribal government recipient of funding shall commit ten percent of grant funding received under this heading and ten percent of all matching funds required pursuant to the previous proviso to a State, local, or tribal "Continued Maintenance Fund" to be managed by the Chief Information Officer, or equivalent official, of a State, locality, or tribe: *Provided further*, That the "Continued Maintenance Fund" required pursuant to the previous proviso shall not be accessed during the duration of the grant period and shall be used for the continued maintenance of programs and projects funded by a grant received under this heading after the five-year disbursement period. *Provided further*, That any application made by a State, locality, or tribe shall affirm the primary role of the State, locality, or tribal Chief Information Officer, or an equivalent official, in the management and allocation of funds received pursuant to this heading; *Provided further*, That the Secretary may permit a State to submit an application for Statewide or multi-jurisdiction projects and further permit the State to allocate grant funds as subgrants to localities named in the grant application; *Provided further*, That a State, locality, or tribe receiving funds under this heading shall submit a report to the Secretary, at such time and in such manner as the Secretary may require, that describes the use of funds, including the use of funds made available as subgrants: *Provided further*, That no recipient of funds under this heading shall use the funds to procure IT products or services that do not adhere to commonly accepted standards, to include security standards, as identified by the Secretary: *Provided further*, That within one year of the date of enactment of this Act, the Secretary, in consultation with the Secretary of Commerce, shall select and publish, or update previously published, commonly accepted security standards and certifications to which IT products and services purchased with funds made available under this heading must adhere. *Provided further*, That the term "fiscal year" shall have the meaning given such term under State law: *Provided further*, That the term "State" means each of the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico: *Provided further*, That such amount is designated by the Congress as being for an emergency requirement pursuant to section 251(b)(2)(A)(i) of the Balanced Budget and Emergency Deficit Control Act of 1985.

PAN 1.2 Pass an Internet of Things Security Law

This proposal implements the Commission's recommendation to pass an Internet of Things (IoT) security law. The law focuses on known challenges, like unsecured Wi-Fi routers, and mandates that these devices have reasonable security measures, such as those outlined under the National Institute of Standards and Technology's "Recommendations for IoT Device Manufacturers." The law stresses the creation of enduring standards both for authentication, such as requiring default passwords that a user must change to their own authentication mechanism upon first use, and for patching, such as ensuring a device is capable of receiving a remote update. The proposal explicitly tasks the Federal Trade Commission with enforcement of the law on the basis of existing authorities under Section 5 of the Federal Trade Commission Act. Parts of this legislation are modeled on the IoT Cybersecurity Act of 2019.

A BILL

To create an Internet of Things (IoT) security law to strengthen the security of IoT devices sold in the United States, and for other purposes.

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".

SEC. 2. ACTS PROHIBITED.

(a) MANUFACTURE OF INSECURE COVERED INTERNET OF THINGS DEVICES.—It shall be unlawful for a manufacturer of a covered Internet of Things device, as defined in section 3 of this Act, to manufacture any covered Internet of Things device that does not meet the minimum security requirements set forth in the regulations prescribed under section 5 of this Act.

(b) SALE, LICENSING, OR OTHERWISE OFFER OF INSECURE COVERED INTERNET OF THINGS DEVICES.—It shall be unlawful for any person to knowingly cause the importation into the United States, to offer for sale, to offer for license or lease, or otherwise offer any covered Internet of Things device that does not meet the minimum security requirements set forth in the regulations prescribed under section 5 of this Act.

(c) EXCEPTIONS.—Notwithstanding the prohibitions in subsection (a) and (b), it shall not be unlawful:

(1) For an individual or business to manufacture and distribute a covered Internet of Things device that does not meet the minimum security requirements set forth in the regulations prescribed under section 5 of this Act for the purposes of free-of-cost prototyping or demonstration.

(2) For an individual to build for personal use or educational purposes a covered Internet of Things device that does not meet the minimum security requirements set forth in the regulations prescribed under section 5 of this Act.

(3) To purchase or cause the importation of a covered Internet of Things device that does not meet the minimum security requirements set forth in the regulations prescribed under section 5 of this Act in order to conduct security research on such covered Internet of Things device.

(4) For an individual consumer to resell a covered Internet of Things device that does not meet the minimum security requirements set forth in the regulations prescribed under section 5 of this Act, provided that the device offered for resale was originally purchased for personal use by such individual consumer.

(5) To offer for sale, or to offer for license or lease, an automobile, mobile home, motorcycle, airplane, helicopter or other transportation device containing a covered Internet of Things device that does not meet the minimum security requirements set forth in the regulations prescribed under section 5 of this Act.

SEC. 3. COVERED INTERNET OF THINGS DEVICES DEFINED.

(a) IN GENERAL.—For the purposes of this Act, the term "covered Internet of Things device" means any embedded system containing at least one transducer and at least one network interface that can function on its own, though it may be dependent on specific other devices.

(b) EXEMPTION.—The term "covered Internet of Things device" as defined in subsection (a) shall not include:

(1) Any embedded system that is not designed to interact with an industrial control system and has been determined by the National Institute of Standards and Technology pursuant to section 4 of this Act not to pose undue risk to health and human safety, privacy, or cybersecurity.

(2) Any embedded system with an intended operational life that is no longer than 30 days.

(3) Any of the following classes of technology if they are not embedded in a physical system:

(A) Laptops.

(B) Tablets.

(C) Personal computers.

(D) Smartphones.

(E) High performance computers.

SEC. 4. CONSIDERATIONS AND RECOMMENDATIONS REGARDING MINIMUM SECURITY GUIDELINES FOR INTERNET OF THINGS DEVICES.

(a) INITIAL IDENTIFICATION OF MINIMUM SECURITY GUIDELINES.—

(1) IN GENERAL.—Within one year of the enactment of this Act, the Director of the National Institute of Standards and Technology, in consultation with the Secretary of Homeland Security, shall identify and publish minimum security guidelines for Internet of Things devices, to include standards, guidelines, and frameworks. To the maximum extent appropriate, standards, guidelines, and frameworks for minimum security guidelines for Internet of Things devices shall—

(A) account for the relative risk profile of different classes of covered Internet of Things devices;

(B) contain sufficient specificity to permit an objective evaluation of an Internet of Things device against such standard, guideline, or framework; and

(C) be verifiable by third parties.

(2) CONSULTATION WITH RELEVANT STAKEHOLDERS.—

(A) NOTICE.—Within 180 days of the enactment of this Act, the Director of the National Institute of Standards and Technology shall publish a notice for dates for no less than three separate open consultations with relevant industry and consumer stakeholders representing a diverse cross-section of interests.

(B) INITIAL CONSULTATION.—Within 12 months of the enactment of the Act, the Director of the National Institute of Standards and

Technology shall hold no less than three separate open consultations with relevant industry and consumer stakeholders representing a diverse cross-section of interests.

(3) CONSISTENCY WITH ONGOING EFFORTS.—Consistent with the standards conformity requirements enumerated in section 2(b) of the National Institute of Standards and Technology Act (15 U.S.C. 272(b)) and the findings of the Office of Management and Budget Circular No. A-119, in developing the guidelines required pursuant to this subsection, the Director of the National Institute of Standards and Technology shall prioritize, consider, and incorporate to the maximum extent appropriate efforts by other United States government agencies, existing international standards, voluntary consensus standards, as well as other standards and findings of industry and international standards bodies relating to managing Internet of Things cybersecurity risks.

(4) CONFORMITY REVIEW.—The Director of the National Institute of Standards and Technology shall conduct a review and publish a list of existing standards that shall be deemed to meet the minimum security guidelines published pursuant to paragraph (1).

(b) ASSESSMENT AND UPDATE OF MINIMUM SECURITY GUIDELINES.—

(1) ASSESSMENT AND UPDATE CYCLE.—Every 24 months, the Director of the National Institute of Standards and Technology, in consultation with the Secretary of Homeland Security, shall assess and update the guidelines established pursuant to subsection (a) for minimum security guidelines for Internet of Things devices.

(2) CONSULTATION WITH RELEVANT STAKEHOLDERS.—The Director of the National Institute of Standards and Technology shall publish a notice for and hold no less than three open consultations with relevant industry and consumer stakeholders representing a diverse cross-section of interest per 24-month cycle.

(3) CONSISTENCY WITH ONGOING EFFORTS.—The Director of the National Institute of Standards and Technology shall ensure that updates to guidelines developed under this subsection prioritize, consider, and incorporate to the maximum extent appropriate efforts by other government agencies, existing international standards, voluntary consensus standards, as well as other standards and findings of industry and international standards bodies relating to managing Internet of Things cybersecurity risks, consistent with the standards conformity requirements enumerated in section 2(b) of the National Institute of Standards and Technology Act (15

U.S.C. 272(b)) and the findings of the Office of Management and Budget Circular No. A-119.

(4) CONFORMITY REVIEW.—The Director of the National Institute of Standards and Technology shall conduct a review and publish a list of existing standards that shall be deemed to meet the updated minimum security guidelines published pursuant to paragraph (1).

(c) DETERMINATION OF EXEMPT TECHNOLOGIES.—As appropriate, the Director of the National Institute of Standards and Technology may develop a list of embedded systems that qualify for the exemption in section (3)(b)(1) of this Act.

SEC. 5. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) ENFORCEMENT.—Section 2 of this Act shall be enforced by the Federal Trade Commission in the same manner, by the same means, and with the same jurisdiction as though all applicable terms of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(b) VIOLATION TREATED AS UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A violation of section 2 of this Act shall be treated as an unfair and deceptive act or practice proscribed under a rule issued under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(c) REGULATIONS.—Not later than 18 months after the enactment of this Act, to carry out the prohibitions in section 2 of this Act, the Federal Trade Commission shall, in consultation with relevant agencies to include the National Institute of Standards and Technology promulgate regulations pursuant to section 553 of title 5, United States Code, that:

(1) Require that the manufacturer of any covered Internet of Things device to ensure that any covered Internet of Things device it manufactures meets minimum security requirements, consistent with the guidelines published by the National Institute of Standards and Technology pursuant to section 4 of this Act.

(2) Require that any person selling, licensing, or otherwise offering a covered Internet of Things device for purchase shall not knowingly cause the importation into the United States or offer any covered Internet of Things device that does not meet minimum security requirements, consistent with the guidelines published by the National Institute of Standards and Technology pursuant to section 4 of this Act.

(3) Require that any person or business manufacturing a covered Internet of Things device shall attest to the Federal Trade Commission compliance with the regulations prescribed in subparagraph (1).

(4) Require that any person or business selling, licensing, or otherwise offering a covered Internet of Things shall attest to the Federal Trade Commission compliance with the regulations prescribed in subparagraph (2).

(d) UPDATE OF FEDERAL TRADE COMMISSION REGULATIONS.—Not later than 1 year after the publication of any updated guidelines issued by the National Institute of Standards and Technology pursuant to section 4(b) of this Act, the Federal Trade Commission shall issue updated regulations under subsection (c), to the extent necessary to achieve consistency with the National Institute of Standards and Technology guidelines.

(e) ENFORCEMENT PRIORITIES.—In carrying out this section, the Federal Trade Commission shall prioritize actions related to:

(1) Customer Premise Equipment Routers.

(2) Devices that interact with industrial control systems.

(3) Devices that collect personal health information.

(4) Medical devices.

(f) NO PRIVATE RIGHT OF ACTION.—Nothing in this Act may be construed to create a private right of action for enforcement of any provision of this Act.

SEC. 6. EFFECTIVE DATE.

(a) MANUFACTURING REQUIREMENTS.—The prohibition in section 2(a) of this Act shall take effect on the date that is 1 year after the Federal Trade Commission publishes the regulations required pursuant to section 5(c) and 5(d).

(b) PROHIBITION ON IMPORTATION OR SALE.—The prohibition in section 2(b) of this Act shall take effect on the date that is 18 months after the Federal Trade Commission publishes the regulations required pursuant to section 5(c) and 5(d).

SEC. 7. DEFINITIONS.

In this Act:

(1) EMBEDDED SYSTEM.— The term "embedded system" refers to a combination of computer hardware and software, and perhaps additional mechanical or other parts,

designed to perform a dedicated function. In some cases, embedded systems are part of a larger system or product.

(2) INTENDED OPERATIONAL LIFE.—The term "intended operational life" refers to the total time an embedded system is designed to perform its intended function.

(3) INDUSTRIAL CONTROL SYSTEM.—The term "industrial control system" means an operational technology used to measure, control, or manage industrial functions, and includes supervisory control and data acquisition systems, distributed control systems, and programmable logic or embedded controllers.

(4) PROTOTYPING.—The term "prototyping" refers to the creation of the first, or preliminary, version of an Internet of Things device for the purposes of testing the device.

(5) DEMONSTRATION.—The term "demonstration" refers to the creation of an example or an otherwise incomplete version of a conceivable Internet of Things product, put together as proof of concept with the primary purpose of showcasing the possible applications, feasibility, performance and method of an idea for a new technology.

SEC. 8. EFFECT ON STATE LAW.

The provisions of this Act, and any regulation issued pursuant to this Act, shall preempt any provision of the law of any State, or a political subdivision thereof, directly relating to security requirements for Internet of Things devices offered in interstate commerce. Nothing in this section may be construed to preempt any provision of any data protection or data privacy law that does not impose security requirements for Internet of Things devices offered in interstate commerce.

PAN 1.3 Support Nonprofits That Assist Law Enforcement's Cybercrime and Victim Support Efforts

This proposal provides grants through the Department of Justice's Office of Justice Programs to help fund cyber-specific nonprofit organizations that collaborate with law enforcement in writing cybercrime reports, carrying out enforcement operations, and providing victim support services. As the COVID-19 pandemic has proven, trusted nonprofit organizations serve as critical law enforcement partners that can quickly mobilize to help identify and dismantle major online schemes. Such nonprofits have the expertise and flexibility to reinforce law enforcement efforts to disrupt cybercrime and assist victims. However, they often face financial challenges.

A BILL

To increase support to nonprofits that assist law enforcement's cybercrime and victim support efforts, and for other purposes.

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 "Cybercrime Victim Support Act".

SEC. 2. GRANTS TO NONPROFIT ORGANIZATIONS THAT SUPPORT LAW ENFORCEMENT IN COMBATTING CYBERCRIME.

(a) AUTHORITY TO PROVIDE ASSISTANCE.—From amounts made available to carry out this section, the Attorney General shall make grants to organizations described in 501(c)(3) of the Internal Revenue Code of 1986 (hereinafter "nonprofit organization") that collaborate with law enforcement by writing cybercrime reports, supporting enforcement operations, and providing victim support services.

(b) APPLICATION .—

(1) APPLICATION REQUIRED.—To be eligible to receive a grant under subsection (a), a prospective grantee shall submit an application to the Attorney General, at such time and in such manner as the Attorney General may require.

(2) APPLICATION REQUIREMENTS.—Not later than 90 days following the date of the enactment of this Act, the Attorney General shall issue requirements and

procedures for applications for grant funding and guidance on criteria by which grant applications will be evaluated.

(3) APPLICATION NOTICE.—The Attorney General shall issue a notice inviting applications not later than 180 days after the date of enactment of this Act.

(c) ELIGIBILITY.—

(1) An entity applying for a grant must be a non-profit organization with programming or projects producing cybercrime reports supporting enforcement operations and providing victim support services.

(2) A nonprofit organization desiring to receive a grant under this heading shall submit an application at such time, in such manner, and containing such information as the Attorney General may reasonably require.

(3) No grantee may receive multiple concurrent grants from this fund.

(d) GRANTEE SELECTION.—Following the end of an application window, the Attorney General shall award grant funds competitively, in consultation with the Secretary of the Department of Homeland Security and Director of the National Science Foundation, based on the merits of projects and program proposals.

(e) ALLOCATION OF FUNDS.—Of the amounts made available pursuant to carry out this section, the Attorney General—

(1) shall reserve $XX,000,000 for grants to nonprofit organizations; and

(2) may reserve up to $X,000,000 for administration and oversight of activities necessary to carry out this section.

(f) GRANT AMOUNTS.—In carrying out subsection (d), the Attorney General shall not grant any nonprofit organization—

(1) less than $100,000; or

(2) more than $5,000,000.

(g) RETURN OF FUNDS.—A nonprofit organization shall return to the Attorney General any funds received pursuant to this section that the nonprofit organization does not expend for a permissible purpose and consistent with the requirements of this section within two years of receiving such funds, and the Attorney General shall return such funds to the Treasury.

(h) GRANTEE REPORT.—A nonprofit organization receiving grant funds pursuant to this section shall submit to the Attorney General, at such time and in such manner as the Attorney General may require, a report that—

(1) describes the grantee's use of the grant funds, including the use of funds made available as subgrants; and

(2) demonstrates the grantee's compliance with the requirements of this subsection.

(i) REPORT TO CONGRESS.—Not later than one year after the disbursement of the first grant and annually until the expiration of the funds made available pursuant to this heading, the Attorney General, in consultation with the Secretary of the Department of Homeland Security and Director of the National Science Foundation, shall submit to Congress a report detailing the total amount of funds disbursed, the grantees, the programs administered, and the assessed results of these programs.

(j) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to carry out this section $XX,000,000,000, which shall remain available until September 30, 202X.

PAN 1.3.a Grants to Nonprofits that Assist Law Enforcement's Cybercrime and Victim Support Efforts (Appropriation)

For making grants to organizations described in 501(c)(3) of the Internal Revenue Code of 1986 that collaborate with law enforcement in writing cybercrime reports, carrying out enforcement operations, and providing victim support services, $XX,000,000, to remain available until September 30, 202X: *Provided*, That the Attorney General shall make grants to organizations described in 501(c)(3) of the Internal Revenue Code of 1986 for the purposes of assisting law enforcement in the identification and dismantling of cybercrime schemes or supporting victims of cybercrime: *Provided further*, That the Department of Justice's Office of Justice Programs shall be responsible for the day-to-day administration of this grant program: *Provided further*, That the Attorney General may reserve up to $X,000,000 for administration and oversight of the activities under this heading: *Provided further*, That each grant shall not be less than $X00,000 and not more than $X,000,000: *Provided further*, That a grantee may not receive multiple concurrent grants from this fund: *Provided further*, That a grantee shall return to the Attorney General any funds received pursuant to this heading that the grantee does not expend for a permissible purpose within five years of receiving such funds, and the Attorney General shall return such funds to the Treasury: *Provided further*, That a grantee receiving funds pursuant to this heading may use the funds only to hire staff, procure resources, or otherwise administer a program to assist law enforcement in the identification and dismantling of cybercrime schemes or supporting victims of cybercrime: *Provided further*, That within 90 days of the enactment of this Act, the Attorney General shall issue requirements and procedures for applications for grant funding and guidance on criteria by which grant applications will be evaluated: *Provided further*, That the Attorney General shall issue a notice inviting applications not later than 180 days after the date of enactment of this Act: *Provided further*, That a grantee desiring to receive a grant under this heading shall submit an application at such time, in such manner, and containing such information as the Attorney General may reasonably require: *Provided further*, That the Attorney General shall notice a window for grant application submissions annually and that such application window shall remain open for not less than 90 days: *Provided further*, That following the end of an application window, the grant funds shall be awarded competitively based on the merits of projects and program proposals: *Provided further*, That a grantee receiving funds under this heading shall submit a report to the Attorney General, at such time and in such manner as the Attorney General may require, that describes the use of funds, including the use of funds made available as subgrants: *Provided further*, That not later than one year after the disbursement of the first grant and annually until the expiration of the funds made available pursuant to this heading, the Attorney General, shall submit to Congress a

report detailing the total amount of funds disbursed, grantees, the programs administered, and the assessed results of these programs.

PAN 1.4 Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns

This proposal authorizes the Department of Justice to provide grants, in consultation with the Department of Homeland Security and the National Science Foundation, to nonprofit centers seeking to identify, expose, and explain malign foreign influence campaigns to the American public while putting those campaigns in context to avoid amplifying them. Such malign foreign influence campaigns can include covert foreign state and non-state propaganda, disinformation, or other inauthentic activity across online platforms, social networks, or other communities. These centers should analyze and monitor foreign influence operations, identify trends, put those trends into context, and create a robust, credible source of information for the American public. To ensure success, these centers should be well-resourced and coordinated with ongoing government efforts and international partners' efforts.

A BILL

To increase nongovernmental capacity to identify and counter foreign disinformation and influence campaigns, and for other purposes.

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 "Combating Malign Foreign Influence Operations and Campaigns through Civil Society Act".

SEC. 2. GRANTS TO NONPROFIT ORGANIZATIONS TO INCREASE NON GOVERNMENTAL CAPACITY TO IDENTIFY AND COUNTER MALICIOUS FOREIGN INFLUENCE OPERATIONS AND CAMPAIGNS.

(a) AUTHORITY TO PROVIDE ASSISTANCE.—From amounts made available to carry out this section, the Attorney General shall make grants to organizations described in 501(c)(3) of the Internal Revenue Code of 1986 (hereinafter "nonprofit organization") seeking to identify, expose, explain, and counter malign foreign influence operations and campaigns targeting the American public.

(b) ASSISTANCE PRIORITIZATION.—Within one year of the date of enactment of this Act, the Department of Justice, in consultation with the Department of State and Department of Homeland Security, shall issue guidance on the scope of malign foreign influence operations and campaigns to be countered, ensuring adequate protections for domestic freedom of expression as guaranteed by the U.S. Constitution.

(c) APPLICATION.—

(1) APPLICATION REQUIRED.—To be eligible to receive a grant under subsection (a), a prospective grantee shall submit an application to the Attorney General, at such time and in such manner as the Attorney General may require.

(2) APPLICATION REQUIREMENTS.—Not later than 90 days following the date of the enactment of this Act, the Attorney General shall issue requirements and procedures for applications for grant funding and guidance on criteria by which grant applications will be evaluated.

(3) APPLICATION NOTICE.—The Attorney General shall issue a notice inviting applications not later than 180 days after the date of enactment of this Act.

(d) ELIGIBILITY.—

(1) An entity applying for a grant must be an organization described in 501(c)(3) of the Internal Revenue Code of 1986 with programming or projects that seek to identify, expose, explain, and counter malign foreign influence operations and campaigns targeting the American public.

(2) A nonprofit organization desiring to receive a grant under this heading shall submit an application at such time, in such manner, and containing such information as the Attorney General may reasonably require.

(3) No grantee may receive multiple concurrent grants from this fund.

(e) GRANTEE SELECTION.—

(1) Following the end of an application window, the grant funds shall be awarded competitively based on the merits of projects and program proposals.

(2) The Attorney General shall consult the Secretary of Homeland Security, the Secretary of State, and the Director of the National Science Foundation in order to select suitable grantees and administer the granted funds.

(f) ALLOCATION OF FUNDS.—Of the amounts made available pursuant to carry out this section, the Attorney General—

(1) shall reserve $XX,000,000 for grants to nonprofit organizations; and

(2) may reserve up to $X,000,000 for administration and oversight of activities necessary to carry out this section.

(g) GRANT AMOUNTS.—In carrying out subsection (e), the Secretary shall not grant any nonprofit organization—

(1) less than $100,000; or

(2) more than $5,000,000.

(h) GRANTEE USE OF FUNDS.—

(1) A grantee receiving funds pursuant to this heading may use the funds only to hire staff, procure resources, or otherwise administer a program to analyze and monitor foreign influence operations, identify trends, contextualize trends, and create a robust, credible source of information for the American public.

(2) A grantee receiving funds pursuant to this heading shall publish its findings for consumption by the American public at no fee.

(i) RETURN OF FUNDS.—A nonprofit organization shall return to the Attorney General any funds received pursuant to this section that the nonprofit organization does not expend for a permissible purpose and consistent with the requirements of this section within two years of receiving such funds, and the Attorney General shall return such funds to the Treasury.

(j) GRANTEE REPORT.—A nonprofit organization receiving grant funds pursuant to this section shall submit to the Attorney General, at such time and in such manner as the Attorney General may require, a report that—

(1) describes the grantee's use of the grant funds, including the use of funds made available as subgrants; and

(2) demonstrates the grantee's compliance with the requirements of this subsection.

(k) REPORT TO CONGRESS.—Not later than one year after the disbursement of the first grant and annually until the expiration of the funds made available pursuant to this heading, the Attorney General, in consultation with the Secretary of the Department of Homeland Security, the Secretary of the Department of State, and Director of the National Science Foundation, shall submit to Congress a report detailing the total amount of funds disbursed, the grantees, the programs administered, and the assessed results of these programs.

(l) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to carry out this section $XX,000,000,000, which shall remain available until September 30, 202X.

(m) DEFINITIONS.—

(1) FOREIGN INFLUENCE CAMPAIGN.—As used in this Act, the term "foreign influence campaign" holds the same meaning as in 50 USC 3021(h).

PAN 1.4.a Increase Nongovernmental Capacity to Identify and Counter Foreign Disinformation and Influence Campaigns (Appropriation)

For making grants to organizations described in 501(c)(3) of the Internal Revenue Code of 1986 seeking to identify, expose, and explain malign foreign influence campaigns to the American public, $XX,000,000, to remain available until September 30, 202X: *Provided*, That the Attorney General shall make grants to organizations described in 501(c)(3) of the Internal Revenue Code of 1986 for the purposes of identifying and countering foreign disinformation and influence campaigns: *Provided further*, That the Attorney General shall consult the Secretary of Homeland Security and the Director of the National Science Foundation in order to select suitable grantees and administer the granted funds: *Provided further*, That the Attorney General may reserve up to $X,000,000 for administration and oversight of the activities under this heading: *Provided further*, That each grant shall not be less than $X00,000 and not more than $X,000,000: *Provided further*, That a grantee may not receive multiple concurrent grants from this fund: *Provided further*, That a grantee shall return to the Attorney General any funds received pursuant to this heading that the grantee does not expend for a permissible purpose within five years of receiving such funds, and the Attorney General shall return such funds to the Treasury: *Provided further*, That a grantee receiving funds pursuant to this heading may use the funds only to hire staff, procure resources, or otherwise administer a program to analyze and monitor foreign influence operations, identify trends, put those trends into context, and create a robust, credible source of information for the American public: *Provided further*, That a grantee receiving funds pursuant to this heading shall publish its findings for consumption by the American public: *Provided further*, That within one year of the date of enactment of this Act, the Department of Justice shall issue guidance on the scope of malign foreign influence campaigns to be countered, ensuring adequate protections for domestic freedom of expression as guaranteed by the U.S. Constitution: *Provided further*, That within 90 days of the enactment of this Act, the Attorney General shall issue requirements and procedures for applications for grant funding and guidance on criteria by which grant applications will be evaluated: *Provided further*, That the Attorney General shall issue a notice inviting applications not later than 180 days after the date of enactment of this Act: *Provided further*, That a grantee desiring to receive a grant under this heading shall submit an application at such time, in such manner, and containing such information as the Attorney General may reasonably require: *Provided further*, That the Attorney General shall notice a window for grant application submissions annually and that such application window shall remain open for not less than 90 days: *Provided further*, That following the end of an application window, the grant funds shall be awarded competitively based on the merits of projects and program proposals: *Provided further*, That a grantee receiving funds under this heading shall submit a report to the Attorney General, at such time and in such

manner as the Attorney General may require, that describes the use of funds, including the use of funds made available as subgrants: *Provided further*, That not later than one year after the disbursement of the first grant and annually until the expiration of the funds made available pursuant to this heading, the Attorney General, in consultation with the Secretary of the Department of Homeland Security and Director of the National Science Foundation, shall submit to Congress a report detailing the total amount of funds disbursed, the grantees, the programs administered, and the assessed results of these programs.


U.S. CYBERSPACE SOLARIUM COMMISSION