I then held a second press conference on February 24th to continue efforts to raise public knowledge of the impending threat.

On February 26th, I wrote the Chair and Ranking Member of the Committee on Homeland Security requesting to be briefed by Acting Secretary of Homeland Security Chad Wolf regarding the preparedness of the Department of Homeland Security to address a possible pandemic.

On March 19th, I announced an innovative partnership with United Methodist Medical Center (UMMC) to open the first drive-through Coronavirus Test Screening facility in the Greater Houston area, which proved beneficial to everyone in the Greater Houston area, as with UMMC's help we have opened multiple that are located within high-risk communities in the Greater Houston area, to reduce the need for travel to get access to COVID–19 testing.

Since the start of this pandemic, I have sought to proactively addressing the critical issues and concerns tied to the COVID–19 virus.

As I stated at the beginning of this pandemic, We must not panic, but prepare.''

I am pleased to see that this bill is not a panic-induced response, but a well-though-out proposal to further protect our citizens.

The COVID–19 pandemic revealed a number of challenges for public health information systems, but worst among them is the limited capacity of existing state Immunization Information Systems.

The importance of these systems cannot be understated: they allow providers to keep vaccines and supplies in stock, prevent over—or under—vaccination, remind patients when they are due for a recommended vaccine, and identify areas with low vaccination rates to ensure equitable distribution of vaccines.

However, states lack modern, comprehensive information systems that can meet the challenges of COVID–19 and future public health threats through the secure exchange of real-time immunization data.

Consequently, many state systems struggled to accommodate additional demand, implement new functionalities, onboard immunization providers, support interoperable exchange with health care partners and enable timely reporting of immunization data to federal partners.

These issues are exactly what this legislation seeks to address.

Through H.R. 550, HHS will develop a strategy and a plan to improve immunization information system and designate data and technology standards for use in these systems.

Additionally, HHS will award grants to health departments and other government agencies to improve their systems contingent upon meeting designated standards.

As the vaccine rollout continues and the time for boosters is upon us, immunization data systems will be a critical tool in the success of these efforts, and they are in need of modernization.

That is why I rise in ardent support of H.R. 550, and that is why the bill has strong bipartisan backing.

Lastly, I want to thank Congresswoman KUSTER and Congressman BUCSHON for introducing and shepherding this bill.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. PALLONE) that the House suspend the rules and pass the bill, H.R. 550, as amended.

The question was taken.

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

Mr. ROY. 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.

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

## UNDERSTANDING CYBERSECURITY OF MOBILE NETWORKS ACT

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2685) to direct the Assistant Secretary of Commerce for Communications and Information to submit to Congress a report examining the cybersecurity of mobile service networks, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2685

*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 ''Understanding Cybersecurity of Mobile Networks Act''.

**SEC. 2. REPORT ON CYBERSECURITY OF MOBILE SERVICE NETWORKS.**

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Assistant Secretary, in consultation with the Department of Homeland Security, shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report examining the cybersecurity of mobile service networks and the vulnerability of such networks and mobile devices to cyberattacks and surveillance conducted by adversaries.

(b) MATTERS TO BE INCLUDED.—The report required by subsection (a) shall include the following:

(1) An assessment of the degree to which providers of mobile service have addressed, are addressing, or have not addressed cybersecurity vulnerabilities (including vulnerabilities the exploitation of which could lead to surveillance conducted by adversaries) identified by academic and independent researchers, multistakeholder standards and technical organizations, industry experts, and Federal agencies, including in relevant reports of—

(A) the National Telecommunications and Information Administration;

(B) the National Institute of Standards and Technology; and

(C) the Department of Homeland Security, including—

(i) the Cybersecurity and Infrastructure Security Agency; and

(ii) the Science and Technology Directorate.

(2) A discussion of—

(A) the degree to which customers (including consumers, companies, and government agencies) consider cybersecurity as a factor when considering the purchase of mobile service and mobile devices; and

(B) the commercial availability of tools, frameworks, best practices, and other resources for enabling such customers to evaluate cybersecurity risk and price tradeoffs.

(3) A discussion of the degree to which providers of mobile service have implemented cybersecurity best practices and risk assessment frameworks.

(4) An estimate and discussion of the prevalence and efficacy of encryption and authentication algorithms and techniques used in each of the following:

(A) Mobile service.

(B) Mobile communications equipment or services.

(C) Commonly used mobile phones and other mobile devices.

(D) Commonly used mobile operating systems and communications software and applications.

(5) A discussion of the barriers for providers of mobile service to adopt more efficacious encryption and authentication algorithms and techniques and to prohibit the use of older encryption and authentication algorithms and techniques with established vulnerabilities in mobile service, mobile communications equipment or services, and mobile phones and other mobile devices.

(6) An estimate and discussion of the prevalence, usage, and availability of technologies that authenticate legitimate mobile service and mobile communications equipment or services to which mobile phones and other mobile devices are connected.

(7) An estimate and discussion of the prevalence, costs, commercial availability, and usage by adversaries in the United States of cell site simulators (often known as international mobile subscriber identity-catchers) and other mobile service surveillance and interception technologies.

(c) CONSULTATION.—In preparing the report required by subsection (a), the Assistant Secretary shall, to the degree practicable, consult with—

(1) the Federal Communications Commission;

(2) the National Institute of Standards and Technology;

(3) the intelligence community;

(4) the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security;

(5) the Science and Technology Directorate of the Department of Homeland Security;

(6) academic and independent researchers with expertise in privacy, encryption, cybersecurity, and network threats;

(7) participants in multistakeholder standards and technical organizations (including the 3rd Generation Partnership Project and the Internet Engineering Task Force);

(8) international stakeholders, in coordination with the Department of State as appropriate;

(9) providers of mobile service, including small providers (or the representatives of such providers) and rural providers (or the representatives of such providers);

(10) manufacturers, operators, and providers of mobile communications equipment or services and mobile phones and other mobile devices;

(11) developers of mobile operating systems and communications software and applications; and

(12) other experts that the Assistant Secretary considers appropriate.

(d) SCOPE OF REPORT.—The Assistant Secretary shall—

(1) limit the report required by subsection (a) to mobile service networks;

(2) exclude consideration of 5G protocols and networks in the report required by subsection (a);

(3) limit the assessment required by subsection (b)(1) to vulnerabilities that have been shown to be—

(A) exploited in non-laboratory settings; or

(B) feasibly and practicably exploitable in real-world conditions; and

(4) consider in the report required by subsection (a) vulnerabilities that have been effectively mitigated by manufacturers of mobile phones and other mobile devices.

(e) FORM OF REPORT.—

(1) CLASSIFIED INFORMATION.—The report required by subsection (a) shall be produced in unclassified form but may contain a classified annex.

(2) POTENTIALLY EXPLOITABLE UNCLASSIFIED INFORMATION.—The Assistant Secretary shall redact potentially exploitable unclassified information from the report required by subsection (a) but shall provide an unredacted form of the report to the committees described in such subsection.

(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $500,000 for fiscal year 2022. Such amount is authorized to remain available through fiscal year 2023.

(g) DEFINITIONS.—In this section:

(1) ADVERSARY.—The term ''adversary'' includes—

(A) any unauthorized hacker or other intruder into a mobile service network; and

(B) any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.

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

(3) ENTITY.—The term ''entity'' means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(4) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(5) MOBILE COMMUNICATIONS EQUIPMENT OR SERVICE.—The term ''mobile communications equipment or service'' means any equipment or service that is essential to the provision of mobile service.

(6) MOBILE SERVICE.—The term ''mobile service'' means, to the extent provided to United States customers, either or both of the following services:

(A) Commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))).

(B) Commercial mobile data service (as defined in section 6001 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1401)).

(7) PERSON.—The term ''person'' means an individual or entity.

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) an individual who is a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

(C) any person in the United States.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Ohio (Mr. LATTA) each will control 20 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. 2685.

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. 2685, the Understanding Cybersecurity of Mobile Networks Act.

There is no shortage of concerning headlines about cybersecurity attacks on our critical infrastructure, including our communications networks. The reports range anywhere from a hacker looking for users' personal information to sophisticated intelligence gathering on U.S. officials by foreign adversaries.

The severe nature of these attacks coupled with the important information carried across wireless networks demands our attention. We must be vigilant in ensuring our networks are as secure as possible. That is the goal of H.R. 2685, the Understanding Cybersecurity of Mobile Networks Act. It will help us gain additional data and insights from experts to determine what more we can do to make that happen.

Specifically, Mr. Speaker, the legislation requires the Assistant Secretary of Commerce for Communications and Information to lead a study with the Department of Homeland Security. This study will examine the cybersecurity of mobile service networks and the vulnerability of those networks and mobile devices to cyberattacks and surveillance by adversaries. It not only includes an assessment of what providers are doing to keep their networks secure, but also an examination of consumer expectations with respect to network security.

I am proud of the bipartisan work that the Energy and Commerce Committee has undertaken over the past several years to secure our communication networks. This is another important step toward that effort, and I applaud Representatives ESHOO and KINZINGER for their leadership on this bill.

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

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

Mr. Speaker, I rise today in support of H.R. 2685, the Understanding Cybersecurity of Mobile Networks Act, which was introduced by Representatives ESHOO and KINZINGER.

Congress tasked the National Telecommunications and Information Administration with ensuring the national security of our Nation's telecommunications networks. In recent years we have seen large scale cybersecurity attacks that put Americans at risk.

□ 1600

While mobile service providers take numerous steps to address vulnerabilities in their networks and respond to threats, we know that threats to our mobile networks continue to exist.

The Energy and Commerce Committee has focused on securing our communications supply chains, and today we are taking another step forward to understanding these challenges. This legislation requires NTIA to study the cybersecurity of mobile networks and the vulnerabilities of these networks and mobile devices to cyberattacks and surveillance conducted by our adversaries.

This report will not only help inform NTIA's cybersecurity activities, including its work on the Communications Supply Chain Risk Information Sharing Program, but will also help providers understand the risks their networks face so they can respond appropriately.

Mr. Speaker, I want to thank the majority for working with us on this legislation. I urge my colleagues to support H.R. 2685, and I yield back the balance of my time.

Mr. PALLONE. Mr. Speaker, I urge support for this legislation, and I yield back the balance of my time.

Ms. ESHOO. Mr. Speaker, I rise in strong support of H.R. 2685, the Understanding Cybersecurity of Mobile Networks Act, bipartisan legislation I'm proud to have authored.

While all of us are inundated by advertisements for 5G, nearly all of our calls, texts, and mobile data traverse through 2G, 3G, and 4G networks today. We're moving toward a 5G world, but for the foreseeable future these older networks will handle most of our wireless communications.

Since cellphones became common in the 1990s, government agencies, academics, think tanks, industry associations, and independent researchers have discovered various cybersecurity vulnerabilities in our wireless networks. Wireless network companies, mobile devices manufacturers, and other companies have responded to many of these vulnerabilities, but recent cybersecurity developments depict that vulnerabilities continue to exit in mobile cybersecurity. For example, Stingray's cell site simulators continue to intercept calls, texts, and mobile data of unwitting victims; SIM swaps are increasing as a means of identity fraud; and mobile spyware made by NSO Group and others has threatened the safety of journalists, activists, dissidents, and government officials around the globe. In each of these instances companies have taken certain actions to mitigate threats, but we lack a sophisticated, comprehensive, and independent assessment of what vulnerabilities persist, what issues have been resolved, and where mobile cybersecurity policymaking should be focused.

H.R 2685 solves this lack of information. The legislation requires the National Telecommunications and Information Administration (NTIA), in coordination with the Department of Homeland Security (DHS), to conduct a comprehensive study on the cybersecurity vulnerabilities of our 2G, 3G, and 4G networks.

Specifically, the study will include an assessment of responses to known vulnerabilities and deployment of best practices; an estimate of the prevalence of effective encryption and authentication techniques,

along with a discussion of barriers to adopting more efficacious techniques; a discussion of the prevalence, costs, availability, and usage of cell site simulators and other surveillance and interception technologies.

In addition to coordinating with DHS, the NTIA is required to consult the various federal agencies with relevant expertise, academic and independent researchers, multistakeholder and international organizations, and industry groups. While the report will be public, it will include a classified annex so details about vulnerabilities that could aid our adversaries are not publicized.

I first introduced the Understanding Cybersecurity of Mobile Networks Act last Congress with Rep. ADAM KINZINGER, and I thank him for his continued partnership on the legislation, and I thank Communications and Technology Subcommittee Chairman DOYLE and Ranking Member LATTA and the Energy and Commerce Committee Chairman PALLONE and Ranking Member RODGERS, for their support of this legislation

I ask my colleagues to support the passage of H.R. 2685

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. PALLONE) that the House suspend the rules and pass the bill, H.R. 2685, as amended.

The question was taken.

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

Mr. ROY. 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.

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

## FUTURE USES OF TECHNOLOGY UPHOLDING RELIABLE AND ENHANCED NETWORKS ACT

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4045) to direct the Federal Communications Commission to establish a task force to be known as the ''6G Task Force'', and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4045

*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 ''Future Uses of Technology Upholding Reliable and Enhanced Networks Act'' or the ''FUTURE Networks Act''.*

***SEC. 2. 6G TASK FORCE.***

*(a) ESTABLISHMENT.—Not later than 120 days after the date of the enactment of this Act, the Commission shall establish a task force to be known as the ''6G Task Force''.*

*(b) MEMBERSHIP.—*

*(1) APPOINTMENT.—The members of the Task Force shall be appointed by the Chair.*

*(2) COMPOSITION.—To the extent practicable, the membership of the Task Force shall be composed of the following:*

*(A) Representatives of companies in the communications industry, except companies that are determined by the Chair to be not trusted.*

*(B) Representatives of public interest organizations or academic institutions, except public interest organizations or academic institutions that are determined by the Chair to be not trusted.*

*(C) Representatives of the Federal Government, State governments, local governments, or Tribal Governments, with at least one member representing each such type of government.*

*(c) REPORT.—*

*(1) IN GENERAL.—Not later than 1 year after the date on which the Task Force is established under subsection (a), the Task Force shall publish in the Federal Register and on the website of the Commission, and submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate, a report on sixth-generation wireless technology, including—*

*(A) the status of industry-led standards-setting bodies in setting standards for such technology;*

*(B) possible uses of such technology identified by industry-led standards-setting bodies that are setting standards for such technology;*

*(C) any limitations of such technology (including any supply chain or cybersecurity limitations) identified by industry-led standards-setting bodies that are setting standards for such technology; and*

*(D) how to best work with entities across the Federal Government, State governments, local governments, and Tribal Governments to leverage such technology, including with regard to siting, deployment, and adoption.*

*(2) DRAFT REPORT; PUBLIC COMMENT.—The Task Force shall—*

*(A) not later than 180 days after the date on which the Task Force is established under subsection (a), publish in the Federal Register and on the website of the Commission a draft of the report required by paragraph (1); and*

*(B) accept public comments on such draft and take such comments into consideration in preparing the final version of such report.*

*(d) DEFINITIONS.—In this section:*

*(1) CHAIR.—The term ''Chair'' means the Chair of the Commission.*

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

*(3) NOT TRUSTED.—*

*(A) IN GENERAL.—The term ''not trusted'' means, with respect to an entity, that—*

*(i) the Chair has made a public determination that such entity is owned by, controlled by, or subject to the influence of a foreign adversary; or*

*(ii) the Chair otherwise determines that such entity poses a threat to the national security of the United States.*

*(B) CRITERIA FOR DETERMINATION.—In making a determination under subparagraph (A)(ii), the Chair shall use the criteria described in paragraphs (1) through (4) of section 2(c) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(c)), as appropriate.*

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

*(5) TASK FORCE.—The term ''Task Force'' means the 6G Task Force established under subsection (a).*

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Ohio (Mr. LATTA) each will control 20 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. 4045.

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. 4045, the FUTURE Networks Act. Even as we await the full deployment and utilization of fifth generation, or 5G, wireless networks, U.S. communications and technology companies are collaborating on the next generation of networks; specifically, 6G networks.

We may not be able to predict now the technological innovation that will come with these networks, but based on our Nation's experience to this point, we can foresee the issues that will need to be addressed to get 6G networks off the ground. Issues like supply chain availability, security, and equality in deployment and adoption will all need to be reviewed and resolved; and, therefore, it is not too early for government and relevant stakeholders to begin discussing these issues now. That is the goal of H.R. 4045, the FUTURE Networks Act.

This bipartisan legislation would require the FCC to convene a task force to examine relevant 6G issues. The task force will be made up of stakeholders from industry, public interest organizations, academic institutions, and relevant Federal, State, local, and Tribal Government representatives.

Finding agreed-upon approaches and solutions to these issues now will make for a smoother transition in the future.

I want to thank our Communications and Technology Subcommittee chairman, MIKE DOYLE, as well as Representatives JOHNSON and MCBATH, for their bipartisan leadership on this bill.

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

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

Mr. Speaker, I rise today in support of H.R. 4045, the FUTURE Networks Act, which was introduced by Representatives DOYLE, JOHNSON, and MCBATH.

This legislation will establish a task force at the Federal Communications Commission to follow industry-led progress in the development of 6G. The task force will be required to publish a report on the status of industry-led standards development, possible use-cases of 6G technology, and how best to facilitate the siting and infrastructure deployment of 6G technology.

While many parts of our country are waiting to see the new use-cases that 5G will drive, trusted vendors—including American companies—are leading the way on the fundamental aspects that will inform 6G. As the private sector identifies the contours of what this next generation of technology will look like, we must make sure that our regulatory environment will facilitate investment and innovation.

Republicans on the Energy and Commerce Committee have been spearheading efforts to deploy mobile