To establish a governmentwide approach to improving digital identity, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 30, 2021

Mr. Foster (for himself, Mr. Katko, Mr. Langevin, and Mr. Loudermilk) introduced the following bill; which was referred to the Committee on Oversight and Reform, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To establish a governmentwide approach to improving digital identity, and for other purposes.

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

2 SECTION 1. SHORT TITLE.

3 This Act may be cited as the “Improving Digital Identity Act of 2021”.

4 SEC. 2. FINDINGS.

5 Congress finds the following:
(1) The lack of an easy, affordable, and reliable way for organizations, businesses, and government agencies to identify whether an individual is who they claim to be online creates an attack vector that is widely exploited by adversaries in cyberspace, and precludes many high-value transactions from being available online.

(2) Incidents of identity theft and identity fraud continue to rise in the United States, where more than 164,000,000 consumer records containing personally identifiable information were breached in 2019, increasing the total number of data breaches by 17 percent from the previous year.

(3) In 2019, losses resulting from identity fraud amounted to $16,900,000,000.

(4) In 2019, the Director of the Treasury Department Financial Crimes Enforcement Network stated, “The abuse of personally identifiable information, and other building blocks of identity, is a key enabler behind much of the fraud and cybercrime affecting our nation today.”

(5) Trustworthy digital identity solutions can help under-banked and unbanked individuals better access to digital financial services through innovative delivery channels that promote financial inclusion.
(6) The inadequacy of current digital identity solutions degrades security and privacy for all Americans, and next generation solutions are needed that improve both security and privacy.

(7) Government entities, as authoritative issuers of identity in the United States, are uniquely positioned to deliver critical components that address deficiencies in our digital identity infrastructure and augment private sector digital identity and authentication solutions.

(8) State governments are particularly well suited to play a role in enhancing digital identity solutions used by both the public and private sectors, given the role of State governments as the issuers of driver’s licenses and other identity documents commonly used today.

(9) The private sector drives much of the innovation around digital identity in the United States and has an important role to play in delivering digital identity solutions.

(10) The 2016 bipartisan Commission on Enhancing National Cybersecurity called for the Federal Government to “create an interagency task force directed to find secure, user-friendly, privacy-centric ways in which agencies can serve as one au-
thoritative source to validate identity attributes in the broader identity market. This action would enable government agencies and the private sector to drive significant risk out of new account openings and other high-risk, high-value online services, and it would help all citizens more easily and securely engage in transactions online”.

(11) The public and private sectors should collaborate to deliver solutions that promote confidence, privacy, choice, and innovation.

(12) It should be the policy of the Government to use the authorities and capabilities of the Government to enhance the security, reliability, privacy, and convenience of digital identity solutions that support and protect transactions between individuals, government entities, and businesses, and that enable Americans to prove who they are online.

SEC. 3. IMPROVING DIGITAL IDENTITY TASK FORCE.

(a) Establishment.—There is established in the Executive Office of the President a task force to be known as the “Improving Digital Identity Task Force” (in this section referred to as the “Task Force”).

(b) Purpose.—The purpose of the Task Force is to establish a governmentwide effort to develop secure methods for Federal, State, and local agencies to validate iden-
entity attributes to protect the privacy and security of individuals and support reliable, interoperable digital identity verification in the public and private sectors.

(c) DIRECTOR.—The Task Force shall have a Director who shall be appointed by the President.

(d) MEMBERSHIP.—The Task Force shall include the following individuals or the designees of such individuals:

(1) FEDERAL GOVERNMENT MEMBERSHIP.—

(A) The Secretary of the Treasury.

(B) The Secretary of Homeland Security.

(C) The Secretary of State.

(D) The Secretary of Education.

(E) The Director of the Office of Management and Budget.

(F) The Commissioner of the Social Security Administration.

(G) The Director of the National Institute of Standards and Technology.

(H) The Administrator of General Services.

(I) The heads of other Federal agencies and offices who the President may designate or invite.

(2) STATE GOVERNMENT MEMBERSHIP.—The Task Force shall include 5 State government offi-
cials who represent State agencies that issue identity credentials and who have knowledge of the systems used to provide such credentials. Such officials shall include the following:

(A) A member appointed by the Speaker of the House of Representatives, in consultation with the Chairman of the Committee on Oversight and Reform and the Chairman of the Committee on Homeland Security of the House of Representatives.

(B) A member appointed by the minority leader of the House of Representatives, in consultation with the Ranking Member of the Committee on Oversight and Reform and the Ranking Member of the Committee on Homeland Security of the House of Representatives.

(C) A member appointed by the majority leader of the Senate, in consultation with the Chairman of the Committee on Homeland Security and Governmental Affairs of the Senate.

(D) A member appointed by the minority leader of the Senate, in consultation with the Ranking Member of the Committee on Homeland Security and Governmental Affairs of the Senate.
(E) A member appointed by the President.

(3) LOCAL GOVERNMENT MEMBERSHIP.—The Task Force shall include 5 local government officials who represent local agencies that issue identity credentials and who have knowledge of the systems used to provide such credentials. Such officials shall include the following:

(A) A member appointed by the Speaker of the House of Representatives, in consultation with the Chairman of the Committee on Oversight and Reform and Chairman of the Committee on Homeland Security of the House of Representatives.

(B) A member appointed by the minority leader of the House of Representatives, in consultation with the Chairman of the Committee on Oversight and Reform and the Chairman of the Committee on Homeland Security of the House of Representatives.

(C) A member appointed by the majority leader of the Senate, in consultation with the Chairman of the Committee on Homeland Security and Governmental Affairs of the Senate.

(D) A member appointed by the minority leader of the Senate, in consultation with the
Ranking Member of the Committee on Homeland Security and Governmental Affairs of the Senate.

(E) A member appointed by the President.

(e) MEETINGS.—The Task Force shall convene at the call of the Director.

(f) DUTIES.—The Task Force shall—

(1) identify Federal, State, and local agencies that issue identity information or hold information related to identifying an individual;

(2) assess restrictions with respect to the abilities of such agencies to verify identity information for other agencies and for nongovernmental organizations;

(3) assess any necessary changes in statute, regulation, or policy to address any restrictions determined under paragraph (2);

(4) recommend a standards-based architecture to enable agencies to provide services related to digital identity verification in a way that is secure, protects privacy, and is rooted in consumer consent;

(5) identify funding or resources needed to support such agencies that provide digital identity verification, including a recommendation with re-
spect to additional funding required for the grant program under section 5;

(6) determine whether it would be practicable for such agencies to use a fee-based model to provide digital identity verification to private sector entities;

(7) determine if any additional steps are necessary with respect to Federal, State, and local agencies to improve digital identity verification and management processes for the purpose of enhancing the security, reliability, privacy, and convenience of digital identity solutions that support and protect transactions between individuals, government entities, and businesses;

(8) assess risks related to potential criminal exploitation of digital identity verification services;

(9) evaluate the security, effectiveness, and benefits of a digital identity as compared to legacy physical identity verification; and

(10) to the extent practicable, seek input from and collaborate with interested parties in the private sector to carry out the purpose under subsection (b).

(g) RECOMMENDATIONS.—Not later than 180 days after the date of the enactment of this Act, the Task Force shall publish a report on the activities of the Task force, including recommendations on—
(1) priorities for research and development in
the systems that enable digital identity verification,
including how such priorities can be executed; and
(2) the standards-based architecture developed
pursuant to subsection (f)(4).

SEC. 4. DIGITAL IDENTITY FRAMEWORK.
(a) Establishment of a Framework.—Not later
than 1 year after the date of the enactment of this Act,
the Director of the National Institute of Standards and
Technology (in this section referred to as the “Director”)
shall develop and periodically update a framework of
standards, methodologies, procedures, and processes (in
this section referred to as the “Framework”) as a guide
for Federal, State, and local governments to follow when
providing services to support digital identity verification.
(b) Consideration.—In developing the Framework,
the Director shall consider—
(1) methods to protect the privacy of individ-
uals;
(2) security needs; and
(3) the needs of potential end-users and individ-
uals that will use services related to digital identity
verification.
(c) Consultation.—In carrying out subsection (a)
the Director shall consult with—
(1) the Improving Digital Identity Task Force established under section 3;

(2) potential end-users and individuals that will use services related to digital identity verification; and

(3) experts with relevant experience in the systems that enable digital identity verification, as determined by the Director.

(d) INTERIM PUBLICATION.—Not later than 240 days after the date of the enactment of this Act, the Director shall publish an interim version of the Framework.

(e) FINAL PUBLICATION.—Not later than 1 year after the date of enactment of this Act, the Director shall publish a final version of the Framework.

(f) UPDATES TO THE FRAMEWORK.—The Director shall, from time to time, update the Framework, with consideration given to—

(1) feedback from Federal, State, and local agencies that provide services related to digital identity verification; and

(2) any technological changes to the systems that enable digital identity verification.

(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary of Com-
merce $10,000,000 for each of fiscal years 2022 through 2026 to carry out this Act.

SEC. 5. DIGITAL IDENTITY INNOVATION GRANTS.

(a) Establishment.—Not later than 18 months after the date of the enactment of this Act, the Secretary of Homeland Security (in this section referred to as the “Secretary”) shall award grants to States to upgrade systems that provide drivers’ licenses or other types of identity credentials to support the development of highly secure, interoperable State systems that enable digital identity verification.

(b) Use of Funds.—A State that receives a grant under this section shall use—

(1) grant funds for services related to digital identity verification using the Framework developed pursuant to section 4; and

(2) not less than 10 percent of grant funds to provide services that assist individuals with obtaining identity credentials or identity verification services needed to obtain a digital driver’s license or digital State identity card.

(c) Authorization of Appropriations.—There is authorized to be appropriated to the Secretary such sums as may be necessary to carry out this section.
SEC. 6. REPORT AND RECOMMENDATION ON THE USE OF
SOCIAL SECURITY NUMBERS BY NON-
GOVERNMENTAL ORGANIZATIONS.

Not later than 1 year after the date of the enactment
of this Act, the Comptroller General of the United States
shall submit to the Committees on Ways and Means and
Financial Services of the House of Representatives and
the Committee on Finance of the Senate a report that in-
cludes the following:

(1) An analysis of legal and regulatory require-
ments with respect to the collection and retention of
Social Security numbers by nongovernmental organi-
izations.

(2) A recommendation on the necessity and ef-
effectiveness of any legal and regulatory requirement
analyzed pursuant to paragraph (1) and the use of
a form of identification other than a Social Security
number.

SEC. 7. SECURITY ENHANCEMENTS TO FEDERAL SYSTEMS.

(a) DIRECTIVES FOR FEDERAL AGENCIES.—Not
later than 6 months after the date of the enactment of
this Act, the Secretary of Homeland Security shall issue
binding operational directives to Federal agencies for pur-
pose of implementing—

(1) the guidelines published by the National In-
stitute of Standards and Technology in “Special
Publication 800–63” (commonly referred to as the “Digital Identity Guidelines’’); and

(2) the memorandum of the Office of Management and Budget issued on May 21, 2019, which includes the subject “Enabling Mission Delivery through Improved Identity, Credential, and Access Management’’.

(b) Reports.—

(1) Federal agency reports.—Not later than 1 year after the date of the enactment of this Act, the head of each Federal agency shall submit to the Secretary of Homeland Security a report on the efforts of each such Federal agency to implement the directives issued pursuant to subsection (a).

(2) Report to Congress.—Not later than 2 years after the date of the enactment of this Act, the Secretary of Homeland Security shall submit a report summarizing the efforts from the reports submitted pursuant to paragraph (1) to the following:

(A) The Committee on Homeland Security of the House of Representatives.

(B) The Committee on Oversight and Reform of the House of Representatives.
(C) The Committee on Homeland Security and Governmental Affairs of the Senate.

SEC. 8. DEFINITIONS.

For purposes of this Act:

(1) Digital identity verification.—The term “digital identity verification” means a process to verify the identity of an individual accessing a service online or through another electronic means.

(2) Identity credential.—The term “identity credential” means a document or other evidence of the identity of an individual issued by a government agency that conveys the identity of the individual, including a driver’s license or passport.