AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

117TH CONGRESS
2D SESSION

S. 4528

To establish a Government-wide approach to improving digital identity, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 13, 2022

Ms. SINEMA (for herself and Ms. LUMMIS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To establish a Government-wide approach to improving digital identity, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Improving Digital Identity Act of 2022''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) The lack of an easy, affordable, reliable, and secure way for organizations, businesses, and government agencies to identify whether an indi-

vidual 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 293,000,000 people were impacted by data breaches in 2021.

(3) Since 2017, losses resulting from identity fraud have increased by 333 percent, and, in 2020, those losses totaled $56,000,000,000.

(4) The Director of the Treasury Department Financial Crimes Enforcement Network has stated that the abuse of personally identifiable information and other building blocks of identity is a key enabler behind much of the fraud and cybercrime affecting the United States today.

(5) Trustworthy digital identity solutions can help give 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 people in the United States, and next generation solutions

are needed that improve security, privacy, equity, and accessibility.

(7) Government entities, as authoritative issuers of identity in the United States, are uniquely positioned to deliver critical components that address deficiencies in the digital identity infrastructure of the United States 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 public and private sectors should collaborate to deliver solutions that promote confidence, privacy, choice, equity, accessibility, and innovation. 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 bipartisan Commission on Enhancing National Cybersecurity has 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 1 authoritative 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 National Institute of Standards and Technology has published digital identity guidelines that address technical requirements for identity proofing and the authentication of users, but those guidelines do not cover requirements for providing identity attribute validation services that could be used to support identity proofing.

(12) It should be the policy of the Federal Government to use the authorities and capabilities of the Federal Government to enhance the security, reliability, privacy, equity, accessibility, and convenience of digital identity solutions that support and protect transactions between individuals, government entities, and businesses, and that enable people in the United States to prove who they are online, by providing consent-based identity attribute validation services and other components that address defi-

ciencies in the digital identity infrastructure of the United States and augment private sector digital identity and authentication solutions.

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE NOTIFICATION ENTITIES.—The term ''appropriate notification entities'' means—

(A) the President;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Oversight and Reform of the House of Representatives.

(2) DIGITAL IDENTITY VERIFICATION.—The term ''digital identity verification'' means a process to verify the identity or an identity attribute of an individual accessing a service online or through another electronic means.

(3) DIRECTOR.—The term ''Director'' means the Director of the Task Force.

(4) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given the term in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(5) IDENTITY ATTRIBUTE.—The term ''identity attribute'' means a data element associated with the identity of an individual, including, the name, address, or date of birth of an individual.

(6) 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.

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

(8) TASK FORCE.—The term ''Task Force'' means the Improving Digital Identity Task Force established under section 4(a).

SEC. 4. 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''.

(b) PURPOSE.—The purpose of the Task Force shall be to establish and coordinate a government-wide effort to develop secure methods for Federal, State, local, Tribal, and territorial agencies to improve access and enhance security between physical and digital identity credentials to—

(1) protect the privacy and security of individuals;

(2) support reliable, interoperable digital identity verification in the public and private sectors; and

(3) in achieving paragraphs (1) and (2), place a particular emphasis on—

(A) reducing identity theft and fraud;

(B) enabling trusted transactions; and

(C) ensuring equitable access to digital identity verification.

(c) DIRECTOR.—

(1) IN GENERAL.—The Task Force shall have a Director, who shall be appointed by the President.

(2) POSITION.—The Director shall serve at the pleasure of the President.

(3) PAY AND ALLOWANCES.—The Director shall be compensated at the rate of basic pay prescribed for level II of the Executive Schedule under section 5313 of title 5, United States Code.

(4) QUALIFICATIONS.—The Director shall have substantive technical expertise and managerial acumen that—

(A) is in the business of digital identity management, information security, or benefits administration;

(B) is gained from not less than 1 organization; and

(C) includes specific expertise gained from academia, advocacy organizations, and the private sector.

(5) EXCLUSIVITY.—The Director may not serve in any other capacity within the Federal Government while serving as Director.

(6) TERM.—The term of the Director, including any official acting in the role of the Director, shall terminate on the date described in subsection (k).

(d) MEMBERSHIP.—

(1) FEDERAL GOVERNMENT REPRESENTATIVES.—The Task Force shall include the following individuals or the designees of such individuals:

(A) The Secretary.

(B) The Secretary of the Treasury.

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

(D) The Director of the Financial Crimes Enforcement Network.

(E) The Commissioner of Social Security.

(F) The Secretary of State.

(G) The Administrator of General Services.

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

(I) The heads of other Federal agencies or offices as the President may designate or invite, as appropriate.

(2) STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT REPRESENTATIVES.—The Director shall appoint to the Task Force 6 State, local, Tribal, and territorial government officials who represent agencies that issue identity credentials and who have—

(A) experience in identity technology and services;

(B) knowledge of the systems used to provide identity credentials; or

(C) any other qualifications or competencies that may help achieve balance or otherwise support the mission of the Task Force.

(3) NONGOVERNMENTAL EXPERTS.—

(A) IN GENERAL.—The Director shall appoint to the Task Force 5 nongovernmental experts.

(B) SPECIFIC APPOINTMENTS.—The experts appointed under subparagraph (A) shall include the following:

(i) A member who is a privacy and civil liberties expert.

(ii) A member who is a technical expert in identity verification.

(iii) A member who is a technical expert in cybersecurity focusing on identity verification services.

(iv) A member who represents an industry identity verification service provider.

(v) A member who represents a party that relies on effective identity verification services to conduct business.

(e) WORKING GROUPS.—The Director shall organize the members of the Task Force into appropriate working groups for the purpose of increasing the efficiency and effectiveness of the Task Force, as appropriate.

(f) MEETINGS.—The Task Force shall—

(1) convene at the call of the Director; and

(2) provide an opportunity for public comment in accordance with section 10(a)(3) of the Federal Advisory Committee Act (5 U.S.C. App.).

(g) DUTIES.—In carrying out the purpose described in subsection (b), the Task Force shall—

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

(2) assess restrictions with respect to the abilities of the agencies described in paragraph (1) to verify identity information for other agencies and nongovernmental organizations;

(3) assess any necessary changes in statutes, regulations, or policy to address any restrictions assessed under paragraph (2);

(4) recommend a standards-based architecture to enable agencies to provide services relating to digital identity verification in a way that—

(A) is secure, protects privacy, and protects individuals against unfair and misleading practices;

(B) prioritizes equity and accessibility;

(C) requires individual consent for the provision of digital identify verification services by a Federal, State, local, Tribal, or territorial agency; and

(D) is interoperable among participating Federal, State, local, Tribal, and territorial agencies, as appropriate and in accordance with applicable laws;

(5) recommend principles to promote policies for shared identity proofing across public sector agencies, which may include single sign-on or broadly accepted attestations;

(6) identify funding or other resources needed to support the agencies described in paragraph (4) that provide digital identity verification, including a recommendation with respect to additional funding required for the grant program under section 5;

(7) recommend funding models to provide digital identity verification to private sector entities, which may include fee-based funding models;

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

(9) undertake other activities necessary to assess and address other matters relating to digital identity verification, including with respect to—

(A) the potential exploitation of digital identity tools or associated products and services by malign actors;

(B) privacy implications; and

(C) increasing access to foundational identity documents.

(h) PROHIBITION.—The Task Force may not implicitly or explicitly recommend the creation of—

(1) a single identity credential provided or mandated by the Federal Government for the purposes of verifying identity or associated attributes;

(2) a unilateral central national identification registry relating to digital identity verification; or

(3) a requirement that any individual be forced to use digital identity verification for a given public purpose.

(i) REQUIRED CONSULTATION.—The Task Force shall closely consult with leaders of Federal, State, local, Tribal, and territorial governments and nongovernmental leaders, which shall include the following:

(1) The Administrator of General Services.

(2) The Secretary of Education.

(3) The heads of other Federal agencies and offices determined appropriate by the Director.

(4) State, local, Tribal, and territorial government officials focused on identity, such as information technology officials and directors of State departments of motor vehicles and vital records bureaus.

(5) Digital privacy experts.

(6) Civil liberties experts.

(7) Technology and cybersecurity experts.

(8) Users of identity verification services.

(9) Representatives with relevant expertise from academia and advocacy organizations.

(10) Industry representatives with experience implementing digital identity systems.

(11) Identity theft and fraud prevention experts, including advocates for victims of identity theft and fraud.

(j) REPORTS.—

(1) INITIAL REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit to the appropriate notification entities a report on the activities of the Task Force, including—

(A) recommendations on—

(i) priorities for research and development in the systems that enable digital identity verification, including how the priorities can be executed;

(ii) the standards-based architecture developed pursuant to subsection (g)(4);

(iii) methods to leverage digital driver's licenses, distributed ledger technology, and other technologies; and

(iv) priorities for research and development in the systems and processes that reduce identity fraud; and

(B) summaries of the input and recommendations of the leaders consulted under subsection (i).

(2) INTERIM REPORTS.—The Director may submit to the appropriate notification entities interim reports the Director determines necessary to support the work of the Task Force and educate the public.

(3) FINAL REPORT.—Not later than 45 days before the date described in subsection (k), the Director shall submit to the appropriate notification entities a final report that includes recommendations for the President and Congress relating to any rel-

evant matter within the scope of the duties of the Task Force.

(4) PUBLIC AVAILABILITY.—The Task Force shall make the reports required under this subsection publicly available on centralized website as an open Government data asset (as defined in section 3502 of title 44, United States Code).

(k) SUNSET.—The Task Force shall conclude business on the date that is 3 years after the date of enactment of this Act.

SEC. 5. DIGITAL IDENTITY INNOVATION GRANTS.

(a) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall establish a grant program to award grants to State, local, Tribal, and territorial governments to upgrade systems that provide identity credentials to support the development of highly secure, interoperable systems that enable digital identity verification.

(b) REQUIRED CONSULTATION.—In establishing the grant program under subsection (a), the Secretary shall consult with the Task Force and the governmental and nongovernmental leaders described in section 4(i), with an emphasis on the consultation of—

(1) leaders of State, local, Tribal, and territorial governments; and

(2) leaders of State, local, Tribal, and territorial agencies that issue identity credentials or provide identity verification services and support relating to identify verification services.

(c) USE OF FUNDS.—A State, local, Tribal, or territorial government that receives a grant under this section shall—

(1) use funds from the grant for services relating to digital identity verification;

(2) implement meaningful digital identity verification cybersecurity, data protection, and privacy safeguards consistent with, or in excess of, any safeguards described in management guidance issued by the National Institute of Standards and Technology relating to—

(A) digital identity;

(B) cybersecurity;

(C) privacy;

(D) equity; or

(E) accessibility;

(3) expend 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 driver's license or a comparable identity card; and

(4) comply with any other requirements determined relevant by the Secretary to ensure the effective administration of the grant program established under this section.

(d) REQUIREMENTS.—A State, local, Tribal, or territorial government that receives a grant under this section shall expend amounts from the grant in a manner that—

(1) complies with the management guidance of the National Institute of Standards and Technology described in subsection (c)(2); and

(2) does not correspond with a matter described in section 4(h).

(e) 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. SECURITY ENHANCEMENTS TO FEDERAL SYSTEMS.

(a) GUIDANCE FOR FEDERAL AGENCIES.—Not later than 180 days after the date on which the Director submits the report required under section 4(j)(1), the Director of the Office of Management and Budget shall issue guidance to Federal agencies for the purpose of implementing any recommendations included in such report determined appropriate by the Director of the Office of Management and Budget.

(b) REPORTS ON FEDERAL AGENCY PROGRESS IMPROVING DIGITAL IDENTITY VERIFICATION CAPABILITIES.—

(1) ANNUAL REPORT ON GUIDANCE IMPLEMENTATION.—Not later than 1 year after the date of the issuance of guidance under subsection (a), and annually thereafter, the head of each Federal agency shall submit to the Director of the Office of Management and Budget a report on the efforts of the Federal agency to implement that guidance.

(2) PUBLIC REPORT.—

(A) IN GENERAL.—Not later than 450 days after the date of the issuance of guidance under subsection (a), and annually thereafter, the Director shall develop and make publicly available a report that includes—

(i) a list of digital identity verification services offered by Federal agencies;

(ii) the volume of digital identity verifications performed by each Federal agency;

(iii) information relating to the effectiveness of digital identity verification services by Federal agencies; and

(iv) recommendations to improve the effectiveness of digital identity verification services by Federal agencies.

(B) CONSULTATION.—In developing the first report required under subparagraph (A), the Director shall consult the Task Force.

(3) CONGRESSIONAL REPORT ON FEDERAL AGENCY DIGITAL IDENTITY CAPABILITIES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report relating to the implementation and effectiveness of the digital identity capabilities of Federal agencies.

(B) CONSULTATION.—In developing the report required under subparagraph (A), the Director of the Office of Management and Budget shall—

(i) consult with the Task Force; and

(ii) to the greatest extent practicable, include in the report recommendations of the Task Force.

(C) CONTENTS OF REPORT.—The report required under subparagraph (A) shall include—

(i) an analysis, including metrics and milestones, for the implementation by Federal agencies of—

(I) the guidelines published by the National Institute of Standards and Technology in the document entitled ''Special Publication 800–63'' (commonly referred to as the ''Digital Identity Guidelines''), or any successor document; and

(II) if feasible, any additional requirements relating to enhancing digital identity capabilities identified in the document of the Office of Management and Budget entitled ''M–19–17'' and issued on May 21, 2019, or any successor document;

(ii) a review of measures taken to advance the equity, accessibility, cybersecu-

rity, and privacy of digital identity verification services offered by Federal agencies; and

(iii) any other relevant data, information, or plans for Federal agencies to improve the digital identity capabilities of Federal agencies.

(c) ADDITIONAL REPORTS.—On the first March 1 occurring after the date described in subsection (b)(3)(A), and annually thereafter, the Director of the Office of Management and Budget shall include in the report required under section 3553(c) of title 44, United States Code—

(1) any additional and ongoing reporting on the matters described in subsection (b)(3)(C); and

(2) associated information collection mechanisms.

SEC. 7. GAO REPORT.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the estimated potential savings, due to the increased adoption and widespread use of digital identification, of—

(1) the Federal Government from averted benefit fraud; and

(2) the economy of the United States and consumers from averted identity theft.

(b) CONTENTS.—Among other variables the Comptroller General of the United States determines relevant, the report required under subsection (a) shall include multiple scenarios with varying uptake rates to demonstrate a range of possible outcomes.

○