Guthrie
Hagedorn
Harris
Harshbarger
Hartzler
Hern
Herrell
Herrera Beutler
Hice (GA)
Hill
Hinson
Hollingsworth
Hudson
Huizenga
Issa
Jackson
Jacobs (NY)
Johnson (LA)
Johnson (OH)
Johnson (SD)
Jordan
Joyce (OH)
Joyce (PA)
Katko
Keller
Kelly (MS)
Kelly (PA)
Kim (CA)
Kinzinger
Kustoff
LaHood
Lamborn
Latta
LaTurner
Letlow
Long
Loudermilk
Lucas
Luetkemeyer
Mace
Malliotakis
Mann
Massie
Mast
McCarthy
McCaul
McClain
McClintock
McHenry
McKinley
Meijer
Meuser
Miller (IL)
Miller (WV)
Miller-Meeks
Moolenaar
Mooney
Moore (AL)
Moore (UT)
Mullin
Murphy (NC)
Nehls
Newhouse
Norman
Nunes
Obernolte
Owens
Palazzo
Palmer
Pence
Perry
Pfluger
Posey
Reed
Reschenthaler
Rice (SC)
Rodgers (WA)
Rogers (AL)
Rogers (KY)
Rose
Rosendale
Rouzer
Roy
Rutherford
Salazar
Scalise
Schweikert
Sessions
Simpson
Smith (MO)
Smith (NE)
Smith (NJ)
Smucker
Spartz
Stauber
Steel
Stefanik
Steil
Steube
Stewart
Taylor
Tenney
Thompson (PA)
Tiffany
Timmons
Turner
Upton
Valadao
Van Drew
Van Duyne
Wagner
Walberg
Walorski
Waltz
Weber (TX)
Webster (FL)
Wenstrup
Westerman
Williams (TX)
Wilson (SC)
Wittman
Womack
Young
Zeldin

NOT VOTING—7

Costa
Crow
Gonzalez, Vicente
Higgins (LA)
LaMalfa
Lesko
Scott, Austin

□ 1537

Messrs. WESTERMAN and LAHOOD changed their vote from ''yea'' to ''nay.''

Ms. LOFGREN changed her vote from ''nay'' to ''yea.''

So the previous question was ordered.

The result of the vote was announced as above recorded.

MEMBERS RECORDED PURSUANT TO HOUSE RESOLUTION 8, 117TH CONGRESS

Aderholt (Moolenaar)
Buchanan (LaHood)
DeSaulnier (Matsui)
Doyle, Michael F. (Cartwright)
Frankel, Lois (Clark (MA))
Fulcher (Simpson)
García (IL) (Garcia (TX))
Gottheimer (Panetta)
Granger (Calvert)
Grijalva (Stanton)
Johnson (TX) (Jeffries)
Jones (Williams (GA))
Kahele (Moulton)
Kirkpatrick (Stanton)
Lawson (FL) (Evans)
McEachin (Wexton)
Meng (Jeffries)
Napolitano (Correa)
Payne (Pallone)
Ruiz (Correa)
Rush (Underwood)
Stewart (Owens)
Trone (Beyer)
Wilson (FL) (Hayes)

The SPEAKER pro tempore. The question is on the adoption of the resolution.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. BURGESS. Mr. Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

The vote was taken by electronic device, and there were—yeas 219, nays 208, not voting 3, as follows:

[Roll No. 211]

YEAS—219

Adams
Aguilar
Allred
Auchincloss
Axne
Barragán
Bass
Beatty
Bera
Beyer
Bishop (GA)
Blumenauer
Blunt Rochester
Bonamici
Bourdeaux
Bowman
Boyle, Brendan F.
Brown
Brownley
Bush
Bustos
Butterfield
Carbajal
Cárdenas
Carson
Carter (LA)
Cartwright
Case
Casten
Castor (FL)
Castro (TX)
Chu
Cicilline
Clark (MA)
Clarke (NY)
Cleaver
Clyburn
Cohen
Connolly
Cooper
Correa
Costa
Courtney
Craig
Crist
Crow
Cuellar
Davids (KS)
Davis, Danny K.
Dean
DeFazio
DeGette
DeLauro
DelBene
Delgado
Demings
DeSaulnier
Deutch
Dingell
Doggett
Doyle, Michael F.
Escobar
Eshoo
Espaillat
Evans
Fletcher
Foster
Frankel, Lois
Gallego
Garamendi
García (IL)
Garcia (TX)
Golden
Gomez
Gonzalez, Vicente
Gottheimer
Green, Al (TX)
Grijalva
Harder (CA)
Hayes
Higgins (NY)
Himes
Horsford
Houlahan
Hoyer
Huffman
Jackson Lee
Jacobs (CA)
Jayapal
Jeffries
Johnson (GA)
Johnson (TX)
Jones
Kahele
Kaptur
Keating
Kelly (IL)
Khanna
Kildee
Kilmer
Kim (NJ)
Kind
Kirkpatrick
Krishnamoorthi
Kuster
Lamb
Langevin
Larsen (WA)
Larson (CT)
Lawrence
Lawson (FL)
Lee (CA)
Lee (NV)
Leger Fernandez
Levin (CA)
Levin (MI)
Lieu
Lofgren
Lowenthal
Luria
Lynch
Malinowski
Maloney, Carolyn B.
Maloney, Sean
Manning
Matsui
McBath
McCollum
McEachin
McGovern
McNerney
Meeks
Meng
Mfume
Moore (WI)
Morelle
Moulton
Mrvan
Murphy (FL)
Nadler
Napolitano
Neal
Neguse
Newman
Norcross
O'Halleran
Ocasio-Cortez
Omar
Pallone
Panetta
Pappas
Pascrell
Payne
Perlmutter
Peters
Phillips
Pingree
Pocan
Porter
Pressley
Price (NC)
Quigley
Raskin
Rice (NY)
Ross
Roybal-Allard
Ruiz
Ruppersberger
Rush
Ryan
Sánchez
Sarbanes
Scanlon
Schakowsky
Schiff
Schneider
Schrader
Schrier
Scott (VA)
Scott, David
Sewell
Sherman
Sherrill
Sires
Slotkin
Smith (WA)
Soto
Spanberger
Speier
Stansbury
Stanton
Stevens
Strickland
Suozzi
Swalwell
Takano
Thompson (CA)
Thompson (MS)
Titus
Tlaib
Tonko
Torres (CA)
Torres (NY)
Trahan
Trone
Underwood
Vargas
Veasey
Vela
Velázquez
Wasserman Schultz
Waters
Watson Coleman
Welch
Wexton
Wild
Williams (GA)
Wilson (FL)
Yarmuth

NAYS—208

Aderholt
Allen
Amodei
Armstrong
Arrington
Babin
Bacon
Baird
Balderson
Banks
Barr
Bentz
Bergman
Bice (OK)
Biggs
Bilirakis
Bishop (NC)
Boebert
Bost
Brooks
Buchanan
Buck
Bucshon
Budd
Burchett
Burgess
Calvert
Cammack
Carl
Carter (GA)
Carter (TX)
Cawthorn
Chabot
Cheney
Cline
Cloud
Clyde
Cole
Comer
Crawford
Crenshaw
Curtis
Davidson
Davis, Rodney
DesJarlais
Diaz-Balart
Donalds
Duncan
Dunn
Emmer
Estes
Fallon
Feenstra
Ferguson
Fischbach
Fitzgerald
Fitzpatrick
Fleischmann
Fortenberry
Foxx
Franklin, C. Scott
Fulcher
Gaetz
Gallagher
Garbarino
Garcia (CA)
Gibbs
Gimenez
Gohmert
Gonzales, Tony
Gonzalez (OH)
Good (VA)
Gooden (TX)
Gosar
Granger
Graves (LA)
Graves (MO)
Green (TN)
Greene (GA)
Griffith
Grothman
Guest
Guthrie
Hagedorn
Harris
Harshbarger
Hartzler
Hern
Herrell
Herrera Beutler
Hice (GA)
Hill
Hinson
Hollingsworth
Hudson
Huizenga
Issa
Jackson
Jacobs (NY)
Johnson (LA)
Johnson (OH)
Johnson (SD)
Jordan
Joyce (OH)
Joyce (PA)
Katko
Keller
Kelly (MS)
Kelly (PA)
Kim (CA)
Kinzinger
Kustoff
LaHood
LaMalfa
Lamborn
Latta
LaTurner
Lesko
Letlow
Long
Loudermilk
Lucas
Luetkemeyer
Mace
Malliotakis
Mann
Massie
Mast
McCarthy
McCaul
McClain
McClintock
McHenry
McKinley
Meijer
Meuser
Miller (IL)
Miller (WV)
Miller-Meeks
Moolenaar
Mooney
Moore (AL)
Moore (UT)
Mullin
Murphy (NC)
Nehls
Newhouse
Norman
Nunes
Obernolte
Owens
Palazzo
Palmer
Pence
Perry
Pfluger
Posey
Reed
Reschenthaler
Rice (SC)
Rodgers (WA)
Rogers (AL)
Rogers (KY)
Rose
Rosendale
Rouzer
Roy
Rutherford
Salazar
Scalise
Schweikert
Sessions
Simpson
Smith (MO)
Smith (NE)
Smith (NJ)
Smucker
Spartz
Stauber
Steel
Stefanik
Steil
Steube
Stewart
Taylor
Tenney
Thompson (PA)
Tiffany
Timmons
Turner
Upton
Valadao
Van Drew
Van Duyne
Wagner
Walberg
Walorski
Waltz
Weber (TX)
Webster (FL)
Wenstrup
Westerman
Williams (TX)
Wilson (SC)
Wittman
Womack
Young
Zeldin

NOT VOTING—3

Brady
Higgins (LA)
Scott, Austin

□ 1600

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

MEMBERS RECORDED PURSUANT TO HOUSE RESOLUTION 8, 117TH CONGRESS

Aderholt (Moolenaar)
Buchanan (LaHood)
DeSaulnier (Matsui)
Doyle, Michael F. (Cartwright)
Frankel, Lois (Clark (MA))
Fulcher (Simpson)
García (IL) (Garcia (TX))
Gottheimer (Panetta)
Granger (Calvert)
Grijalva (Stanton)
Johnson (TX) (Jeffries)
Jones (Williams (GA))
Kahele (Moulton)
Kirkpatrick (Stanton)
Lawson (FL) (Evans)
McEachin (Wexton)
Meng (Jeffries)
Napolitano (Correa)
Payne (Pallone)
Ruiz (Correa)
Rush (Underwood)
Stewart (Owens)
Trone (Beyer)
Wilson (FL) (Hayes)

MOTION TO SUSPEND THE RULES AND PASS CERTAIN BILLS AND AGREE TO CERTAIN RESOLUTIONS

Mr. HOYER. Mr. Speaker, pursuant to section 7 of House Resolution 535, I move to suspend the rules and pass the bills: H.R. 678; H.R. 1036; H.R. 1079; H.R. 1158; H.R. 1250; H.R. 1754; H.R. 1833; H.R. 1850; H.R. 1871; H.R. 1877; H.R. 1893; H.R. 1895; H.R. 2118; H.R. 2795; H.R. 2928; H.R. 2980; H.R. 3003; H.R. 3138; H.R. 3223; H.R.

3263; and H.R. 3264, and agree to H. Res. 277; and H. Res. 294.

The Clerk read the title of the bills and the resolutions.

The text of the bills and the resolutions are as follows:

PRESERVING HOME AND OFFICE NUMBERS IN EMERGENCIES ACT OF 2021

H.R. 678

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 ''Preserving Home and Office Numbers in Emergencies Act of 2021'' or the ''PHONE Act of 2021''.

SEC. 2. MORATORIUM ON NUMBER REASSIGNMENT AFTER DISASTER DECLARATION.

(a) IN GENERAL.—Section 251(e) of the Communications Act of 1934 (47 U.S.C. 251(e)) is amended by adding at the end the following:

''(5) MORATORIUM ON NUMBER REASSIGNMENT AFTER DISASTER DECLARATION.—

''(A) IN GENERAL.—In the case of a number assigned to a subscriber for the provision of fixed wireline voice service at a location in a designated area during a covered period—

''(i) the number may not be reassigned, except at the request of the subscriber; and

''(ii) the assignment of the number may not be rescinded or otherwise modified, except at the request of the subscriber.

''(B) EXTENSION AT REQUEST OF SUBSCRIBER.—During the covered period, at the request of a subscriber described in subparagraph (A), the prohibition in subparagraph (A) shall be extended for the number for 1 year after the date on which the covered period expires.

''(C) SUBSCRIBER RIGHT TO CANCEL AND RESUBSCRIBE.—

''(i) IN GENERAL.—In the case of a number described under subparagraph (A) or (B), if the subscriber assigned to such number demonstrates to the provider of the service (or, under subclause (II), any other provider of fixed wireline voice service that serves the local area) that the residence where the number is located is inaccessible or uninhabitable—

''(I) the provider may not charge the subscriber an early termination or other fee in connection with the cancellation of such service, if cancelled during the covered period or the extension of the period described in subparagraph (B); and

''(II) if the subscriber cancels the service during the covered period or the extension of the period described in subparagraph (B), the provider (or any other provider of fixed wireline voice service that serves the local area)—

''(aa) shall permit the subscriber to subscribe or resubscribe, as the case may be, to fixed wireline voice service with the number at the residence or at a different residence (if such number is available in the location of such different residence); and

''(bb) may not charge the subscriber a connection fee or any other fee relating to the initiation of fixed wireline voice service.

''(ii) CANCELLATION WITHOUT DEMONSTRATION OF INACCESSIBILITY OR UNINHABITABILITY.—If a subscriber cancels the provision of service assigned to a number described in subparagraph (A) or (B) and does not demonstrate to the provider of such service that the residence where the number is located is inaccessible or uninhabitable as described under clause (i), the number is no longer subject to the prohibition under subparagraph (A) or (B).

''(D) IDENTIFICATION ON COMMISSION WEBSITE.—The Commission shall publicly identify on the website of the Commission each designated area that is in a covered period, not later than 15 days after the submission of a public designation by a State under subparagraph (E)(iii) with respect to such area. In identifying a designated area under subparagraph (E)(iii), a State shall consult with providers of fixed wireline voice service that serve such area and coordinate with the Federal Emergency Management Agency to reasonably limit the designated area to areas that have sustained covered damage.

''(E) DEFINITIONS.—In this paragraph:

''(i) COVERED DAMAGE.—The term 'covered damage' means, with respect to an area—

''(I) damage that renders residences in such area inaccessible or uninhabitable; or

''(II) damage that otherwise results in the displacement of subscribers from or within such area.

''(ii) COVERED PERIOD.—The term 'covered period' means a period that—

''(I) begins on the date of a declaration by the President of a major disaster under section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170) with respect to a designated area; and

''(II) ends on the date that is 1 year after such date.

''(iii) DESIGNATED AREA.—The term 'designated area' means a geographic area for which a State has submitted a public designation to the Commission, within 15 days after a declaration by the President of a major disaster under section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170) with respect to such area, stipulating that the State has determined that—

''(I) covered damage was sustained in such area; and

''(II) the prohibitions described in this paragraph are necessary and in the public interest.

''(iv) VOICE SERVICE.—The term 'voice service' has the meaning given the term 'voice service' in section 227(e)(8).''.

(b) AMENDMENT OF FCC RULES REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Federal Communications Commission shall amend its rules to reflect the requirements of paragraph (5) of section 251(e) of the Communications Act of 1934 (47 U.S.C. 251(e)), as added by subsection (a).

(c) APPLICABILITY.—Paragraph (5) of section 251(e) of the Communications Act of 1934 (47 U.S.C. 251(e)), as added by subsection (a), shall apply with respect to a major disaster declared by the President under section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170) after the date that is 180 days after the date on which the Commission announces that the Commission is capable of publicly identifying a designated area on the website of the Commission under subparagraph (D) of such paragraph (5).

(d) ORDER OF AMENDMENT EXECUTION.—If this Act is enacted before October 17, 2021, section 3(a) of the National Suicide Hotline Designation Act of 2020 (Public Law 116–172) is amended, effective on the date of the enactment of this Act, by striking ''adding at the end'' and inserting ''inserting after paragraph (3)'', so that the paragraph (4) that is to be added by such section to section 251(e) of the Communications Act of 1934 (47 U.S.C. 251(e)) appears after paragraph (3) of such section 251(e) and before the paragraph (5) added to such section 251(e) by subsection (a) of this section.

BASSAM BARABANDI REWARDS FOR JUSTICE ACT

H.R. 1036

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 ''Bassam Barabandi Rewards for Justice Act''.

SECTION 2. AMENDMENT TO DEPARTMENT OF STATE REWARDS PROGRAM.

Subsection (b) of section 36 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2708) is amended—

(1) in paragraph (11), by striking ''or'' after the semicolon at the end;

(2) in paragraph (12), by striking the period at the end and inserting ''; or''; and

(3) by adding at the end the following new paragraph.

''(13) the identification or location of an individual or entity that—

''(A) knowingly, directly or indirectly, imports, exports, or reexports to, into, or from any country any goods, services, or technology controlled for export by the United States because of the use of such goods, services, or technology in contravention of a United States or United Nations sanction; or

''(B) knowingly, directly or indirectly, provides training, advice, or other services or assistance, or engages in significant financial transactions, relating to any such goods, services, or technology in contravention of such sanction.''.

DESERT LOCUST CONTROL ACT

H.R. 1079

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 ''Desert Locust Control Act''.

SEC. 2. STATEMENT OF POLICY.

It is the policy of the United States to prioritize efforts to control the ongoing desert locust outbreak in East Africa and other affected regions, mitigate the impacts on food security, economic productivity, and political stability, improve interagency coordination to prevent future outbreaks, and promote resilience in affected countries.

SEC. 3. FINDINGS.

Congress finds the following:

(1) The United States Agency for International Development reports that countries in East Africa are currently suffering the worst desert locust outbreak in decades, which will devour crops and pasture and destroy local livelihoods across the region.

(2) As of December 2020, the Food and Agriculture Organization reported that there were 42 million people experiencing acute food insecurity in East Africa, which numbers are projected to increase if the desert locust outbreak is not controlled.

(3) The desert locust outbreak in East Africa, particularly in Kenya, Ethiopia, and Somalia, is negatively impacting food security, local livelihoods and economic productivity, and may threaten political stability in the region.

(4) Proactive investments now to control the desert locust outbreak could reduce the need for a much larger United States humanitarian response effort later, as well as support economic and political stability and build resilience in affected countries.

(5) In order to optimize the United States response to the desert locust outbreak, an interagency working group should be established to develop and implement a comprehensive, strategic plan to control the desert locust outbreak in East Africa and other affected regions, mitigate impacts on food security, economic productivity, and political stability and prevent future outbreaks.

SEC. 4. INTERAGENCY WORKING GROUP.

(a) ESTABLISHMENT.—The President shall establish an interagency working group to coordinate the United States response to the

ongoing desert locust outbreak in East Africa and other affected regions, including the development of a comprehensive, strategic plan to control the outbreak, mitigate the impacts on food security, economic productivity, and political stability, and prevent future outbreaks.

(b) MEMBERSHIP.—

(1) IN GENERAL.—The interagency working group shall be composed of the following:

(A) Two representatives from the United States Agency for International Development.

(B) One representative from each of the following:

(i) The United States Mission to the United Nations Agencies for Food and Agriculture.

(ii) The National Security Council.

(iii) The Department of State.

(iv) The Department of Defense.

(v) The Department of Agriculture.

(vi) Any other relevant Federal department or agency.

(2) CHAIR.—The President shall designate one of the representatives from the United States Agency for International Development described in paragraph (1)(A) to serve as chair of the interagency working group.

(c) DUTIES.—The interagency working group shall—

(1) assess the scope of the desert locust outbreak in East Africa and other affected regions, including its impact on food security, economic productivity, and political stability in affected countries;

(2) assess the impacts of restrictions relating to the coronavirus disease 2019 (commonly referred to as ''COVID–19'') pandemic on efforts to control the desert locust outbreak and mitigate its impacts and in exacerbating food insecurity;

(3) monitor the effectiveness of ongoing assistance efforts to control the desert locust outbreak and mitigate its impacts and identify gaps and opportunities for additional support to such programs;

(4) review the effectiveness of regional and multilateral efforts to control the desert locust outbreak and the coordination among relevant United States Government agencies, regional governments, and international organizations, including the World Food Programme and the United Nations Food and Agriculture Organization; and

(5) not later than 90 days after the establishment of the interagency working group under subsection (a), develop and submit to the President and the appropriate congressional committees a comprehensive, strategic plan to control the desert locust outbreak, including a description of efforts to—

(A) improve coordination among relevant United States Government agencies, regional governments, and international organizations, including the World Food Programme and the United Nations Food and Agriculture Organization;

(B) ensure delivery of necessary assets control the desert locust outbreak and humanitarian and development assistance to address and mitigate impacts to food security, economic productivity, and political stability; and

(C) to the extent practicable, prevent and mitigate future desert locust and other, similar destructive insect outbreaks (such as Fall Armyworm) in Africa and other parts of the world, which require a humanitarian response.

(d) INTERAGENCY WORKING GROUP SUPPORT.—The interagency working group shall continue to meet not less than semi-annually to facilitate implementation of the comprehensive, strategic plan required by subsection (c)(5).

(e) SUNSET.—This Act shall terminate on the date that is 2 years after the date of the enactment of this Act, or at such time as there is no longer an upsurge in the desert locust outbreak in East Africa, whichever occurs earlier.

(g) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives; and

(2) the Committee on Foreign Relations and the Committee on Appropriations of the Senate.

REFUGEE SANITATION FACILITY SAFETY ACT OF 2021

H.R. 1158

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 ''Refugee Sanitation Facility Safety Act of 2021''.

SEC. 2. SECURE ACCESS TO SANITATION FACILITIES FOR WOMEN AND GIRLS.

Subsection (a) of section 501 of the Foreign Relations Authorization Act, Fiscal Years 1994 and 1995 (22 U.S.C. 2601 note) is amended—

(1) by redesignating paragraphs (6) through (11) as paragraphs (7) through (12), respectively; and

(2) by inserting after paragraph (5) the following new paragraph:

''(6) the provision of safe and secure access to sanitation facilities, with a special emphasis on women, girls, and vulnerable populations.''.

EMERGENCY REPORTING ACT

H.R. 1250

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 ''Emergency Reporting Act''.

SEC. 2. REPORTS AFTER ACTIVATION OF DISASTER INFORMATION REPORTING SYSTEM; IMPROVEMENTS TO NETWORK OUTAGE REPORTING.

(a) REPORTS AFTER ACTIVATION OF DISASTER INFORMATION REPORTING SYSTEM.—

(1) PRELIMINARY REPORT.—

(A) IN GENERAL.—Not later than 6 weeks after the deactivation of the Disaster Information Reporting System with respect to an event for which the System was activated for at least 7 days, the Commission shall issue a preliminary report on, with respect to such event and to the extent known—

(i) the number and duration of any outages of—

(I) broadband internet access service;

(II) interconnected VoIP service;

(III) commercial mobile service; and

(IV) commercial mobile data service;

(ii) the approximate number of users or the amount of communications infrastructure potentially affected by an outage described in clause (i);

(iii) the number and duration of any outages at public safety answering points that prevent public safety answering points from receiving emergency calls and routing such calls to emergency service personnel; and

(iv) any additional information determined appropriate by the Commission.

(B) DEVELOPMENT OF REPORT.—The Commission shall develop the report required by subparagraph (A) using information collected by the Commission, including information collected by the Commission through the System.

(2) PUBLIC FIELD HEARINGS.—

(A) REQUIREMENT.—Not later than 8 months after the deactivation of the Disaster Information Reporting System with respect to an event for which the System was activated for at least 7 days, the Commission shall hold at least 1 public field hearing in the area affected by such event.

(B) INCLUSION OF CERTAIN INDIVIDUALS IN HEARINGS.—For each public field hearing held under subparagraph (A), the Commission shall consider including—

(i) representatives of State government, local government, or Indian Tribal governments in areas affected by such event;

(ii) residents of the areas affected by such event, or consumer advocates;

(iii) providers of communications services affected by such event;

(iv) faculty of institutions of higher education;

(v) representatives of other Federal agencies;

(vi) electric utility providers;

(vii) communications infrastructure companies; and

(viii) first responders, emergency managers, or 9–1–1 directors in areas affected by such event.

(3) FINAL REPORT.—Not later than 12 months after the deactivation of the Disaster Information Reporting System with respect to an event for which the System was activated for at least 7 days, the Commission shall issue a final report that includes, with respect to such event—

(A) the information described under paragraph (1)(A); and

(B) any recommendations of the Commission on how to improve the resiliency of affected communications or networks recovery efforts.

(4) DEVELOPMENT OF REPORTS.—In developing a report required under this subsection, the Commission shall consider information collected by the Commission, including information collected by the Commission through the System, and any public hearing described in paragraph (2) with respect to the applicable event.

(5) PUBLICATION.—The Commission shall publish each report, excluding information that is otherwise exempt from public disclosure under the rules of the Commission, issued under this subsection on the website of the Commission upon the issuance of such report.

(b) IMPROVEMENTS TO NETWORK OUTAGE REPORTING.—Not later than 1 year after the date of the enactment of this Act, the Commission shall conduct a proceeding and, after public notice and an opportunity for comment, adopt rules to—

(1) determine the circumstances under which to require service providers subject to the 9–1–1 regulations established under part 9 of title 47, Code of Federal Regulations, to submit a timely notification, (in an easily accessible format that facilities situational awareness) to public safety answering points regarding communications service disruptions within the assigned territories of such public safety answering points that prevent—

(A) the origination of 9–1–1 calls;

(B) the delivery of Automatic Location Information; or

(C) Automatic Number Identification;

(2) require such notifications to be made; and

(3) specify the appropriate timing of such notification.

(c) DEFINITIONS.—In this section:

(1) AUTOMATIC LOCATION INFORMATION; AUTOMATIC NUMBER IDENTIFICATION.—The terms ''Automatic Location Information'' and ''Automatic Number Identification'' have the meaning given those terms in section 9.3 of title 47, Code of Federal Regulations, or any successor regulation.

(2) BROADBAND INTERNET ACCESS SERVICE.—The term ''broadband internet access service'' has the meaning given such term in section 8.1(b) of title 47, Code of Federal Regulations, or any successor regulation.

(3) COMMERCIAL MOBILE SERVICE.—The term ''commercial mobile service'' has the meaning given such term in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d)).

(4) COMMERCIAL MOBILE DATA SERVICE.—The term ''commercial mobile data service'' has the meaning given such term in section 6001 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1401).

(5) COMMISSION.—The term ''Commission'' means the Federal Communications Commission.

(6) INDIAN TRIBAL GOVERNMENT; LOCAL GOVERNMENT.—The terms ''Indian Tribal government'' and ''Indian Tribal Government'' have the meaning given those terms in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121).

(7) INTERCONNECTED VOIP SERVICE.—The term ''interconnected VoIP service'' has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

(8) PUBLIC SAFETY ANSWERING POINT.—The term ''public safety answering point'' has the meaning given such term in section 222 of the Communications Act of 1934 (47 U.S.C. 222).

(9) STATE.—The term ''State'' has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

MEASURING THE ECONOMICS DRIVING INVESTMENTS AND ACCESS FOR DIVERSITY ACT OF 2021

H.R. 1754

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 ''Measuring the Economics Driving Investments and Access for Diversity Act of 2021'' or the ''MEDIA Diversity Act of 2021''.

SEC. 2. CONSIDERING MARKET ENTRY BARRIERS FOR SOCIALLY DISADVANTAGED INDIVIDUALS.

Section 13(d) of the Communications Act of 1934 (47 U.S.C. 163(d)) is amended by adding at the end the following:

''(4) CONSIDERING SOCIALLY DISADVANTAGED INDIVIDUALS.—In assessing the state of competition under subsection (b)(1) and regulatory barriers under subsection (b)(3), the Commission, with the input of the Office of Communications Business Opportunities of the Commission, shall consider market entry barriers for socially disadvantaged individuals in the communications marketplace in accordance with the national policy under section 257(b).''.

DHS INDUSTRIAL CONTROL SYSTEMS CAPABILITIES ENHANCEMENT ACT OF 2021

H.R. 1833

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 ''DHS Industrial Control Systems Capabilities Enhancement Act of 2021''.

SEC. 2. CAPABILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS.

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (e)(1)—

(A) in subparagraph (G), by striking ''and'' after the semicolon;

(B) in subparagraph (H), by inserting ''and'' after the semicolon; and

(C) by adding at the end the following new subparagraph:

''(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;''; and

(2) by adding at the end the following new subsection:

''(p) INDUSTRIAL CONTROL SYSTEMS.—The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

''(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

''(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

''(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;

''(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and

''(5) conduct such other efforts and assistance as the Secretary determines appropriate.''.

(b) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act and every six months thereafter during the subsequent 4-year period, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the industrial control systems capabilities of the Agency under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a).

(c) GAO REVIEW.—Not later than two years after the date of the enactment of this Act, the Comptroller General of the United States shall review implementation of the requirements of subsections (e)(1)(I) and (p) of section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by subsection (a), and submit to the Committee on Homeland Security in the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate a report containing findings and recommendations relating to such implementation. Such report shall include information on the following:

(1) Any interagency coordination challenges to the ability of the Director of the Cybersecurity and Infrastructure Agency of the Department of Homeland Security to lead Federal efforts to identify and mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(1) of such section.

(2) The degree to which the Agency has adequate capacity, expertise, and resources to carry out threat hunting and incident response capabilities to mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(2) of such section, as well as additional resources that would be needed to close any operational gaps in such capabilities.

(3) The extent to which industrial control system stakeholders sought cybersecurity technical assistance from the Agency pursuant to subsection (p)(3) of such section, and the utility and effectiveness of such technical assistance.

(4) The degree to which the Agency works with security researchers and other industrial control systems stakeholders, pursuant to subsection (p)(4) of such section, to provide vulnerability information to the industrial control systems community.

SUPPORTING RESEARCH AND DEVELOPMENT FOR FIRST RESPONDERS ACT

H.R. 1850

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 ''Supporting Research and Development for First Responders Act''.

SEC. 2. NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY.

(a) IN GENERAL.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

''SEC. 322. NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY.

''(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 308(c)(2). Such laboratory shall be used to test and evaluate emerging technologies and conduct research and development to assist emergency response providers in preparing for, and protecting against, threats of terrorism.

''(b) LABORATORY DESCRIBED.—The laboratory described in this subsection is the laboratory—

''(1) known, as of the date of the enactment of this section, as the National Urban Security Technology Laboratory; and

''(2) transferred to the Department pursuant to section 303(1)(E).

''(c) LABORATORY ACTIVITIES.—The National Urban Security Technology Laboratory shall—

''(1) conduct tests, evaluations, and assessments of current and emerging technologies, including, as appropriate, the cybersecurity of such technologies that can connect to the internet, for emergency response providers;

''(2) act as a technical advisor to emergency response providers; and

''(3) carry out other such activities as the Secretary determines appropriate.

''(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed as affecting in any manner the authorities or responsibilities of the Countering Weapons of Mass Destruction Office of the Department.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 321 the following new item:

''Sec. 322. National Urban Security Technology Laboratory.''.

TRANSPORTATION SECURITY TRANSPARENCY IMPROVEMENT ACT

H.R. 1871

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 ''Transportation Security Transparency Improvement Act''.

SEC. 2. SENSITIVE SECURITY INFORMATION; INTERNATIONAL AVIATION SECURITY.

(a) SENSITIVE SECURITY INFORMATION.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall—

(A) ensure clear and consistent designation of ''Sensitive Security Information'', including reasonable security justifications for such designation;

(B) develop and implement a schedule to regularly review and update, as necessary, TSA Sensitive Security Information Identification guidelines;

(C) develop a tracking mechanism for all Sensitive Security Information redaction and designation challenges;

(D) document justifications for changes in position regarding Sensitive Security Information redactions and designations, and make such changes accessible to TSA personnel for use with relevant stakeholders, including air carriers, airport operators, surface transportation operators, and State and local law enforcement, as necessary; and

(E) ensure that TSA personnel are adequately trained on appropriate designation policies.

(2) STAKEHOLDER OUTREACH.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall conduct outreach to relevant stakeholders described in paragraph (1)(D) that regularly are granted access to Sensitive Security Information to raise awareness of the TSA's policies and guidelines governing the designation and use of Sensitive Security Information.

(b) INTERNATIONAL AVIATION SECURITY.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall develop and implement guidelines with respect to last point of departure airports to—

(A) ensure the inclusion, as appropriate, of air carriers and other transportation security stakeholders in the development and implementation of security directives and emergency amendments;

(B) document input provided by air carriers and other transportation security stakeholders during the security directive and emergency amendment, development, and implementation processes;

(C) define a process, including time frames, and with the inclusion of feedback from air carriers and other transportation security stakeholders, for cancelling or incorporating security directives and emergency amendments into security programs;

(D) conduct engagement with foreign partners on the implementation of security directives and emergency amendments, as appropriate, including recognition if existing security measures at a last point of departure airport are found to provide commensurate security as intended by potential new security directives and emergency amendments; and

(E) ensure that new security directives and emergency amendments are focused on defined security outcomes.

(2) BRIEFING TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the guidelines described in paragraph (1).

(3) DECISIONS NOT SUBJECT TO JUDICIAL REVIEW.—Notwithstanding any other provision of law, any action of the Administrator of the Transportation Security Administration under paragraph (1) is not subject to judicial review.

SECURITY SCREENING DURING COVID–19 ACT

H.R. 1877

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 ''Security Screening During COVID–19 Act''.

SEC. 2. PLAN.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Administrator, in coordination with the Chief Medical Officer of the Department of Homeland Security, and in consultation with the Secretary of Health and Human Services and the Director of the Centers for Disease Control and Prevention, shall issue and commence implementing a plan to enhance, as appropriate, security operations at airports during the COVID–19 national emergency in order to reduce risk of the spread of the coronavirus at passenger screening checkpoints and among the TSA workforce.

(b) CONTENTS.—The plan required under subsection (a) shall include the following:

(1) An identification of best practices developed in response to the coronavirus among foreign governments, airports, and air carriers conducting aviation security screening operations, as well as among Federal agencies conducting similar security screening operations outside of airports, including in locations where the spread of the coronavirus has been successfully contained, that could be further integrated into the United States aviation security system.

(2) Specific operational changes to aviation security screening operations informed by the identification of best practices under paragraph (1) that could be implemented without degrading aviation security and a corresponding timeline and costs for implementing such changes.

(c) CONSIDERATIONS.—In carrying out the identification of best practices under subsection (b), the Administrator shall take into consideration the following:

(1) Aviation security screening procedures and practices in place at security screening locations, including procedures and practices implemented in response to the coronavirus.

(2) Volume and average wait times at each such security screening location.

(3) Public health measures already in place at each such security screening location.

(4) The feasibility and effectiveness of implementing similar procedures and practices in locations where such are not already in place.

(5) The feasibility and potential benefits to security, public health, and travel facilitation of continuing any procedures and practices implemented in response to the COVID–19 national emergency beyond the end of such emergency.

(d) CONSULTATION.—In developing the plan required under subsection (a), the Administrator shall consult with public and private stakeholders and the TSA workforce, including through the labor organization certified as the exclusive representative of full- and part-time non-supervisory TSA personnel carrying out screening functions under section 44901 of title 49, U.S. Code.

(e) SUBMISSION.—Upon issuance of the plan required under subsection (a), the Administrator shall submit the plan to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(f) IMPLEMENTATION.—The Administrator shall not be required to implement the plan required under subsection (a) upon the termination of the COVID–19 national emergency except to the extent the Administrator determines such implementation to be feasible and beneficial to security screening operations.

(g) GAO REVIEW.—Not later than one year after the commencement of implementation pursuant to subsection (e) of the plan required under subsection (a), the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a review of such implementation.

(h) DEFINITIONS.—In this section:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Transportation Security Administration.

(2) CORONAVIRUS.—The term ''coronavirus'' has the meaning given such term in section 506 of the Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020 (Public Law 116–123).

(3) COVID–19 NATIONAL EMERGENCY.—The term ''COVID–19 national emergency'' means the national emergency declared by the President under the National Emergencies Act (50 U.S.C. 1601 et seq.) on March 13, 2020, with respect to the coronavirus.

(4) PUBLIC AND PRIVATE STAKEHOLDERS.—The term ''public and private stakeholders'' has the meaning given such term in section 114(t)(1)(C) of title 49, United States Code.

(5) TSA.—The term ''TSA'' means the Transportation Security Administration.

TRANSPORTATION SECURITY PREPAREDNESS ACT OF 2021

H.R. 1893

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 ''Transportation Security Preparedness Act of 2021''.

SEC. 2. SURVEY OF THE TRANSPORTATION SECURITY ADMINISTRATION WORKFORCE REGARDING COVID–19 RESPONSE.

(a) SURVEY.—Not later than 1 year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (referred to in this section as the ''Administrator''), in consultation with the labor organization certified as the exclusive representative of full- and part-time non-supervisory Administration personnel carrying out screening functions under section 44901 of title 49, United States Code, shall conduct a survey of the Transportation Security Administration (referred to in this section as the ''Administration'') workforce regarding the Administration's response to the COVID–19 pandemic. Such survey shall be conducted in a manner that allows for the greatest practicable level of workforce participation.

(b) CONTENTS.—In conducting the survey required under subsection (a), the Administrator shall solicit feedback on the following:

(1) The Administration's communication and collaboration with the Administration's workforce regarding the Administration's response to the COVID–19 pandemic and efforts to mitigate and monitor transmission of COVID–19 among its workforce, including through—

(A) providing employees with personal protective equipment and mandating its use;

(B) modifying screening procedures and Administration operations to reduce transmission among officers and passengers and ensuring compliance with such changes;

(C) adjusting policies regarding scheduling, leave, and telework;

(D) outreach as a part of contact tracing when an employee has tested positive for COVID–19; and

(E) encouraging COVID–19 vaccinations and efforts to assist employees that seek to be vaccinated such as communicating the availability of duty time for travel to vaccination sites and recovery from vaccine side effects.

(2) Any other topic determined appropriate by the Administrator.

(c) REPORT.—Not later than 30 days after completing the survey required under subsection (a), the Administration shall provide a report summarizing the results of the survey to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

SEC. 3. TRANSPORTATION SECURITY PREPAREDNESS PLAN.

(a) PLAN REQUIRED.—Section 114 of title 49, United States Code, is amended by adding at the end the following new subsection:

''(x) TRANSPORTATION SECURITY PREPAREDNESS PLAN.—

''(1) IN GENERAL.—Not later than two years after the date of the enactment of this subsection, the Secretary of Homeland Security, acting through the Administrator, in coordination with the Chief Medical Officer of the Department of Homeland Security and in consultation with the partners identified under paragraphs (3)(A)(i) through (3)(A)(iv), shall develop a transportation security preparedness plan to address the event of a communicable disease outbreak. The Secretary, acting through the Administrator, shall ensure such plan aligns with relevant Federal plans and strategies for communicable disease outbreaks.

''(2) CONSIDERATIONS.—In developing the plan required under paragraph (1), the Secretary, acting through the Administrator, shall consider each of the following:

''(A) The findings of the survey required under section 2 of the Transportation Security Preparedness Act of 2021.

''(B) All relevant reports and recommendations regarding the Administration's response to the COVID–19 pandemic, including any reports and recommendations issued by the Comptroller General and the Inspector General of the Department of Homeland Security.

''(C) Lessons learned from Federal interagency efforts during the COVID–19 pandemic.

''(3) CONTENTS OF PLAN.—The plan developed under paragraph (1) shall include each of the following:

''(A) Plans for communicating and collaborating in the event of a communicable disease outbreak with the following partners:

''(i) Appropriate Federal departments and agencies, including the Department of Health and Human Services, the Centers for Disease Control and Prevention, the Department of Transportation, the Department of Labor, and appropriate interagency task forces.

''(ii) The workforce of the Administration, including through the labor organization certified as the exclusive representative of full- and part-time non-supervisory Administration personnel carrying out screening functions under section 44901 of this title.

''(iii) International partners, including the International Civil Aviation Organization and foreign governments, airports, and air carriers.

''(iv) Public and private stakeholders, as such term is defined under subsection (t)(1)(C).

''(v) The traveling public.

''(B) Plans for protecting the safety of the Transportation Security Administration workforce, including—

''(i) reducing the risk of communicable disease transmission at screening checkpoints and within the Administration's workforce related to the Administration's transportation security operations and mission;

''(ii) ensuring the safety and hygiene of screening checkpoints and other workstations;

''(iii) supporting equitable and appropriate access to relevant vaccines, prescriptions, and other medical care; and

''(iv) tracking rates of employee illness, recovery, and death.

''(C) Criteria for determining the conditions that may warrant the integration of additional actions in the aviation screening system in response to the communicable disease outbreak and a range of potential roles and responsibilities that align with such conditions.

''(D) Contingency plans for temporarily adjusting checkpoint operations to provide for passenger and employee safety while maintaining security during the communicable disease outbreak.

''(E) Provisions setting forth criteria for establishing an interagency task force or other standing engagement platform with other appropriate Federal departments and agencies, including the Department of Health and Human Services and the Department of Transportation, to address such communicable disease outbreak.

''(F) A description of scenarios in which the Administrator should consider exercising authorities provided under subsection (g) and for what purposes.

''(G) Considerations for assessing the appropriateness of issuing security directives and emergency amendments to regulated parties in various modes of transportation, including surface transportation, and plans for ensuring compliance with such measures.

''(H) A description of any potential obstacles, including funding constraints and limitations to authorities, that could restrict the ability of the Administration to respond appropriately to a communicable disease outbreak.

''(4) DISSEMINATION.—Upon development of the plan required under paragraph (1), the Administrator shall disseminate the plan to the partners identified under paragraph (3)(A) and to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

''(5) REVIEW OF PLAN.—Not later than two years after the date on which the plan is disseminated under paragraph (4), and biennially thereafter, the Secretary, acting through the Administrator and in coordination with the Chief Medical Officer of the Department of Homeland Security, shall review the plan and, after consultation with the partners identified under paragraphs (3)(A)(i) through (3)(A)(iv), update the plan as appropriate.''.

(b) COMPTROLLER GENERAL REPORT.—Not later than one year after the date on which the transportation security preparedness plan required under subsection (x) of section 114 of title 49, United States Code, as added by subsection (a), is disseminated under paragraph (4) of such subsection (x), the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report containing the results of a study assessing the transportation security preparedness plan, including an analysis of—

(1) whether such plan aligns with relevant Federal plans and strategies for communicable disease outbreaks; and

(2) the extent to which the Transportation Security Administration is prepared to implement the plan.

TRANSPORTATION SECURITY PUBLIC HEALTH THREAT PREPAREDNESS ACT OF 2021

H.R. 1895

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 ''Transportation Security Public Health Threat Preparedness Act of 2021''.

SEC. 2. DEFINITIONS.

For purposes of this Act:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Transportation Security Administration.

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

(A) the Committee on Homeland Security of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate.

(3) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(4) STERILE AREA.—The term ''sterile area'' has the meaning given such term in section 1540.5 of title 49, Code of Federal Regulations.

(5) TSA.—The term ''TSA'' means the Transportation Security Administration.

SEC. 3. AUTHORIZATION OF TSA PERSONNEL DETAILS.

(a) COORDINATION.—Pursuant to sections 106(m) and 114(m) of title 49, United States Code, the Administrator may provide TSA personnel, who are not engaged in front line transportation security efforts, to other components of the Department and other Federal agencies to improve coordination with such components and agencies to prepare for, protect against, and respond to public health threats to the transportation security system of the United States.

(b) BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Administrator shall brief the appropriate congressional committees regarding efforts to improve coordination with other components of the Department and other Federal agencies to prepare for, protect against, and respond to public health threats to the transportation security system of the United States.

SEC. 4. TSA PREPAREDNESS.

(a) ANALYSIS.—

(1) IN GENERAL.—The Administrator shall conduct an analysis of preparedness of the transportation security system of the United States for public health threats. Such analysis shall assess, at a minimum, the following:

(A) The risks of public health threats to the transportation security system of the United States, including to transportation hubs, transportation security stakeholders, TSA personnel, and passengers.

(B) Information sharing challenges among relevant components of the Department, other Federal agencies, international entities, and transportation security stakeholders.

(C) Impacts to TSA policies and procedures for securing the transportation security system.

(2) COORDINATION.—The analysis conducted of the risks described in paragraph (1)(A) shall be conducted in coordination with the Chief Medical Officer of the Department of Homeland Security, the Secretary of Health and Human Services, and transportation security stakeholders.

(b) BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Administrator shall brief the appropriate congressional committees on the following:

(1) The analysis required under subsection (a).

(2) Technologies necessary to combat public health threats at security screening checkpoints to better protect from future public health threats TSA personnel, passengers, aviation workers, and other personnel authorized to access the sterile area of an airport through such checkpoints, and

the estimated cost of technology investments needed to fully implement across the aviation system solutions to such threats.

(3) Policies and procedures implemented by TSA and transportation security stakeholders to protect from public health threats TSA personnel, passengers, aviation workers, and other personnel authorized to access the sterile area through the security screening checkpoints, as well as future plans for additional measures relating to such protection.

(4) The role of TSA in establishing priorities, developing solutions, and coordinating and sharing information with relevant domestic and international entities during a public health threat to the transportation security system, and how TSA can improve its leadership role in such areas.

SECURING AMERICA FROM EPIDEMICS ACT

H.R. 2118

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 ''Securing America From Epidemics Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Due to increasing population and population density, human mobility, and ecological change, emerging infectious diseases pose a real and growing threat to global health security.

(2) While vaccines can be the most effective tools to protect against infectious disease, the absence of vaccines for a new or emerging infectious disease with epidemic potential is a major health security threat globally, posing catastrophic potential human and economic costs.

(3) The COVID–19 pandemic has infected more than 119,960,700 individuals and has killed at least 2,656,822 people worldwide, and it is likely that unreported cases and deaths are significant.

(4) Even regional outbreaks can have enormous human costs and substantially disrupt the global economy and cripple regional economies. The 2014 Ebola outbreak in West Africa killed more than 11,000 and cost $2,800,000,000 in losses in the affected countries alone.

(5) While the need for vaccines to address emerging epidemic threats is acute, markets to drive the necessary development of vaccines to address them—a complex and expensive undertaking—are very often critically absent. Also absent are mechanisms to ensure access to those vaccines by those who need them when they need them.

(6) To address this global vulnerability and the deficit of political commitment, institutional capacity, and funding, in 2017, several countries and private partners launched the Coalition for Epidemic Preparedness Innovations (CEPI). CEPI's mission is to stimulate, finance, and coordinate development of vaccines for high-priority, epidemic-potential threats in cases where traditional markets do not exist or cannot create sufficient demand.

(7) Through funding of partnerships, CEPI seeks to bring priority vaccines candidates through the end of phase II clinical trials, as well as support vaccine platforms that can be rapidly deployed against emerging pathogens.

(8) CEPI supported the manufacturing of the United States-developed Moderna COVID–19 vaccine during its Phase 1 clinical trial, and CEPI has initiated at least 12 partnerships to develop vaccines against COVID–19.

(9) CEPI is co-leading COVAX, the vaccines pillar of the ACT–Accelerator, which is a global collaboration to quickly produce and equitably distribute safe and effective vaccines and therapeutics for COVID–19.

(10) Support for and participation in CEPI is an important part of the United States own health security and biodefense and is in the national interest, complementing the work of many Federal agencies and providing significant value through global partnership and burden-sharing.

SEC. 3. AUTHORIZATION FOR UNITED STATES PARTICIPATION.

(a) IN GENERAL.—The United States is hereby authorized to participate in the Coalition for Epidemic Preparedness Innovations (''Coalition'').

(b) DESIGNATION.—The President is authorized to designate an employee of the relevant Federal department or agency providing the majority of United States contributions to the Coalition, who should demonstrate knowledge and experience in the fields of development and public health, epidemiology, or medicine, to serve—

(1) on the Investors Council of the Coalition; and

(2) if nominated by the President, on the Board of Directors of the Coalition, as a representative of the United States.

(c) REPORTS TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the President shall submit to the appropriate congressional committees a report that includes the following:

(1) The United States planned contributions to the Coalition and the mechanisms for United States participation in such Coalition.

(2) The manner and extent to which the United States shall participate in the governance of the Coalition.

(3) How participation in the Coalition supports relevant United States Government strategies and programs in health security and biodefense, including—

(A) the Global Health Security Strategy required by section 7058(c)(3) of division K of the Consolidated Appropriations Act, 2018 (Public Law 115–141);

(B) the applicable revision of the National Biodefense Strategy required by section 1086 of the National Defense Authorization Act for Fiscal Year 2017 (6 U.S.C. 104); and

(C) any other relevant decision-making process for policy, planning, and spending in global health security, biodefense, or vaccine and medical countermeasures research and development.

(d) UNITED STATES CONTRIBUTIONS.—Amounts authorized to be appropriated under chapters 1 and 10 of part I and chapter 4 of part II of the Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.) are authorized to be made available for United States contributions to the Coalition.

(e) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives; and

(2) the Committee on Foreign Relations and the Committee on Appropriations of the Senate.

DHS BLUE CAMPAIGN ENHANCEMENT ACT

H.R. 2795

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 ''DHS Blue Campaign Enhancement Act''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY BLUE CAMPAIGN ENHANCEMENT.

Section 434 of the Homeland Security Act of 2002 (6 U.S.C. 242) is amended—

(1) in subsection (e)(6), by striking ''utilizing resources,'' and inserting ''developing and utilizing, in consultation with the Advisory Board established pursuant to subsection (g), resources''; and

(2) by adding at the end the following new subsections:

''(f) WEB-BASED TRAINING PROGRAMS.—To enhance training opportunities, the Director of the Blue Campaign shall develop web-based interactive training videos that utilize a learning management system to provide online training opportunities that shall be made available to the following individuals:

''(1) Federal, State, local, Tribal, and territorial law enforcement officers.

''(2) Non-Federal correction system personnel.

''(3) Such other individuals as the Director determines appropriate.

''(g) BLUE CAMPAIGN ADVISORY BOARD.—

''(1) IN GENERAL.—The Secretary shall establish within the Department a Blue Campaign Advisory Board and shall assign to such Board a representative from each of the following components:

''(A) The Transportation Security Administration.

''(B) U.S. Customs and Border Protection.

''(C) U.S. Immigration and Customs Enforcement.

''(D) The Federal Law Enforcement Training Center.

''(E) The United States Secret Service.

''(F) The Office for Civil Rights and Civil Liberties.

''(G) The Privacy Office.

''(H) Any other components or offices the Secretary determines appropriate.

''(2) CHARTER.—The Secretary is authorized to issue a charter for the Board, and such charter shall specify the following:

''(A) The Board's mission, goals, and scope of its activities.

''(B) The duties of the Board's representatives.

''(C) The frequency of the Board's meetings.

''(3) CONSULTATION.—The Director shall consult the Board established pursuant to paragraph (1) regarding the following:

''(A) Recruitment tactics used by human traffickers to inform the development of training and materials by the Blue Campaign.

''(B) The development of effective awareness tools for distribution to Federal and non-Federal officials to identify and prevent instances of human trafficking.

''(C) Identification of additional persons or entities that may be uniquely positioned to recognize signs of human trafficking and the development of materials for such persons.

''(4) APPLICABILITY.—The Federal Advisory Committee Act (5 U.S.C. App.) does not apply to—

''(A) the Board; or

''(B) consultations under paragraph (2).

''(h) CONSULTATION.—With regard to the development of programs under the Blue Campaign and the implementation of such programs, the Director is authorized to consult with State, local, Tribal, and territorial agencies, non-governmental organizations, private sector organizations, and experts. Such consultation shall be exempt from the Federal Advisory Committee Act (5 U.S.C. App.).''.

CYBER SENSE ACT OF 2021

H.R. 2928

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 ''Cyber Sense Act of 2021''.

SEC. 2. CYBER SENSE.

(a) IN GENERAL.—The Secretary of Energy, in coordination with relevant Federal agencies, shall establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)).

(b) PROGRAM REQUIREMENTS.—In carrying out subsection (a), the Secretary of Energy shall—

(1) establish a testing process under the Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, including products relating to industrial control systems and operational technologies, such as supervisory control and data acquisition systems;

(2) for products and technologies tested under the Cyber Sense program, establish and maintain cybersecurity vulnerability reporting processes and a related database;

(3) provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to develop solutions to mitigate identified cybersecurity vulnerabilities in products and technologies tested under the Cyber Sense program;

(4) biennially review products and technologies tested under the Cyber Sense program for cybersecurity vulnerabilities and provide analysis with respect to how such products and technologies respond to and mitigate cyber threats;

(5) develop guidance, that is informed by analysis and testing results under the Cyber Sense program, for electric utilities for procurement of products and technologies;

(6) provide reasonable notice to the public, and solicit comments from the public, prior to establishing or revising the testing process under the Cyber Sense program;

(7) oversee testing of products and technologies under the Cyber Sense program; and

(8) consider incentives to encourage the use of analysis and results of testing under the Cyber Sense program in the design of products and technologies for use in the bulk-power system.

(c) DISCLOSURE OF INFORMATION.—Any cybersecurity vulnerability reported pursuant to a process established under subsection (b)(2), the disclosure of which the Secretary of Energy reasonably foresees would cause harm to critical electric infrastructure (as defined in section 215A of the Federal Power Act), shall be deemed to be critical electric infrastructure information for purposes of section 215A(d) of the Federal Power Act.

(d) FEDERAL GOVERNMENT LIABILITY.—Nothing in this section shall be construed to authorize the commencement of an action against the United States Government with respect to the testing of a product or technology under the Cyber Sense program.

CYBERSECURITY VULNERABILITY REMEDIATION ACT

H.R. 2980

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity Vulnerability Remediation Act''.

SEC. 2. CYBERSECURITY VULNERABILITIES.

Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''and'' after the semicolon at the end;

(B) by redesignating paragraph (6) as paragraph (7); and

(C) by inserting after paragraph (5) the following new paragraph:

''(6) the term 'cybersecurity vulnerability' has the meaning given the term 'security vulnerability' in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and''.

(2) in subsection (c)—

(A) in paragraph (5)—

(i) in subparagraph (A), by striking ''and'' after the semicolon at the end;

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting after subparagraph (A) the following new subparagraph:

''(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and''; and

(iv) in subparagraph (C), as so redesignated, by inserting ''and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)'' before ''with Federal'';

(B) in paragraph (7)(C), by striking ''sharing'' and inserting ''share''; and

(C) in paragraph (9), by inserting ''mitigation protocols to counter cybersecurity vulnerabilities,'' after ''measures,'';

(3) in subsection (e)(1)(G), by striking the semicolon after ''and'' at the end;

(4) by redesignating subsection (o) as subsection (p); and

(5) by inserting after subsection (n) following new subsection:

''(o) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.''.

SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.

(a) REPORT.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how the Agency carries out subsection (n) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (o) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, that includes the following:

(1) A description of the policies and procedures relating to the coordination of vulnerability disclosures.

(2) A description of the levels of activity in furtherance of such subsections (n) and (o) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in such section 2209) between the Department and industry and other stakeholders.

(4) Any available information on the degree to which such information was acted upon by industry and other stakeholders.

(5) A description of how privacy and civil liberties are preserved in the collection, retention, use, and sharing of vulnerability disclosures.

(b) FORM.—The report required under subsection (b) shall be submitted in unclassified form but may contain a classified annex.

SEC. 4. COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES.

The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002, as amended by section 2) to information systems (as such term is defined in such section 2209) and industrial control systems, including supervisory control and data acquisition systems.

SEC. 5. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) TECHNICAL AMENDMENTS.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PROMOTING UNITED STATES WIRELESS LEADERSHIP ACT OF 2021

H.R. 3003

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 ''Promoting United States Wireless Leadership Act of 2021''.

SEC. 2. REPRESENTATION AND LEADERSHIP OF UNITED STATES IN COMMUNICATIONS STANDARDS-SETTING BODIES.

(a) IN GENERAL.—In order to enhance the representation of the United States and promote United States leadership in standards-setting bodies that set standards for 5G networks and for future generations of wireless communications networks, the Assistant Secretary shall, in consultation with the National Institute of Standards and Technology—

(1) equitably encourage participation by companies and a wide variety of relevant stakeholders, but not including any company or relevant stakeholder that the Assistant Secretary has determined to be not trusted, (to the extent such standards-setting bodies allow such stakeholders to participate) in such standards-setting bodies; and

(2) equitably offer technical expertise to companies and a wide variety of relevant stakeholders, but not including any company or relevant stakeholder that the Assistant Secretary has determined to be not trusted, (to the extent such standards-setting bodies allow such stakeholders to participate) to facilitate such participation.

(b) STANDARDS-SETTING BODIES.—The standards-setting bodies referred to in subsection (a) include—

(1) the International Organization for Standardization;

(2) the voluntary standards-setting bodies that develop protocols for wireless devices and other equipment, such as the 3GPP and the Institute of Electrical and Electronics Engineers; and

(3) any standards-setting body accredited by the American National Standards Institute or Alliance for Telecommunications Industry Solutions.

(c) BRIEFING.—Not later than 60 days after the date of the enactment of this Act, the Assistant Secretary shall brief the Committees on Energy and Commerce and Foreign Affairs of the House of Representatives and the Committees on Commerce, Science, and Transportation and Foreign Relations of the Senate on a strategy to carry out subsection (a).

(d) DEFINITIONS.—In this section:

(1) 3GPP.—The term ''3GPP'' means the 3rd Generation Partnership Project.

(2) 5G NETWORK.—The term ''5G network'' means a fifth-generation mobile network as described by 3GPP Release 15 or higher.

(3) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary of Commerce for Communications and Information.

(4) CLOUD COMPUTING.—The term ''cloud computing'' has the meaning given the term in Special Publication 800–145 of the National Institute of Standards and Technology, entitled ''The NIST Definition of Cloud Computing'', published in September 2011, or any successor publication.

(5) COMMUNICATIONS NETWORK.—The term ''communications network'' means any of the following:

(A) A system enabling the transmission, between or among points specified by the user, of information of the user's choosing.

(B) Cloud computing resources.

(C) A network or system used to access cloud computing resources.

(6) NOT TRUSTED.—The term ''not trusted'' means, with respect to a company or stakeholder, that the company or stakeholder is determined by the Assistant Secretary to pose a threat to the national security of the United States. In making such a determination, the Assistant Secretary shall rely solely on one or more of the following determinations:

(A) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code.

(B) A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain).

(C) Whether a company or stakeholder produces or provides covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918).

STATE AND LOCAL CYBERSECURITY IMPROVEMENT ACT

H.R. 3138

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 ''State and Local Cybersecurity Improvement Act''.

SEC. 2. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

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

''SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

''(a) DEFINITIONS.—In this section:

''(1) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(2) CYBERSECURITY PLAN.—The term 'Cybersecurity Plan' means a plan submitted by an eligible entity under subsection (e)(1).

''(3) ELIGIBLE ENTITY.—The term 'eligible entity' means—

''(A) a State; or

''(B) an Indian tribe that, not later than 120 days after the date of the enactment of this section or not later than 120 days before the start of any fiscal year in which a grant under this section is awarded—

''(i) notifies the Secretary that the Indian tribe intends to develop a Cybersecurity Plan; and

''(ii) agrees to forfeit any distribution under subsection (n)(2).

''(4) INCIDENT.—The term 'incident' has the meaning given the term in section 2209.

''(5) INDIAN TRIBE; TRIBAL ORGANIZATION.—The term 'Indian tribe' or 'Tribal organization' has the meaning given that term in section 4(e) of the of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(e)).

''(6) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'information sharing and analysis organization' has the meaning given the term in section 2222.

''(7) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(8) ONLINE SERVICE.—The term 'online service' means any internet-facing service, including a website, email, virtual private network, or custom application.

''(9) RANSOMWARE INCIDENT.—The term 'ransomware incident' means an incident that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system for the purpose of coercing the information system's owner, operator, or another person.

''(10) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term 'State and Local Cybersecurity Grant Program' means the program established under subsection (b).

''(11) STATE AND LOCAL CYBERSECURITY RESILIENCE COMMITTEE.—The term 'State and Local Cybersecurity Resilience Committee' means the committee established under subsection (o)(1).

''(b) ESTABLISHMENT.—

''(1) IN GENERAL.—The Secretary, acting through the Director, shall establish a program, to be known as the 'the State and Local Cybersecurity Grant Program', to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations.

''(2) APPLICATION.—An eligible entity seeking a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

''(c) BASELINE REQUIREMENTS.—An eligible entity or multistate group that receives a grant under this section shall use the grant in compliance with—

''(1)(A) the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group; and

''(B) the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments developed under section 2210(e)(1); or

''(2) activities carried out under paragraphs (3), (4), and (5) of subsection (h).

''(d) ADMINISTRATION.—The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 2003 and 2004.

''(e) CYBERSECURITY PLANS.—

''(1) IN GENERAL.—An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for approval.

''(2) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity shall—

''(A) incorporate, to the extent practicable, any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations;

''(B) describe, to the extent practicable, how the eligible entity will—

''(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

''(ii) monitor, audit, and track activity between information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and between those information systems and information systems not owned or operated by the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity;

''(iii) enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or local or Tribal organizations against cybersecurity risks and cybersecurity threats;

''(iv) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems of the eligible entity or local or Tribal organizations;

''(v) ensure that State, local, and Tribal organizations that own or operate information systems that are located within the jurisdiction of the eligible entity—

''(I) adopt best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by, and the cyber supply chain risk management best practices identified by, the National Institute of Standards and Technology; and

''(II) utilize knowledge bases of adversary tools and tactics to assess risk;

''(vi) promote the delivery of safe, recognizable, and trustworthy online services by State, local, and Tribal organizations, including through the use of the .gov internet domain;

''(vii) ensure continuity of operations of the eligible entity and local, and Tribal organizations in the event of a cybersecurity incident (including a ransomware incident), including by conducting exercises to practice responding to such an incident;

''(viii) use the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of State, local, or Tribal organizations, enhance recruitment and retention efforts for such workforces, and bolster the knowledge, skills, and abilities of State, local, and Tribal organization personnel to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

''(ix) ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity in the event of an incident involving such communications or data networks within the jurisdiction of the eligible entity;

''(x) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats related to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity;

''(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity, including by expanding existing information sharing agreements with the Department;

''(xii) enhance the capability of the eligible entity to share cyber threat indictors and related information with the Department;

''(xiii) leverage cybersecurity services offered by the Department;

''(xiv) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats to information systems of the eligible entity in consultation with—

''(I) local and Tribal organizations within the jurisdiction of the eligible entity; and

''(II) as applicable—

''(aa) States that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an information sharing and analysis organization; and

''(bb) countries that neighbor the jurisdiction of the eligible entity; and

''(xv) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

''(C) describe, to the extent practicable, the individual responsibilities of the eligible entity and local and Tribal organizations within the jurisdiction of the eligible entity in implementing the plan;

''(D) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

''(E) describe how the eligible entity will measure progress towards implementing the plan.

''(3) DISCRETIONARY ELEMENTS.—A Cybersecurity Plan of an eligible entity may include a description of—

''(A) cooperative programs developed by groups of local and Tribal organizations within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

''(B) programs provided by the eligible entity to support local and Tribal organizations and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

''(4) MANAGEMENT OF FUNDS.—An eligible entity applying for a grant under this section shall agree to designate the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity as the primary official for the management and allocation of funds awarded under this section.

''(f) MULTISTATE GRANTS.—

''(1) IN GENERAL.—The Secretary, acting through the Director, may award grants under this section to a group of two or more eligible entities to support multistate efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities.

''(2) SATISFACTION OF OTHER REQUIREMENTS.—In order to be eligible for a multistate grant under this subsection, each eligible entity that comprises a multistate group shall submit to the Secretary—

''(A) a Cybersecurity Plan for approval in accordance with subsection (i); and

''(B) a plan for establishing a cybersecurity planning committee under subsection (g).

''(3) APPLICATION.—

''(A) IN GENERAL.—A multistate group applying for a multistate grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

''(B) MULTISTATE PROJECT DESCRIPTION.—An application of a multistate group under subparagraph (A) shall include a plan describing—

''(i) the division of responsibilities among the eligible entities that comprise the multistate group for administering the grant for which application is being made;

''(ii) the distribution of funding from such a grant among the eligible entities that comprise the multistate group; and

''(iii) how the eligible entities that comprise the multistate group will work together to implement the Cybersecurity Plan of each of those eligible entities.

''(g) PLANNING COMMITTEES.—

''(1) IN GENERAL.—An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

''(A) assist in the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

''(B) approve the Cybersecurity Plan of the eligible entity; and

''(C) assist in the determination of effective funding priorities for a grant under this section in accordance with subsection (h).

''(2) COMPOSITION.—A committee of an eligible entity established under paragraph (1) shall—

''(A) be comprised of representatives from the eligible entity and counties, cities, towns, Tribes, and public educational and health institutions within the jurisdiction of the eligible entity; and

''(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

''(3) CYBERSECURITY EXPERTISE.—Not less than ½ of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

''(4) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this subsection may be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that meets, or may be leveraged to meet, the requirements of this subsection.

''(h) USE OF FUNDS.—An eligible entity that receives a grant under this section shall use the grant to—

''(1) implement the Cybersecurity Plan of the eligible entity;

''(2) develop or revise the Cybersecurity Plan of the eligible entity; or

''(3) assist with activities that address imminent cybersecurity risks or cybersecurity threats to the information systems of the eligible entity or a local or Tribal organization within the jurisdiction of the eligible entity.

''(i) APPROVAL OF PLANS.—

''(1) APPROVAL AS CONDITION OF GRANT.—Before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall review the Cybersecurity Plan, or any revisions thereto, of the eligible entity and approve such plan, or revised plan, if it satisfies the requirements specified in paragraph (2).

''(2) PLAN REQUIREMENTS.—In approving a Cybersecurity Plan of an eligible entity under this subsection, the Director shall ensure that the Cybersecurity Plan—

''(A) satisfies the requirements of subsection (e)(2);

''(B) upon the issuance of the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments authorized pursuant to section 2210(e), complies, as appropriate, with the goals and objectives of the strategy; and

''(C) has been approved by the cybersecurity planning committee of the eligible entity established under subsection (g).

''(3) APPROVAL OF REVISIONS.—The Secretary, acting through the Director, may approve revisions to a Cybersecurity Plan as the Director determines appropriate.

''(4) EXCEPTION.—Notwithstanding subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary if—

''(A) the eligible entity certifies to the Secretary that—

''(i) the activities that will be supported by the grant are integral to the development of the Cybersecurity Plan of the eligible entity; and

''(ii) the eligible entity will submit by September 30, 2023, to the Secretary a Cybersecurity Plan for review, and if appropriate, approval; or

''(B) the eligible entity certifies to the Secretary, and the Director confirms, that the eligible entity will use funds from the grant to assist with the activities described in subsection (h)(3).

''(j) LIMITATIONS ON USES OF FUNDS.—

''(1) IN GENERAL.—An eligible entity that receives a grant under this section may not use the grant—

''(A) to supplant State, local, or Tribal funds;

''(B) for any recipient cost-sharing contribution;

''(C) to pay a demand for ransom in an attempt to—

''(i) regain access to information or an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity; or

''(ii) prevent the disclosure of information that has been removed without authorization from an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity;

''(D) for recreational or social purposes; or

''(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity.

''(2) PENALTIES.—In addition to any other remedy available, the Secretary may take such actions as are necessary to ensure that a recipient of a grant under this section uses the grant for the purposes for which the grant is awarded.

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1) may be construed to prohibit the use of grant funds provided to a State, local, or Tribal organization for otherwise permissible uses under this section on the basis that a State, local, or Tribal organization has previously used State, local, or Tribal funds to support the same or similar uses.

''(k) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct defects, if any, in such applications before making final awards.

''(l) APPORTIONMENT.—For fiscal year 2022 and each fiscal year thereafter, the Secretary shall apportion amounts appropriated to carry out this section among States as follows:

''(1) BASELINE AMOUNT.—The Secretary shall first apportion 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the U.S. Virgin Islands, and 0.75 percent of such amounts to each of the remaining States.

''(2) REMAINDER.—The Secretary shall apportion the remainder of such amounts in the ratio that—

''(A) the population of each eligible entity, bears to

''(B) the population of all eligible entities.

''(3) MINIMUM ALLOCATION TO INDIAN TRIBES.—

''(A) IN GENERAL.—In apportioning amounts under this section, the Secretary shall ensure that, for each fiscal year, directly eligible Tribes collectively receive, from amounts appropriated under the State and Local Cybersecurity Grant Program, not less than an amount equal to three percent of the total amount appropriated for grants under this section.

''(B) ALLOCATION.—Of the amount reserved under subparagraph (A), funds shall be allocated in a manner determined by the Secretary in consultation with Indian tribes.

''(C) EXCEPTION.—This paragraph shall not apply in any fiscal year in which the Secretary—

''(i) receives fewer than five applications from Indian tribes; or

''(ii) does not approve at least two applications from Indian tribes.

''(m) FEDERAL SHARE.—

''(1) IN GENERAL.—The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

''(A) in the case of a grant to an eligible entity—

''(i) for fiscal year 2022, 90 percent;

''(ii) for fiscal year 2023, 80 percent;

''(iii) for fiscal year 2024, 70 percent;

''(iv) for fiscal year 2025, 60 percent; and

''(v) for fiscal year 2026 and each subsequent fiscal year, 50 percent; and

''(B) in the case of a grant to a multistate group—

''(i) for fiscal year 2022, 95 percent;

''(ii) for fiscal year 2023, 85 percent;

''(iii) for fiscal year 2024, 75 percent;

''(iv) for fiscal year 2025, 65 percent; and

''(v) for fiscal year 2026 and each subsequent fiscal year, 55 percent.

''(2) WAIVER.—The Secretary may waive or modify the requirements of paragraph (1) for an Indian tribe if the Secretary determines such a waiver is in the public interest.

''(n) RESPONSIBILITIES OF GRANTEES.—

''(1) CERTIFICATION.—Each eligible entity or multistate group that receives a grant under this section shall certify to the Secretary that the grant will be used—

''(A) for the purpose for which the grant is awarded; and

''(B) in compliance with, as the case may be—

''(i) the Cybersecurity Plan of the eligible entity;

''(ii) the Cybersecurity Plans of the eligible entities that comprise the multistate group; or

''(iii) a purpose approved by the Secretary under subsection (h) or pursuant to an exception under subsection (i).

''(2) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—Not later than 45 days after the date on which an eligible entity or multistate group receives a grant under this section, the eligible entity or multistate group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local and Tribal organizations within the jurisdiction of the eligible entity or the eligible entities that comprise the multistate group, and as applicable, consistent with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group—

''(A) not less than 80 percent of funds available under the grant;

''(B) with the consent of the local and Tribal organizations, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or

''(C) with the consent of the local and Tribal organizations, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

''(3) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—An eligible entity or multistate group shall certify to the Secretary that the eligible entity or multistate group has made the distribution to local, Tribal, and territorial governments required under paragraph (2).

''(4) EXTENSION OF PERIOD.—

''(A) IN GENERAL.—An eligible entity or multistate group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

''(B) APPROVAL.—The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity Grant Program.

''(5) EXCEPTION.—Paragraph (2) shall not apply to the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the Virgin Islands, or an Indian tribe.

''(6) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local or Tribal organization required in accordance with paragraph (2), the local or Tribal organization may petition the Secretary to request that grant funds be provided directly to the local or Tribal organization.

''(7) PENALTIES.—In addition to other remedies available to the Secretary, the Secretary may terminate or reduce the amount of a grant awarded under this section to an eligible entity or distribute grant funds previously awarded to such eligible entity directly to the appropriate local or Tribal organization as a replacement grant in an amount the Secretary determines appropriate if such eligible entity violates a requirement of this subsection.

''(o) ADVISORY COMMITTEE.—

''(1) ESTABLISHMENT.—Not later than 120 days after the date of enactment of this section, the Director shall establish a State and Local Cybersecurity Resilience Committee to provide State, local, and Tribal stakeholder expertise, situational awareness, and recommendations to the Director, as appropriate, regarding how to—

''(A) address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations; and

''(B) improve the ability of State, local, and Tribal organizations to prevent, protect against, respond to, mitigate, and recover from such cybersecurity risks and cybersecurity threats.

''(2) DUTIES.—The committee established under paragraph (1) shall—

''(A) submit to the Director recommendations that may inform guidance for applicants for grants under this section;

''(B) upon the request of the Director, provide to the Director technical assistance to inform the review of Cybersecurity Plans submitted by applicants for grants under this section, and, as appropriate, submit to the Director recommendations to improve those plans prior to the approval of the plans under subsection (i);

''(C) advise and provide to the Director input regarding the Homeland Security Strategy to Improve Cybersecurity for State, Local, Tribal, and Territorial Governments required under section 2210;

''(D) upon the request of the Director, provide to the Director recommendations, as appropriate, regarding how to—

''(i) address cybersecurity risks and cybersecurity threats on information systems of State, local, or Tribal organizations; and

''(ii) improve the cybersecurity resilience of State, local, or Tribal organizations; and

''(E) regularly coordinate with the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

''(3) MEMBERSHIP.—

''(A) NUMBER AND APPOINTMENT.—The State and Local Cybersecurity Resilience Committee established pursuant to paragraph (1)

shall be composed of 15 members appointed by the Director, as follows:

''(i) Two individuals recommended to the Director by the National Governors Association.

''(ii) Two individuals recommended to the Director by the National Association of State Chief Information Officers.

''(iii) One individual recommended to the Director by the National Guard Bureau.

''(iv) Two individuals recommended to the Director by the National Association of Counties.

''(v) One individual recommended to the Director by the National League of Cities.

''(vi) One individual recommended to the Director by the United States Conference of Mayors.

''(vii) One individual recommended to the Director by the Multi-State Information Sharing and Analysis Center.

''(viii) One individual recommended to the Director by the National Congress of American Indians.

''(viii) Four individuals who have educational and professional experience relating to cybersecurity work or cybersecurity policy.

''(B) TERMS.—

''(i) IN GENERAL.—Subject to clause (ii), each member of the State and Local Cybersecurity Resilience Committee shall be appointed for a term of two years.

''(ii) REQUIREMENT.—At least two members of the State and Local Cybersecurity Resilience Committee shall also be members of the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

''(iii) EXCEPTION.—A term of a member of the State and Local Cybersecurity Resilience Committee shall be three years if the member is appointed initially to the Committee upon the establishment of the Committee.

''(iv) TERM REMAINDERS.—Any member of the State and Local Cybersecurity Resilience Committee appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of such term. A member may serve after the expiration of such member's term until a successor has taken office.

''(v) VACANCIES.—A vacancy in the State and Local Cybersecurity Resilience Committee shall be filled in the manner in which the original appointment was made.

''(C) PAY.—Members of the State and Local Cybersecurity Resilience Committee shall serve without pay.

''(4) CHAIRPERSON; VICE CHAIRPERSON.—The members of the State and Local Cybersecurity Resilience Committee shall select a chairperson and vice chairperson from among members of the committee.

''(5) PERMANENT AUTHORITY.—Notwithstanding section 14 of the Federal Advisory Committee Act (5 U.S.C. App.), the State and Local Cybersecurity Resilience Committee shall be a permanent authority.

''(p) REPORTS.—

''(1) ANNUAL REPORTS BY GRANT RECIPIENTS.—

''(A) IN GENERAL.—Not later than one year after an eligible entity or multistate group receives funds under this section, the eligible entity or multistate group shall submit to the Secretary a report on the progress of the eligible entity or multistate group in implementing the Cybersecurity Plan of the eligible entity or Cybersecurity Plans of the eligible entities that comprise the multistate group, as the case may be.

''(B) ABSENCE OF PLAN.—Not later than 180 days after an eligible entity that does not have a Cybersecurity Plan receives funds under this section for developing its Cybersecurity Plan, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds during the fiscal year to—

''(i) so develop such a Cybersecurity Plan; or

''(ii) assist with the activities described in subsection (h)(3).

''(2) ANNUAL REPORTS TO CONGRESS.—Not less frequently than once per year, the Secretary, acting through the Director, shall submit to Congress a report on the use of grants awarded under this section and any progress made toward the following:

''(A) Achieving the objectives set forth in the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments, upon the date on which the strategy is issued under section 2210.

''(B) Developing, implementing, or revising Cybersecurity Plans.

''(C) Reducing cybersecurity risks and cybersecurity threats to information systems, applications, and user accounts owned or operated by or on behalf of State, local, and Tribal organizations as a result of the award of such grants.

''(q) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

''(1) for each of fiscal years 2022 through 2026, $500,000,000; and

''(2) for each subsequent fiscal year, such sums as may be necessary.

''SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOPMENT FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

''The Secretary, acting through the Director, shall develop, regularly update, and maintain a resource guide for use by State, local, Tribal, and territorial government officials, including law enforcement officers, to help such officials identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks (as such term is defined in section 2209), cybersecurity threats, and incidents (as such term is defined in section 2209).''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by section 4, is further amended by inserting after the item relating to section 2220 the following new items:

''Sec. 2220A. State and Local Cybersecurity Grant Program.

''Sec. 2220B. Cybersecurity resource guide development for State, local, Tribal, and territorial government officials.''.

SEC. 3. STRATEGY.

(a) HOMELAND SECURITY STRATEGY TO IMPROVE THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.—Section 2210 of the Homeland Security Act of 2002 (6 U.S.C. 660) is amended by adding at the end the following new subsection:

''(e) HOMELAND SECURITY STRATEGY TO IMPROVE THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.—

''(1) IN GENERAL.—

''(A) REQUIREMENT.—Not later than one year after the date of the enactment of this subsection, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, and other stakeholders, as appropriate, develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

''(B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy required under subparagraph (A) shall—

''(i) provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks (as such term is defined in section 2209), cybersecurity threats, and incidents (as such term is defined in section 2209); and

''(ii) establish baseline requirements for cybersecurity plans under this section and principles with which such plans shall align.

''(2) CONTENTS.—The strategy required under paragraph (1) shall—

''(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;

''(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—

''(i) incident exercises, information sharing and incident notification procedures;

''(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

''(iii) opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40, United States Code;

''(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(F) set short-term and long-term goals that will improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents; and

''(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

''(3) CONSIDERATIONS.—In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, and other stakeholders, as appropriate, shall consider—

''(A) lessons learned from incidents that have affected State, local, Tribal, and territorial governments, and exercises with Federal and non-Federal entities;

''(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

''(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems (as such term is defined in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)) owned or operated by State, local, Tribal, and territorial governments;

''(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies; and

''(E) recommendations made by the State and Local Cybersecurity Resilience Committee established under section 2220A.

''(4) EXEMPTION.—Chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), shall not apply to any action to implement this subsection.''.

(b) RESPONSIBILITIES OF THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—Section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

(1) by redesignating subsections (d) through (i) as subsections (e) through (j), respectively; and

(2) by inserting after subsection (c) the following new subsection:

''(d) ADDITIONAL RESPONSIBILITIES.—In addition to the responsibilities under subsection (c), the Director shall—

''(1) develop program guidance, in consultation with the State and Local Government Cybersecurity Resilience Committee established under section 2220A, for the State and Local Cybersecurity Grant Program under such section or any other homeland security assistance administered by the Department to improve cybersecurity;

''(2) review, in consultation with the State and Local Cybersecurity Resilience Committee, all cybersecurity plans of State, local, Tribal, and territorial governments developed pursuant to any homeland security assistance administered by the Department to improve cybersecurity;

''(3) provide expertise and technical assistance to State, local, Tribal, and territorial government officials with respect to cybersecurity; and

''(4) provide education, training, and capacity development to enhance the security and resilience of cybersecurity and infrastructure security.''.

(c) FEASIBILITY STUDY.—Not later than 270 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security of the Department of Homeland Security shall conduct a study to assess the feasibility of implementing a short-term rotational program for the detail to the Agency of approved State, local, Tribal, and territorial government employees in cyber workforce positions.

SEC. 4. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) TECHNICAL AMENDMENTS.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CISA CYBER EXERCISE ACT

H.R. 3223

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''CISA Cyber Exercise Act''.

SEC. 2. NATIONAL CYBER EXERCISE PROGRAM.

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

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

''(a) ESTABLISHMENT OF PROGRAM.—

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

''(2) REQUIREMENTS.—

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

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

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

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

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

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

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

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

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

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

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

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

''(b) DEFINITIONS.—In this section:

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

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

(b) TECHNICAL AMENDMENTS.—

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

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

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

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

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

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

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

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

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

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

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

and

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

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

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

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

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

DHS MEDICAL COUNTERMEASURES ACT

H.R. 3263

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 ''DHS Medical Countermeasures Act''.

SEC. 2. MEDICAL COUNTERMEASURES PROGRAM.

(a) IN GENERAL.—Subtitle C of title XIX of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) is amended by adding at the end the following new section:

"SEC. 1932. MEDICAL COUNTERMEASURES.

''(a) IN GENERAL.—The Secretary shall establish a medical countermeasures program to facilitate personnel readiness, and protection for the Department's employees and working animals in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic, and to support Department mission continuity.

''(b) OVERSIGHT.—The Chief Medical Officer of the Department shall provide programmatic oversight of the medical countermeasures program established pursuant to subsection (a), and shall—

''(1) develop Department-wide standards for medical countermeasure storage, security, dispensing, and documentation;

''(2) maintain a stockpile of medical countermeasures, including antibiotics, antivirals, and radiological countermeasures, as appropriate;

''(3) preposition appropriate medical countermeasures in strategic locations nationwide, based on threat and employee density, in accordance with applicable Federal statutes and regulations;

''(4) provide oversight and guidance regarding the dispensing of stockpiled medical countermeasures;

''(5) ensure rapid deployment and dispensing of medical countermeasures in a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic;

''(6) provide training to Department employees on medical countermeasure dispensing; and

''(7) support dispensing exercises.

''(c) MEDICAL COUNTERMEASURES WORKING GROUP.—The Chief Medical Officer shall establish a medical countermeasures working group comprised of representatives from appropriate components and offices of the Department to ensure that medical countermeasures standards are maintained and guidance is consistent.

''(d) MEDICAL COUNTERMEASURES MANAGEMENT.—Not later than 120 days after the date of the enactment of this section, the Chief Medical Officer shall develop and submit to the Secretary an integrated logistics support plan for medical countermeasures, including—

''(1) a methodology for determining the ideal types and quantities of medical countermeasures to stockpile and how frequently such methodology shall be reevaluated;

''(2) a replenishment plan; and

''(3) inventory tracking, reporting, and reconciliation procedures for existing stockpiles and new medical countermeasure purchases.

''(e) STOCKPILE ELEMENTS.—In determining the types and quantities of medical countermeasures to stockpile under subsection (d), the Chief Medical Officer shall utilize, if available—

''(1) Department chemical, biological, radiological, and nuclear risk assessments; and

''(2) Centers for Disease Control and Prevention guidance on medical countermeasures.

''(f) REPORT.—Not later than 180 days after the date of the enactment of this section, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the plan developed in accordance with subsection (d) and brief such Committees regarding implementing the requirements of this section.

''(g) DEFINITION.—In this section, the term 'medical countermeasures' means antibiotics, antivirals, radiological countermeasures, and other countermeasures that may be deployed to protect the Department's employees and working animals in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 1931 the following new item:

''Sec. 1932. Medical countermeasures.''.

DOMAINS CRITICAL TO HOMELAND SECURITY ACT

H.R. 3264

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Domains Critical to Homeland Security Act''.

SEC. 2. CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

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

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

''(a) IN GENERAL.—

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

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

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

''(2) REQUIREMENTS.—

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

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

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

''(iii) Influence of malign economic actors.

''(iv) Asset ownership.

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

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

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

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

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

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

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

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

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

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

''(3) CONSULTATION.—In conducting the research under paragraph (1) and subparagraph (B) of paragraph (2), the Secretary may consult with appropriate Federal agencies, State agencies, and private sector stakeholders.

''(4) PUBLICATION.—Beginning one year after the date of the enactment of this section, the Secretary shall publish a report containing information relating to the research under paragraph (1) and subparagraph (B) of paragraph (2), including findings, evidence, analysis, and recommendations. Such report shall be updated annually through 2026.

''(b) SUBMISSION TO CONGRESS.—Not later than 90 days after the publication of each report required under paragraph (4) of subsection (a), the Secretary shall transmit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate each such report, together with a description of actions the Secretary, in consultation with appropriate Federal agencies, will undertake or has undertaken in response to each such report.

''(c) DEFINITIONS.—In this section:

''(1) UNITED STATES CRITICAL DOMAINS FOR ECONOMIC SECURITY.—The term 'United States critical domains for economic security' means the critical infrastructure and other associated industries, technologies, and intellectual property, or any combination thereof, that are essential to the economic security of the United States.

''(2) ECONOMIC SECURITY.—The term 'economic security' means the condition of having secure and resilient domestic production capacity, combined with reliable access to the global resources necessary to maintain an acceptable standard of living and to protect core national values.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $1,000,000 for each of fiscal years 2022 through 2026 to carry out this section.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 890A the following new item:

''Sec. 890B. Homeland security critical domain research and development.''.

REAFFIRMING COMMITMENT TO MEDIA DIVERSITY

H. RES. 277

Whereas the principle that an informed and engaged electorate is critical to a vibrant democracy is deeply rooted in our laws of free speech and underpins the virtues on which we established our Constitution, ''in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity . . .'';

Whereas having independent, diverse, and local media that provide exposure to a broad range of viewpoints and the ability to contribute to the political debate is central to sustaining that informed engagement;

Whereas it is in the public interest to encourage source, content, and audience diversity on our Nation's shared telecommunications and media platforms;

Whereas the survival of small, independent, and diverse media outlets that serve diverse audiences and local media markets is essential to preserving local culture and building understanding on important community issues that impact the daily lives of residents;

Whereas research by the American Society of News Editors, the Radio Television Digital News Association, the Pew Research Center, and others has documented the continued challenges of increasing diversity among all types of media entities;

Whereas with increasing media experience and sophistication, it is even more important to have minority participation in local media to ensure a diverse range of information sources are available and different ideas and viewpoints are expressed to strengthen social cohesion among different communities; and

Whereas the constriction in small, independent, and diverse media outlets and limited participation of diverse populations in media ownership and decision making are combining to negatively impact our goal of increasing local civic engagement and civic knowledge through increased voter participation, membership in civic groups, and knowledge of local political and civil information: Now, therefore, be it

Resolved, That the House of Representatives—

(1) reaffirms its commitment to diversity as a core tenet of the public interest standard in media policy; and

(2) pledges to work with media entities and diverse stakeholders to develop common ground solutions to eliminate barriers to media diversity.

ENCOURAGING REUNIONS OF DIVIDED KOREAN-AMERICAN FAMILIES

H. RES. 294

Whereas the Korean Peninsula, with the Republic of Korea (in this resolution referred to as ''South Korea'') in the South and the Democratic People's Republic of Korea (in this resolution referred to as ''North Korea'') in the North, remains divided following the signing of the Korean War Armistice Agreement on July 27, 1953;

Whereas the division of the Korean Peninsula separated more than 10,000,000 Korean family members, including some who are now citizens of the United States;

Whereas there have been 21 rounds of family reunions between South Koreans and North Koreans along the border since 2000;

Whereas Congress signaled its support for family reunions between United States citizens and their relatives in North Korea in section 1265 of the National Defense Authorization Act for Fiscal Year 2008 (Public Law 110–181), signed into law by President George W. Bush on January 28, 2008;

Whereas most of the population of divided family members in the United States, initially estimated at 100,000 in 2001, has significantly dwindled as many of the individuals have passed away;

Whereas the summit between North Korea and South Korea on April 27, 2018, has prioritized family reunions;

Whereas the United States and North Korea have engaged in talks during 2 historic summits in June 2018 in Singapore and February 2019 in Hanoi; and

Whereas many Korean Americans are waiting for a chance to meet their relatives in North Korea for the first time in more than 60 years: Now, therefore, be it

Resolved, That the House of Representatives—

(1) calls on the United States and North Korea to begin the process of reuniting Korean-American divided family members with their immediate relatives through ways such as—

(A) identifying divided families in the United States and North Korea who are willing and able to participate in a pilot program for family reunions;

(B) finding matches for members of such families through organizations such as the Red Cross; and

(C) working with the Government of South Korea to include American citizens in inter-Korean video reunions;

(2) reaffirms the institution of family as inalienable and, accordingly, urges the restoration of contact between divided families physically, literarily, or virtually; and

(3) calls on the United States and North Korea to pursue reunions as a humanitarian priority of immediate concern.

The SPEAKER pro tempore. Pursuant to section 7 of House Resolution 535, the ordering of the yeas and nays on postponed motions to suspend the rules with respect to such measures is vacated to the end that all such motions are considered as withdrawn.

The question is on the motion offered by the gentleman from Maryland (Mr. HOYER) that the House suspend the rules and pass the bills and agree to the resolutions.

The question was taken.

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

Mr. ROSENDALE. Mr. Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

The vote was taken by electronic device, and there were—yeas 319, nays 105, not voting 6, as follows:

[Roll No. 212]

YEAS—319

Adams
Aguilar
Allred
Amodei
Auchincloss
Axne
Bacon
Baird
Barr
Barragán
Bass
Beatty
Bentz
Bera
Beyer
Bice (OK)
Bilirakis
Bishop (GA)
Blumenauer
Blunt Rochester
Bonamici
Bost
Bourdeaux
Bowman
Boyle, Brendan F.
Brown
Brownley
Buchanan
Bush
Bustos
Butterfield
Calvert
Cammack
Carbajal
Cárdenas
Carson
Carter (LA)
Cartwright
Case
Casten
Castor (FL)
Castro (TX)
Chabot
Cheney
Chu
Cicilline
Clark (MA)
Clarke (NY)
Cleaver
Clyburn
Cohen
Cole
Comer
Connolly
Cooper
Correa
Costa
Courtney
Craig
Crenshaw
Crist
Crow
Cuellar
Davids (KS)
Davis, Danny K.
Davis, Rodney
Dean
DeFazio
DeGette
DeLauro
DelBene
Delgado
Demings
DeSaulnier
Deutch
Diaz-Balart
Dingell
Doggett
Doyle, Michael F.
Emmer
Escobar
Eshoo
Espaillat
Evans
Feenstra
Fischbach
Fitzpatrick
Fletcher
Fortenberry
Foster
Frankel, Lois
Gallagher
Gallego
Garamendi
Garbarino
Garcia (CA)
García (IL)
Garcia (TX)
Gimenez
Golden
Gomez
Gonzales, Tony
Gonzalez (OH)
Gonzalez, Vicente
Gottheimer
Granger
Graves (LA)
Graves (MO)
Green, Al (TX)
Grijalva
Guest
Guthrie
Harder (CA)
Harshbarger
Hartzler
Hayes
Herrera Beutler
Higgins (NY)
Hill
Himes
Hollingsworth
Horsford
Houlahan
Hoyer
Hudson
Huffman
Jackson Lee
Jacobs (CA)
Jacobs (NY)
Jayapal
Jeffries
Johnson (GA)
Johnson (OH)
Johnson (SD)
Johnson (TX)
Jones
Joyce (OH)
Joyce (PA)
Kahele
Kaptur
Katko
Keating
Kelly (IL)
Kelly (PA)
Khanna
Kildee
Kilmer
Kim (CA)
Kim (NJ)
Kind
Kinzinger
Kirkpatrick
Krishnamoorthi
Kuster
Kustoff
LaHood
LaMalfa
Lamb
Langevin
Larsen (WA)
Larson (CT)
Latta
LaTurner
Lawrence
Lawson (FL)
Lee (CA)
Lee (NV)
Leger Fernandez
Letlow
Levin (CA)
Levin (MI)
Lieu
Lofgren
Long
Lowenthal
Lucas
Luetkemeyer
Luria
Lynch
Mace
Malinowski
Malliotakis
Maloney, Carolyn B.
Maloney, Sean
Manning
Matsui
McBath
McCarthy
McClain
McCollum
McEachin
McGovern
McHenry
McKinley
McNerney
Meeks
Meijer
Meng
Meuser
Mfume
Miller-Meeks
Moolenaar
Moore (WI)
Morelle
Moulton
Mrvan
Murphy (FL)
Nadler
Napolitano
Neal
Neguse
Newhouse
Newman
Norcross
Nunes
O'Halleran
Obernolte
Ocasio-Cortez
Omar
Pallone
Panetta
Pappas
Pascrell
Payne
Perlmutter
Peters
Phillips
Pingree
Pocan
Porter
Pressley
Price (NC)
Quigley
Raskin
Reed
Reschenthaler
Rice (NY)
Rodgers (WA)
Rogers (AL)
Rogers (KY)
Ross
Roybal-Allard
Ruiz
Ruppersberger
Rush
Ryan
Sánchez
Sarbanes
Scanlon
Schakowsky
Schiff
Schneider
Schrader
Schrier

Schweikert	Strickland	Vela
Scott (VA)	Suozzi	Velázquez
Scott, David	Swalwell	Wagner
Sewell	Takano	Walberg
Sherman	Tenney	Walorski
Sherrill	Thompson (CA)	Waltz
Simpson	Thompson (MS)	Wasserman Schultz
Sires	Thompson (PA)	Waters
Slotkin	Titus	Watson Coleman
Smith (NE)	Tlaib	Welch
Smith (NJ)	Tonko	Wenstrup
Smith (WA)	Torres (CA)	Wexton
Smucker	Torres (NY)	Wild
Soto	Trahan	Williams (GA)
Spanberger	Trone	Wilson (FL)
Spartz	Turner	Wilson (SC)
Speier	Underwood	Wittman
Stansbury	Upton	Womack
Stanton	Valadao	Yarmuth
Steel	Van Drew	Young
Stefanik	Vargas	Zeldin
Stevens	Veasey	

NAYS—105

Aderholt	Foxx	Mooney
Armstrong	Franklin, C. Scott	Moore (AL)
Arrington	Fulcher	Moore (UT)
Babin	Gaetz	Mullin
Balderson	Gibbs	Murphy (NC)
Banks	Gohmert	Nehls
Bergman	Good (VA)	Norman
Biggs	Gooden (TX)	Owens
Bishop (NC)	Gosar	Palazzo
Boebert	Green (TN)	Palmer
Brady	Greene (GA)	Pence
Brooks	Griffith	Perry
Buck	Grothman	Pfluger
Bucshon	Hagedorn	Posey
Budd	Harris	Rice (SC)
Burchett	Hern	Rose
Burgess	Herrell	Rosendale
Carl	Hice (GA)	Rouzer
Carter (GA)	Hinson	Roy
Carter (TX)	Huizenga	Rutherford
Cawthorn	Jackson	Scalise
Cline	Johnson (LA)	Sessions
Cloud	Jordan	Smith (MO)
Clyde	Keller	Steil
Crawford	Kelly (MS)	Steube
Curtis	Lamborn	Stewart
Davidson	Lesko	Taylor
DesJarlais	Loudermilk	Tiffany
Donalds	Mann	Timmons
Duncan	Massie	Van Duyne
Dunn	Mast	Weber (TX)
Estes	McCaul	Webster (FL)
Fallon	McClintock	Westerman
Ferguson	Miller (IL)	Williams (TX)
Fitzgerald	Miller (WV)	
Fleischmann		

NOT VOTING—6

Allen	Issa	Scott, Austin
Higgins (LA)	Salazar	Stauber

□ 1630

Mr. BALDERSON changed his vote from ''yea'' to ''nay.''

So (two-thirds being in the affirmative) the rules were suspended and the bills were passed and the resolutions were agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated against:

Mr. STAUBER. Mr. Speaker, had I been present, I would have voted "nay" on rollcall No. 212.

Mr. ALLEN. Mr. Speaker, had I been present, I would have voted "nay" on rollcall No. 212.

MEMBERS RECORDED PURSUANT TO HOUSE RESOLUTION 8, 117TH CONGRESS

Aderholt (Moolenaar)	Frankel, Lois (Clark (MA))	Granger (Calvert)
Buchanan (LaHood)	Fulcher (Simpson)	Grijalva (Stanton)
DeSaulnier (Matsui)	García (IL) (Garcia (TX))	Johnson (TX) (Jeffries)
Doyle, Michael F. (Cartwright)	Gottheimer (Panetta)	Jones (Williams (GA))
Kahele (Moulton)	Meng (Jeffries)	Stewart (Owens)
Kirkpatrick (Stanton)	Napolitano (Correa)	Trone (Beyer)
Lawson (FL) (Evans)	Payne (Pallone)	Wilson (FL) (Hayes)
McEachin (Wexton)	Ruiz (Correa)	
	Rush (Underwood)	

MESSAGE FROM THE PRESIDENT

A message in writing from the President of the United States was communicated to the House by Ms. Kaitlyn Roberts, one of his secretaries.

CONSUMER PROTECTION AND RECOVERY ACT

Mr. PALLONE. Mr. Speaker, pursuant to House Resolution 535, I call up the bill (H.R. 2668) to amend the Federal Trade Commission Act to affirmatively confirm the authority of the Federal Trade Commission to seek permanent injunctions and other equitable relief for violations of any provision of law enforced by the Commission, and ask for its immediate consideration in the House.

The Clerk read the title of the bill.

The SPEAKER pro tempore (Mr. CUELLAR). Pursuant to House Resolution 535, in lieu of the amendment in the nature of a substitute recommended by the Committee on Energy and Commerce printed in the bill, an amendment in the nature of a substitute consisting of the text of Rules Committee Print 117–11, is adopted and the bill, as amended, is considered read.

The text of the bill, as amended, is as follows:

H.R. 2668

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 ''Consumer Protection and Recovery Act''.

SEC. 2. FTC AUTHORITY TO SEEK PERMANENT INJUNCTIONS AND OTHER EQUITABLE RELIEF.

(a) PERMANENT INJUNCTIONS AND OTHER EQUITABLE RELIEF.—Section 13 of the Federal Trade Commission Act (15 U.S.C. 53) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by inserting ''has violated,'' after ''corporation'';

(B) in paragraph (2)—

(i) by striking ''that'' and inserting ''that either (A)''; and

(ii) by striking ''final,'' and inserting ''final; or (B) the permanent enjoining thereof or the ordering of equitable relief under subsection (e),''; and

(C) in the matter following paragraph (2)—

(i) by striking ''to enjoin any such act or practice'';

(ii) by striking ''Upon'' and inserting ''In a suit under paragraph (2)(A), upon'';

(iii) by striking ''without bond'';

(iv) by striking ''proper cases'' and inserting ''a suit under paragraph (2)(B)'';

(v) by striking ''injunction.'' and inserting ''injunction, equitable relief under subsection (e), or such other relief as the court determines to be just and proper, including temporary or preliminary equitable relief.'';

(vi) by striking ''Any suit'' and inserting ''Any suit under this subsection''; and

(vii) by striking ''In any suit under this section'' and inserting ''In any such suit''; and

(2) by adding at the end the following:

''(e) EQUITABLE RELIEF.—

''(1) RESTITUTION; CONTRACT RESCISSION AND REFORMATION; REFUNDS; RETURN OF PROPERTY.—In a suit brought under subsection (b)(2)(B), the Commission may seek, and the court may order, with respect to the violation that gives rise to the suit, restitution for losses, rescission or reformation of contracts, refund of money, or return of property.

''(2) DISGORGEMENT.—In a suit brought under subsection (b)(2)(B), the Commission may seek, and the court may order, disgorgement of any unjust enrichment that a person, partnership, or corporation obtained as a result of the violation that gives rise to the suit.

''(3) CALCULATION.—Any amount that a person, partnership, or corporation is ordered to pay under paragraph (2) with respect to a violation shall be offset by any amount such person, partnership, or corporation is ordered to pay, and the value of any property such person, partnership, or corporation is ordered to return, under paragraph (1) with respect to such violation.

''(4) LIMITATIONS PERIOD.—

''(A) IN GENERAL.—A court may not order equitable relief under this subsection with respect to any violation occurring before the period that begins on the date that is 10 years before the date on which the Commission files the suit in which such relief is sought.

''(B) CALCULATION.—For purposes of calculating the beginning of the period described in subparagraph (A), any time during which an individual against which the equitable relief is sought is outside of the United States shall not be counted.''.

(b) CONFORMING AMENDMENT.—Section 16(a)(2)(A) of the Federal Trade Commission Act (15 U.S.C. 56(a)(2)(A)) is amended by striking ''(relating to injunctive relief)''.

(c) APPLICABILITY.—The amendments made by this section shall apply with respect to any action or proceeding that is pending on, or commenced on or after, the date of the enactment of this Act.

The SPEAKER pro tempore. The bill, as amended, shall be debatable for 1 hour equally divided and controlled by the chair and ranking minority member of the Committee on Energy and Commerce or their respective designees.

The gentleman from New Jersey (Mr. PALLONE) and the gentleman from Florida (Mr. BILIRAKIS) each will control 30 minutes.

The Chair recognizes the gentleman from New Jersey.

GENERAL LEAVE

Mr. PALLONE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 2668.

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

There was no objection.

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

Mr. Speaker, I rise in strong support of H.R. 2668, the Consumer Protection and Recovery Act.

This legislation is essential to protect consumers and honest businesses across the country. It restores a critical tool of the Federal Trade Commission to go to court to get victimized consumers their money back and make lawbreakers return their illegal profits. The tool is section 13(b) of the Federal Trade Commission Act.