

Calendar No. 616

117TH CONGRESS
2D SESSION**S. 4528****[Report No. 117–238]**

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

DECEMBER 12, 2022

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]**A BILL**

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Improving Digital
5 Identity Act of 2022”.

1 **SEC. 2. FINDINGS.**

2 Congress finds the following:

3 (1) The lack of an easy, affordable, reliable,
4 and secure way for organizations, businesses, and
5 government agencies to identify whether an indi-
6 vidual is who they claim to be online creates an at-
7 tack vector that is widely exploited by adversaries in
8 cyberspace and precludes many high-value trans-
9 actions from being available online.

10 (2) Incidents of identity theft and identity
11 fraud continue to rise in the United States, where
12 more than 293,000,000 people were impacted by
13 data breaches in 2021.

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

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

23 (5) Trustworthy digital identity solutions can
24 help give under-banked and unbanked individuals
25 better access to digital financial services through in-

1 novative delivery channels that promote financial in-
2 clusion.

3 (6) The inadequacy of current digital identity
4 solutions degrades security and privacy for all people
5 in the United States, and next generation solutions
6 are needed that improve security, privacy, equity,
7 and accessibility.

8 (7) Government entities, as authoritative
9 issuers of identity in the United States, are uniquely
10 positioned to deliver critical components that ad-
11 dress deficiencies in the digital identity infrastruc-
12 ture of the United States and augment private sec-
13 tor digital identity and authentication solutions.

14 (8) State governments are particularly well-suit-
15 ed to play a role in enhancing digital identity solu-
16 tions used by both the public and private sectors,
17 given the role of State governments as the issuers of
18 driver's licenses and other identity documents com-
19 monly used today.

20 (9) The public and private sectors should col-
21 laborate to deliver solutions that promote confidence,
22 privacy, choice, equity, accessibility, and innovation.
23 The private sector drives much of the innovation
24 around digital identity in the United States and has

1 an important role to play in delivering digital iden-
2 tity solutions.

3 (10) The bipartisan Commission on Enhancing
4 National Cybersecurity has called for the Federal
5 Government to “create an interagency task force di-
6 rected to find secure, user-friendly, privacy-centric
7 ways in which agencies can serve as ~~1~~ authoritative
8 source to validate identity attributes in the broader
9 identity market. This action would enable Govern-
10 ment agencies and the private sector to drive signifi-
11 cant risk out of new account openings and other
12 high-risk, high-value online services, and it would
13 help all citizens more easily and securely engage in
14 transactions online.”.

15 (11) The National Institute of Standards and
16 Technology has published digital identity guidelines
17 that address technical requirements for identity
18 proofing and the authentication of users, but those
19 guidelines do not cover requirements for providing
20 identity attribute validation services that could be
21 used to support identity proofing.

22 (12) It should be the policy of the Federal Gov-
23 ernment to use the authorities and capabilities of the
24 Federal Government to enhance the security, reli-
25 ability, privacy, equity, accessibility, and convenience

1 of digital identity solutions that support and protect
2 transactions between individuals, government enti-
3 ties, and businesses, and that enable people in the
4 United States to prove who they are online, by pro-
5 viding consent-based identity attribute validation
6 services and other components that address defi-
7 ciencies in the digital identity infrastructure of the
8 United States and augment private sector digital
9 identity and authentication solutions.

10 **SEC. 3. DEFINITIONS.**

11 In this Act:

12 ~~(1) APPROPRIATE NOTIFICATION ENTITIES.—~~

13 The term “appropriate notification entities”
14 means—

15 ~~(A) the President;~~

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

18 ~~(C) the Committee on Oversight and Re-~~
19 ~~form of the House of Representatives.~~

20 ~~(2) DIGITAL IDENTITY VERIFICATION.—~~The

21 term “digital identity verification” means a process
22 to verify the identity or an identity attribute of an
23 individual accessing a service online or through an-
24 other electronic means.

1 (3) DIRECTOR.—The term “Director” means
2 the Director of the Task Force.

3 (4) FEDERAL AGENCY.—The term “Federal
4 agency” has the meaning given the term in section
5 102 of the Robert T. Stafford Disaster Relief and
6 Emergency Assistance Act (42 U.S.C. 5122).

7 (5) IDENTITY ATTRIBUTE.—The term “identity
8 attribute” means a data element associated with the
9 identity of an individual, including, the name, ad-
10 dress, or date of birth of an individual.

11 (6) IDENTITY CREDENTIAL.—The term “iden-
12 tity credential” means a document or other evidence
13 of the identity of an individual issued by a govern-
14 ment agency that conveys the identity of the indi-
15 vidual, including a driver’s license or passport.

16 (7) SECRETARY.—The term “Secretary” means
17 the Secretary of Homeland Security.

18 (8) TASK FORCE.—The term “Task Force”
19 means the Improving Digital Identity Task Force
20 established under section 4(a).

21 **SEC. 4. IMPROVING DIGITAL IDENTITY TASK FORCE.**

22 (a) ESTABLISHMENT.—There is established in the
23 Executive Office of the President a task force to be known
24 as the “Improving Digital Identity Task Force”.

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

7 (1) protect the privacy and security of individ-
 8 uals;

9 (2) support reliable, interoperable digital iden-
 10 tity verification in the public and private sectors;
 11 and

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

14 (A) reducing identity theft and fraud;

15 (B) enabling trusted transactions; and

16 (C) ensuring equitable access to digital
 17 identity verification.

18 (c) ~~DIRECTOR.~~—

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

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

23 (3) ~~PAY AND ALLOWANCES.~~—The Director shall
 24 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.

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

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

5 (E) The Commissioner of Social Security.

6 (F) The Secretary of State.

7 (G) The Administrator of General Services.

8 (H) The Director of the Office of Manage-
9 ment and Budget.

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

13 (2) STATE, LOCAL, TRIBAL, AND TERRITORIAL
14 GOVERNMENT REPRESENTATIVES.—The Director
15 shall appoint to the Task Force 6 State, local, Trib-
16 al, and territorial government officials who represent
17 agencies that issue identity credentials and who
18 have—

19 (A) experience in identity technology and
20 services;

21 (B) knowledge of the systems used to pro-
22 vide identity credentials; or

23 (C) any other qualifications or com-
24 petencies that may help achieve balance or oth-
25 erwise support the mission of the Task Force.

1 ~~(3) NONGOVERNMENTAL EXPERTS.—~~

2 ~~(A) IN GENERAL.—The Director shall ap-~~
 3 ~~point to the Task Force 5 nongovernmental ex-~~
 4 ~~perts.~~

5 ~~(B) SPECIFIC APPOINTMENTS.—The ex-~~
 6 ~~perts appointed under subparagraph (A) shall~~
 7 ~~include the following:~~

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

10 ~~(ii) A member who is a technical ex-~~
 11 ~~pert in identity verification.~~

12 ~~(iii) A member who is a technical ex-~~
 13 ~~pert in cybersecurity focusing on identity~~
 14 ~~verification services.~~

15 ~~(iv) A member who represents an in-~~
 16 ~~dustry identity verification service provider.~~

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

20 ~~(e) WORKING GROUPS.—The Director shall organize~~
 21 ~~the members of the Task Force into appropriate working~~
 22 ~~groups for the purpose of increasing the efficiency and ef-~~
 23 ~~fectiveness of the Task Force, as appropriate.~~

24 ~~(f) MEETINGS.—The Task Force shall—~~

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

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

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

6 (1) identify Federal, State, local, Tribal, and
 7 territorial agencies that issue identity credentials or
 8 hold information relating to identifying an indi-
 9 vidual;

10 (2) assess restrictions with respect to the abili-
 11 ties of the agencies described in paragraph (1) to
 12 verify identity information for other agencies and
 13 nongovernmental organizations;

14 (3) assess any necessary changes in statutes,
 15 regulations, or policy to address any restrictions as-
 16 sessed under paragraph (2);

17 (4) recommend a standards-based architecture
 18 to enable agencies to provide services relating to dig-
 19 ital identity verification in a way that—

20 (A) is secure, protects privacy, and pro-
 21 tects individuals against unfair and misleading
 22 practices;

23 (B) prioritizes equity and accessibility;

24 (C) requires individual consent for the pro-
 25 vision of digital identity verification services by

1 a Federal, State, local, Tribal, or territorial
2 agency; and

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

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

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

16 (7) recommend funding models to provide dig-
17 ital identity verification to private sector entities;
18 which may include fee-based funding models;

19 (8) determine if any additional steps are nec-
20 essary with respect to Federal, State, local, Tribal,
21 and territorial agencies to improve digital identity
22 verification and management processes for the pur-
23 pose of enhancing the security, reliability, privacy,
24 accessibility, equity, and convenience of digital iden-
25 tity solutions that support and protect transactions

1 between individuals, government entities, and busi-
 2 nesses; and

3 ~~(9) undertake other activities necessary to as-~~
 4 ~~sess and address other matters relating to digital~~
 5 ~~identity verification, including with respect to—~~

6 ~~(A) the potential exploitation of digital~~
 7 ~~identity tools or associated products and serv-~~
 8 ~~ices by malign actors;~~

9 ~~(B) privacy implications; and~~

10 ~~(C) increasing access to foundational iden-~~
 11 ~~tity documents.~~

12 ~~(h) PROHIBITION.—The Task Force may not implic-~~
 13 ~~itly or explicitly recommend the creation of—~~

14 ~~(1) a single identity credential provided or man-~~
 15 ~~dated by the Federal Government for the purposes~~
 16 ~~of verifying identity or associated attributes;~~

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

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

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

1 ~~(1) The Administrator of General Services.~~

2 ~~(2) The Secretary of Education.~~

3 ~~(3) The heads of other Federal agencies and of-~~
4 ~~fices determined appropriate by the Director.~~

5 ~~(4) State, local, Tribal, and territorial govern-~~
6 ~~ment officials focused on identity, such as informa-~~
7 ~~tion technology officials and directors of State de-~~
8 ~~partments of motor vehicles and vital records bu-~~
9 ~~reaus.~~

10 ~~(5) Digital privacy experts.~~

11 ~~(6) Civil liberties experts.~~

12 ~~(7) Technology and cybersecurity experts.~~

13 ~~(8) Users of identity verification services.~~

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

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

18 ~~(11) Identity theft and fraud prevention ex-~~
19 ~~perts, including advocates for victims of identity~~
20 ~~theft and fraud.~~

21 ~~(j) REPORTS.—~~

22 ~~(1) INITIAL REPORT.—Not later than 180 days~~
23 ~~after the date of enactment of this Act, the Director~~
24 ~~shall submit to the appropriate notification entities~~

1 a report on the activities of the Task Force, includ-
 2 ing—

3 (A) recommendations on—

4 (i) priorities for research and develop-
 5 ment in the systems that enable digital
 6 identity verification, including how the pri-
 7 orities can be executed;

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

10 (iii) methods to leverage digital driv-
 11 er's licenses, distributed ledger technology,
 12 and other technologies; and

13 (iv) priorities for research and devel-
 14 opment in the systems and processes that
 15 reduce identity fraud; and

16 (B) summaries of the input and rec-
 17 ommendations of the leaders consulted under
 18 subsection (i).

19 (2) INTERIM REPORTS.—The Director may sub-
 20 mit to the appropriate notification entities interim
 21 reports the Director determines necessary to support
 22 the work of the Task Force and educate the public.

23 (3) FINAL REPORT.—Not later than 45 days
 24 before the date described in subsection (k), the Di-
 25 rector shall submit to the appropriate notification

1 entities a final report that includes recommendations
 2 for the President and Congress relating to any rel-
 3 evant matter within the scope of the duties of the
 4 Task Force.

5 (4) PUBLIC AVAILABILITY.—The Task Force
 6 shall make the reports required under this sub-
 7 section publicly available on centralized website as
 8 an open Government data asset (as defined in sec-
 9 tion 3502 of title 44, United States Code).

10 (k) SUNSET.—The Task Force shall conclude busi-
 11 ness on the date that is 3 years after the date of enact-
 12 ment of this Act.

13 **SEC. 5. DIGITAL IDENTITY INNOVATION GRANTS.**

14 (a) ESTABLISHMENT.—Not later than 1 year after
 15 the date of enactment of this Act, the Secretary shall es-
 16 tablish a grant program to award grants to State, local,
 17 Tribal, and territorial governments to upgrade systems
 18 that provide identity credentials to support the develop-
 19 ment of highly secure, interoperable systems that enable
 20 digital identity verification.

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

1 (1) leaders of State, local, Tribal, and terri-
2 torial governments; and

3 (2) leaders of State, local, Tribal, and terri-
4 torial agencies that issue identity credentials or pro-
5 vide identity verification services and support relat-
6 ing to identity verification services.

7 (e) USE OF FUNDS.—A State, local, Tribal, or terri-
8 torial government that receives a grant under this section
9 shall—

10 (1) use funds from the grant for services relat-
11 ing to digital identity verification;

12 (2) implement meaningful digital identity
13 verification cybersecurity, data protection, and pri-
14 vacy safeguards consistent with, or in excess of, any
15 safeguards described in management guidance issued
16 by the National Institute of Standards and Tech-
17 nology relating to—

18 (A) digital identity;

19 (B) cybersecurity;

20 (C) privacy;

21 (D) equity; or

22 (E) accessibility;

23 (3) expend not less than 10 percent of grant
24 funds to provide services that assist individuals with
25 obtaining identity credentials or identity verification

1 services needed to obtain a driver's license or a com-
 2 parable identity card; and

3 (4) comply with any other requirements deter-
 4 mined relevant by the Secretary to ensure the effec-
 5 tive administration of the grant program established
 6 under this section.

7 (d) REQUIREMENTS.—A State, local, Tribal, or terri-
 8 torial government that receives a grant under this section
 9 shall expend amounts from the grant in a manner that—

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

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

15 (e) AUTHORIZATION OF APPROPRIATIONS.—There is
 16 authorized to be appropriated to the Secretary such sums
 17 as may be necessary to carry out this section.

18 **SEC. 6. SECURITY ENHANCEMENTS TO FEDERAL SYSTEMS.**

19 (a) GUIDANCE FOR FEDERAL AGENCIES.—Not later
 20 than 180 days after the date on which the Director sub-
 21 mits the report required under section 4(j)(1), the Direc-
 22 tor of the Office of Management and Budget shall issue
 23 guidance to Federal agencies for the purpose of imple-
 24 menting any recommendations included in such report de-

1 terminated appropriate by the Director of the Office of Man-
 2 agement and Budget.

3 (b) ~~REPORTS ON FEDERAL AGENCY PROGRESS IM-~~
 4 ~~PROVING DIGITAL IDENTITY VERIFICATION CAPABILI-~~
 5 ~~TIES.—~~

6 (1) ~~ANNUAL REPORT ON GUIDANCE IMPLEMEN-~~
 7 ~~TATION.—~~Not later than 1 year after the date of the
 8 issuance of guidance under subsection (a), and an-
 9 nually thereafter, the head of each Federal agency
 10 shall submit to the Director of the Office of Manage-
 11 ment and Budget a report on the efforts of the Fed-
 12 eral agency to implement that guidance.

13 (2) ~~PUBLIC REPORT.—~~

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

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

21 (ii) the volume of digital identity
 22 verifications performed by each Federal
 23 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

1 Director of the Office of Management and
2 Budget shall—

- 3 (i) consult with the Task Force; and
4 (ii) to the greatest extent practicable,
5 include in the report recommendations of
6 the Task Force.

7 (C) CONTENTS OF REPORT.—The report
8 required under subparagraph (A) shall in-
9 clude—

- 10 (i) an analysis, including metrics and
11 milestones, for the implementation by Fed-
12 eral agencies of—

13 (I) the guidelines published by
14 the National Institute of Standards
15 and Technology in the document enti-
16 tled “Special Publication 800–63”
17 (commonly referred to as the “Digital
18 Identity Guidelines”); or any suc-
19 cessor document; and

20 (II) if feasible, any additional re-
21 quirements relating to enhancing dig-
22 ital identity capabilities identified in
23 the document of the Office of Man-
24 agement and Budget entitled “M–19–

1 17” and issued on May 21, 2019, or
2 any successor document;

3 (ii) a review of measures taken to ad-
4 vance the equity, accessibility, cybersecu-
5 rity, and privacy of digital identity
6 verification services offered by Federal
7 agencies; and

8 (iii) any other relevant data, informa-
9 tion, or plans for Federal agencies to im-
10 prove the digital identity capabilities of
11 Federal agencies.

12 (c) ~~ADDITIONAL REPORTS.~~—On the first March 1 oc-
13 curring after the date described in subsection (b)(3)(A),
14 and annually thereafter, the Director of the Office of Man-
15 agement and Budget shall include in the report required
16 under section 3553(c) of title 44, United States Code—

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

19 (2) associated information collection mecha-
20 nisms.

21 **SEC. 7. GAO REPORT.**

22 (a) ~~IN GENERAL.~~—Not later than 1 year after the
23 date of enactment of this Act, the Comptroller General
24 of the United States shall submit to Congress a report

1 on the estimated potential savings, due to the increased
 2 adoption and widespread use of digital identification, of—

3 (1) the Federal Government from averted ben-
 4 efit fraud; and

5 (2) the economy of the United States and con-
 6 sumers from averted identity theft.

7 (b) CONTENTS.—Among other variables the Comp-
 8 troller General of the United States determines relevant,
 9 the report required under subsection (a) shall include mul-
 10 tiple scenarios with varying uptake rates to demonstrate
 11 a range of possible outcomes.

12 **SECTION 1. SHORT TITLE.**

13 *This Act may be cited as the “Improving Digital Iden-*
 14 *tity Act of 2022”.*

15 **SEC. 2. FINDINGS.**

16 *Congress finds the following:*

17 (1) *The lack of an easy, affordable, reliable, and*
 18 *secure way for organizations, businesses, and govern-*
 19 *ment agencies to identify whether an individual is*
 20 *who they claim to be online creates an attack vector*
 21 *that is widely exploited by adversaries in cyberspace*
 22 *and precludes many high-value transactions from*
 23 *being available online.*

24 (2) *Incidents of identity theft and identity fraud*
 25 *continue to rise in the United States, where more*

1 *than 293,000,000 people were impacted by data*
2 *breaches in 2021.*

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

6 (4) *The Director of the Treasury Department Fi-*
7 *nancial Crimes Enforcement Network has stated that*
8 *the abuse of personally identifiable information and*
9 *other building blocks of identity is a key enabler be-*
10 *hind much of the fraud and cybercrime affecting the*
11 *United States today.*

12 (5) *The inadequacy of current digital identity*
13 *solutions degrades security and privacy for all people*
14 *in the United States, and next generation solutions*
15 *are needed that improve security, privacy, equity,*
16 *and accessibility.*

17 (6) *Government entities, as authoritative issuers*
18 *of identity in the United States, are uniquely posi-*
19 *tioned to deliver critical components that address de-*
20 *ficiencies in the digital identity infrastructure of the*
21 *United States and augment private sector digital*
22 *identity and authentication solutions.*

23 (7) *State governments are particularly well-suit-*
24 *ed to play a role in enhancing digital identity solu-*
25 *tions used by both the public and private sectors,*

1 *given the role of State governments as the issuers of*
2 *driver's licenses and other identity documents com-*
3 *monly used today.*

4 *(8) The public and private sectors should collabo-*
5 *rate to deliver solutions that promote confidence, pri-*
6 *vacy, choice, equity, accessibility, and innovation.*
7 *The private sector drives much of the innovation*
8 *around digital identity in the United States and has*
9 *an important role to play in delivering digital iden-*
10 *tity solutions.*

11 *(9) The bipartisan Commission on Enhancing*
12 *National Cybersecurity has called for the Federal*
13 *Government to "create an interagency task force di-*
14 *rected to find secure, user-friendly, privacy-centric*
15 *ways in which agencies can serve as 1 authoritative*
16 *source to validate identity attributes in the broader*
17 *identity market. This action would enable Govern-*
18 *ment agencies and the private sector to drive signifi-*
19 *cant risk out of new account openings and other high-*
20 *risk, high-value online services, and it would help all*
21 *citizens more easily and securely engage in trans-*
22 *actions online."*

23 *(10) The National Institute of Standards and*
24 *Technology has published digital identity guidelines*
25 *that address technical requirements for identity proof-*

ing 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.

(11) It should be the policy of the Federal Government to use the authorities and capabilities of the Federal Government, in coordination with State, local, Tribal, and territorial partners and private sector innovators, to enhance the security, reliability, privacy, equity, accessibility, and convenience of consent-based 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.

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

1 *verify the identity or an identity attribute of an indi-*
2 *vidual accessing a service online or through another*
3 *electronic means.*

4 (3) *DIRECTOR.*—*The term “Director” means the*
5 *Director of the Task Force.*

6 (4) *FEDERAL AGENCY.*—*The term “Federal agen-*
7 *cy” has the meaning given the term in section 102 of*
8 *the Robert T. Stafford Disaster Relief and Emergency*
9 *Assistance Act (42 U.S.C. 5122).*

10 (5) *IDENTITY ATTRIBUTE.*—*The term “identity*
11 *attribute” means a data element associated with the*
12 *identity of an individual, including, the name, ad-*
13 *dress, or date of birth of an individual.*

14 (6) *IDENTITY CREDENTIAL.*—*The term “identity*
15 *credential” means a document or other evidence of the*
16 *identity of an individual issued by a government*
17 *agency that conveys the identity of the individual, in-*
18 *cluding a driver’s license or passport.*

19 (7) *SECRETARY.*—*The term “Secretary” means*
20 *the Secretary of Homeland Security.*

21 (8) *TASK FORCE.*—*The term “Task Force”*
22 *means the Improving Digital Identity Task Force es-*
23 *tablished under section 4(a).*

1 **SEC. 4. IMPROVING DIGITAL IDENTITY TASK FORCE.**

2 (a) *ESTABLISHMENT.*—*There is established in the Ex-*
 3 *ecutive Office of the President a task force to be known as*
 4 *the “Improving Digital Identity Task Force”.*

5 (b) *PURPOSE.*—*The purpose of the Task Force shall*
 6 *be to establish and coordinate a government-wide effort to*
 7 *develop secure methods for Federal, State, local, Tribal, and*
 8 *territorial agencies to improve access and enhance security*
 9 *between physical and digital identity credentials, particu-*
 10 *larly by promoting the development of digital versions of*
 11 *existing physical identity credentials, including driver’s li-*
 12 *censes, e-Passports, social security credentials, and birth*
 13 *certificates, to—*

14 (1) *protect the privacy and security of individ-*
 15 *uals;*

16 (2) *support reliable, interoperable digital iden-*
 17 *tity verification in the public and private sectors; and*

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

20 (A) *reducing identity theft and fraud;*

21 (B) *enabling trusted transactions; and*

22 (C) *ensuring equitable access to digital*
 23 *identity verification.*

24 (c) *DIRECTOR.*—

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

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

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

7 (4) *QUALIFICATIONS.*—*The Director shall have*
 8 *substantive technical expertise and managerial acu-*
 9 *men that—*

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

13 (B) *is gained from not less than 1 organiza-*
 14 *tion; and*

15 (C) *includes specific expertise gained from*
 16 *academia, advocacy organizations, or the private*
 17 *sector.*

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

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

24 (d) *MEMBERSHIP.*—

1 (1) *FEDERAL GOVERNMENT REPRESENTA-*
 2 *TIVES.—The Task Force shall include the following*
 3 *individuals or the designees of such individuals:*

4 (A) *The Secretary.*

5 (B) *The Secretary of the Treasury.*

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

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

10 (E) *The Commissioner of Social Security.*

11 (F) *The Secretary of State.*

12 (G) *The Administrator of General Services.*

13 (H) *The Director of the Office of Manage-*
 14 *ment and Budget.*

15 (I) *The Postmaster General of the United*
 16 *States Postal Service.*

17 (J) *The National Cyber Director.*

18 (K) *The heads of other Federal agencies or*
 19 *offices as the President may designate or invite,*
 20 *as appropriate.*

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

1 (A) *experience in identity technology and*
 2 *services;*

3 (B) *knowledge of the systems used to pro-*
 4 *vide identity credentials; or*

5 (C) *any other qualifications or competencies*
 6 *that may help achieve balance or otherwise sup-*
 7 *port the mission of the Task Force.*

8 (3) *NONGOVERNMENTAL EXPERTS.—*

9 (A) *IN GENERAL.—The Director shall ap-*
 10 *point to the Task Force 5 nongovernmental ex-*
 11 *perts.*

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

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

17 (ii) *A member who is a technical ex-*
 18 *pert in identity verification.*

19 (iii) *A member who is a technical ex-*
 20 *pert in cybersecurity focusing on identity*
 21 *verification services.*

22 (iv) *A member who represents an in-*
 23 *dustry identity verification service provider.*

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

4 (e) *WORKING GROUPS.—The Director shall organize*
5 *the members of the Task Force into appropriate working*
6 *groups for the purpose of increasing the efficiency and effec-*
7 *tiveness of the Task Force, as appropriate.*

8 (f) *MEETINGS.—The Task Force shall—*

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

10 (2) *provide an opportunity for public comment*
11 *in accordance with section 10(a)(3) of the Federal Ad-*
12 *visory Committee Act (5 U.S.C. App.).*

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

15 (1) *identify Federal, State, local, Tribal, and ter-*
16 *ritorial agencies that issue identity credentials or*
17 *hold information relating to identifying an indi-*
18 *vidual;*

19 (2) *assess restrictions with respect to the abilities*
20 *of the agencies described in paragraph (1) to verify*
21 *identity information for other agencies and non-*
22 *governmental organizations;*

23 (3) *assess any necessary changes in statutes, reg-*
24 *ulations, or policy to address any restrictions assessed*
25 *under paragraph (2);*

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

4 (A) *is secure, protects privacy, and protects*
5 *individuals against unfair and misleading prac-*
6 *tices;*

7 (B) *prioritizes equity and accessibility;*

8 (C) *requires individual consent for the pro-*
9 *vision of digital identify verification services by*
10 *a Federal, State, local, Tribal, or territorial*
11 *agency; and*

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

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

20 (6) *identify funding or other resources needed to*
21 *support the agencies described in paragraph (4) that*
22 *provide digital identity verification, including rec-*
23 *ommendations with respect to the need for and the de-*
24 *sign of a Federal grant program to implement the*
25 *recommendations of the Task Force and facilitate the*

1 *development and upgrade of State, local, Tribal, and*
 2 *territorial highly-secure interoperable systems that en-*
 3 *able digital identity verification;*

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

7 *(8) determine if any additional steps are nec-*
 8 *essary with respect to Federal, State, local, Tribal,*
 9 *and territorial agencies to improve digital identity*
 10 *verification and management processes for the pur-*
 11 *pose of enhancing the security, reliability, privacy,*
 12 *accessibility, equity, and convenience of digital iden-*
 13 *tity solutions that support and protect transactions*
 14 *between individuals, government entities, and busi-*
 15 *nesses; and*

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

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

22 *(B) privacy implications; and*

23 *(C) increasing access to foundational iden-*
 24 *tity documents.*

1 (h) *PROHIBITION.*—*The Task Force may not implic-*
 2 *itly or explicitly recommend the creation of—*

3 (1) *a single identity credential provided or man-*
 4 *dated by the Federal Government for the purposes of*
 5 *verifying identity or associated attributes;*

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

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

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

15 (1) *The Secretary of Education.*

16 (2) *The heads of other Federal agencies and of-*
 17 *fices determined appropriate by the Director.*

18 (3) *State, local, Tribal, and territorial govern-*
 19 *ment officials focused on identity, such as informa-*
 20 *tion technology officials and directors of State depart-*
 21 *ments of motor vehicles and vital records bureaus.*

22 (4) *Digital privacy experts.*

23 (5) *Civil liberties experts.*

24 (6) *Technology and cybersecurity experts.*

25 (7) *Users of identity verification services.*

1 (8) *Representatives with relevant expertise from*
2 *academia and advocacy organizations.*

3 (9) *Industry representatives with experience im-*
4 *plementing digital identity systems.*

5 (10) *Identity theft and fraud prevention experts,*
6 *including advocates for victims of identity theft and*
7 *fraud.*

8 (j) *REPORTS.—*

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

13 (A) *recommendations on—*

14 (i) *priorities for research and develop-*
15 *ment in the systems that enable digital*
16 *identity verification, including how the pri-*
17 *orities can be executed;*

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

20 (iii) *methods to leverage digital driv-*
21 *er's licenses, distributed ledger technology,*
22 *and other technologies; and*

23 (iv) *priorities for research and develop-*
24 *ment in the systems and processes that re-*
25 *duce identity fraud; and*

1 (B) summaries of the input and rec-
 2 ommendations of the leaders consulted under
 3 subsection (i).

4 (2) *INTERIM REPORTS.*—

5 (A) *IN GENERAL.*—*The Director may sub-*
 6 *mit to the appropriate notification entities in-*
 7 *terim reports the Director determines necessary*
 8 *to support the work of the Task Force and edu-*
 9 *cate the public.*

10 (B) *MANDATORY REPORT.*—*Not later than*
 11 *the date that is 18 months after the date of en-*
 12 *actment of this Act, the Director shall submit to*
 13 *the appropriate notification entities an interim*
 14 *report addressing—*

15 (i) *the matters described in paragraphs*
 16 (1), (2), (4), and (6) of subsection (g); and

17 (ii) *any other matters the Director de-*
 18 *termines necessary to support the work of*
 19 *the Task Force and educate the public.*

20 (3) *FINAL REPORT.*—*Not later than 180 days be-*
 21 *fore the date described in subsection (k), the Director*
 22 *shall submit to the appropriate notification entities a*
 23 *final report that includes recommendations for the*
 24 *President and Congress relating to any relevant mat-*
 25 *ter within the scope of the duties of the Task Force.*

1 (4) *PUBLIC AVAILABILITY.*—*The Task Force shall*
 2 *make the reports required under this subsection pub-*
 3 *licly available on centralized website as an open Gov-*
 4 *ernment data asset (as defined in section 3502 of title*
 5 *44, United States Code).*

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

9 **SEC. 5. SECURITY ENHANCEMENTS TO FEDERAL SYSTEMS.**

10 (a) *GUIDANCE FOR FEDERAL AGENCIES.*—*Not later*
 11 *than 180 days after the date on which the Director submits*
 12 *the report required under section 4(j)(1), the Director of the*
 13 *Office of Management and Budget shall issue guidance to*
 14 *Federal agencies for the purpose of implementing any rec-*
 15 *ommendations included in such report determined appro-*
 16 *priate by the Director of the Office of Management and*
 17 *Budget.*

18 (b) *REPORTS ON FEDERAL AGENCY PROGRESS IM-*
 19 *PROVING DIGITAL IDENTITY VERIFICATION CAPABILI-*
 20 *TIES.*—

21 (1) *ANNUAL REPORT ON GUIDANCE IMPLEMENTA-*
 22 *TION.*—*Not later than 1 year after the date of the*
 23 *issuance of guidance under subsection (a), and annu-*
 24 *ally thereafter, the head of each Federal agency shall*
 25 *submit to the Director of the Office of Management*

1 *and Budget a report on the efforts of the Federal*
 2 *agency to implement that guidance.*

3 (2) *PUBLIC REPORT.—*

4 (A) *IN GENERAL.—Not later than 45 days*
 5 *after the date of the issuance of guidance under*
 6 *subsection (a), and annually thereafter, the Di-*
 7 *rector shall develop and make publicly available*
 8 *a report that includes—*

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

11 (ii) *the volume of digital identity*
 12 *verifications performed by each Federal*
 13 *agency;*

14 (iii) *information relating to the effec-*
 15 *tiveness of digital identity verification serv-*
 16 *ices by Federal agencies; and*

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

20 (B) *CONSULTATION.—In developing the first*
 21 *report required under subparagraph (A), the Di-*
 22 *rector shall consult the Task Force.*

23 (3) *CONGRESSIONAL REPORT ON FEDERAL AGEN-*
 24 *CY DIGITAL IDENTITY CAPABILITIES.—*

1 (A) *IN GENERAL.*—Not later than 180 days
2 after the date of the enactment of this Act, the
3 Director of the Office of Management and Budget
4 et, in coordination with the Director of the Cy-
5 bersecurity and Infrastructure Security Agency,
6 shall submit to the Committee on Homeland Se-
7 curity and Governmental Affairs of the Senate
8 and the Committee on Oversight and Reform of
9 the House of Representatives a report relating to
10 the implementation and effectiveness of the dig-
11 ital identity capabilities of Federal agencies.

12 (B) *CONSULTATION.*—In developing the re-
13 port required under subparagraph (A), the Di-
14 rector of the Office of Management and Budget
15 shall—

- 16 (i) consult with the Task Force; and
17 (ii) to the greatest extent practicable,
18 include in the report recommendations of
19 the Task Force.

20 (C) *CONTENTS OF REPORT.*—The report re-
21 quired under subparagraph (A) shall include—

- 22 (i) an analysis, including metrics and
23 milestones, for the implementation by Fed-
24 eral agencies of—

1 (I) the guidelines published by the
 2 National Institute of Standards and
 3 Technology in the document entitled
 4 “Special Publication 800–63” (com-
 5 monly referred to as the “Digital Iden-
 6 tity Guidelines”), or any successor doc-
 7 ument; and

8 (II) if feasible, any additional re-
 9 quirements relating to enhancing dig-
 10 ital identity capabilities identified in
 11 the document of the Office of Manage-
 12 ment and Budget entitled “M–19–17”
 13 and issued on May 21, 2019, or any
 14 successor document;

15 (ii) a review of measures taken to ad-
 16 vance the equity, accessibility, cybersecurity,
 17 and privacy of digital identity verification
 18 services offered by Federal agencies; and

19 (iii) any other relevant data, informa-
 20 tion, or plans for Federal agencies to im-
 21 prove the digital identity capabilities of
 22 Federal agencies.

23 (c) *ADDITIONAL REPORTS.*—On the first March 1 oc-
 24 curring after the date described in subsection (b)(3)(A), and
 25 annually thereafter, the Director of the Office of Manage-

1 *ment and Budget shall include in the report required under*
 2 *section 3553(c) of title 44, United States Code—*

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

5 *(2) associated information collection mecha-*
 6 *nisms.*

7 **SEC. 6. GAO REPORT.**

8 *(a) IN GENERAL.—Not later than 1 year after the date*
 9 *of enactment of this Act, the Comptroller General of the*
 10 *United States shall submit to Congress a report on the esti-*
 11 *mated potential savings, including estimated annual poten-*
 12 *tial savings, due to the increased adoption and widespread*
 13 *use of digital identification, of—*

14 *(1) the Federal Government from averted fraud,*
 15 *including benefit fraud; and*

16 *(2) the economy of the United States and con-*
 17 *sumers from averted identity theft.*

18 *(b) CONTENTS.—Among other variables the Comp-*
 19 *troller General of the United States determines relevant, the*
 20 *report required under subsection (a) shall include multiple*
 21 *scenarios with varying uptake rates to demonstrate a range*
 22 *of possible outcomes.*

Calendar No. 616

117TH CONGRESS
2D Session

S. 4528

[Report No. 117-238]

A BILL

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

DECEMBER 12, 2022

Reported with an amendment