

117TH CONGRESS
2D SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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

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”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

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

1 vidual is who they claim to be online creates an at-
2 tack vector that is widely exploited by adversaries in
3 cyberspace and precludes many high-value trans-
4 actions from being available online.

5 (2) Incidents of identity theft and identity
6 fraud continue to rise in the United States, where
7 more than 293,000,000 people were impacted by
8 data breaches in 2021.

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

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

18 (5) Trustworthy digital identity solutions can
19 help give under-banked and unbanked individuals
20 better access to digital financial services through in-
21 novative delivery channels that promote financial in-
22 clusion.

23 (6) The inadequacy of current digital identity
24 solutions degrades security and privacy for all people
25 in the United States, and next generation solutions

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

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

9 (8) State governments are particularly well-suit-
10 ed to play a role in enhancing digital identity solu-
11 tions used by both the public and private sectors,
12 given the role of State governments as the issuers of
13 driver’s licenses and other identity documents com-
14 monly used today.

15 (9) The public and private sectors should col-
16 laborate to deliver solutions that promote confidence,
17 privacy, choice, equity, accessibility, and innovation.
18 The private sector drives much of the innovation
19 around digital identity in the United States and has
20 an important role to play in delivering digital iden-
21 tity solutions.

22 (10) The bipartisan Commission on Enhancing
23 National Cybersecurity has called for the Federal
24 Government to “create an interagency task force di-
25 rected to find secure, user-friendly, privacy-centric

1 ways in which agencies can serve as 1 authoritative
2 source to validate identity attributes in the broader
3 identity market. This action would enable Govern-
4 ment agencies and the private sector to drive signifi-
5 cant risk out of new account openings and other
6 high-risk, high-value online services, and it would
7 help all citizens more easily and securely engage in
8 transactions online.”.

9 (11) The National Institute of Standards and
10 Technology has published digital identity guidelines
11 that address technical requirements for identity
12 proofing and the authentication of users, but those
13 guidelines do not cover requirements for providing
14 identity attribute validation services that could be
15 used to support identity proofing.

16 (12) It should be the policy of the Federal Gov-
17 ernment to use the authorities and capabilities of the
18 Federal Government to enhance the security, reli-
19 ability, privacy, equity, accessibility, and convenience
20 of digital identity solutions that support and protect
21 transactions between individuals, government enti-
22 ties, and businesses, and that enable people in the
23 United States to prove who they are online, by pro-
24 viding consent-based identity attribute validation
25 services and other components that address defi-

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

4 **SEC. 3. DEFINITIONS.**

5 In this Act:

6 (1) **APPROPRIATE NOTIFICATION ENTITIES.**—

7 The term “appropriate notification entities”
8 means—

9 (A) the President;

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

12 (C) the Committee on Oversight and Re-
13 form of the House of Representatives.

14 (2) **DIGITAL IDENTITY VERIFICATION.**—The
15 term “digital identity verification” means a process
16 to verify the identity or an identity attribute of an
17 individual accessing a service online or through an-
18 other electronic means.

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

21 (4) **FEDERAL AGENCY.**—The term “Federal
22 agency” has the meaning given the term in section
23 102 of the Robert T. Stafford Disaster Relief and
24 Emergency Assistance Act (42 U.S.C. 5122).

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

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

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

12 (8) TASK FORCE.—The term “Task Force”
13 means the Improving Digital Identity Task Force
14 established under section 4(a).

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

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

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

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

3 (2) support reliable, interoperable digital iden-
4 tity verification in the public and private sectors;
5 and

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

8 (A) reducing identity theft and fraud;

9 (B) enabling trusted transactions; and

10 (C) ensuring equitable access to digital
11 identity verification.

12 (c) DIRECTOR.—

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

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

17 (3) PAY AND ALLOWANCES.—The Director shall
18 be compensated at the rate of basic pay prescribed
19 for level II of the Executive Schedule under section
20 5313 of title 5, United States Code.

21 (4) QUALIFICATIONS.—The Director shall have
22 substantive technical expertise and managerial acu-
23 men that—

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

4 (B) is gained from not less than 1 organi-
5 zation; and

6 (C) includes specific expertise gained from
7 academia, advocacy organizations, and the pri-
8 vate sector.

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

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

15 (d) MEMBERSHIP.—

16 (1) FEDERAL GOVERNMENT REPRESENTA-
17 TIVES.—The Task Force shall include the following
18 individuals or the designees of such individuals:

19 (A) The Secretary.

20 (B) The Secretary of the Treasury.

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

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

25 (E) The Commissioner of Social Security.

1 (F) The Secretary of State.

2 (G) The Administrator of General Services.

3 (H) The Director of the Office of Manage-
4 ment and Budget.

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

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

14 (A) experience in identity technology and
15 services;

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

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

21 (3) NONGOVERNMENTAL EXPERTS.—

22 (A) IN GENERAL.—The Director shall ap-
23 point to the Task Force 5 nongovernmental ex-
24 perts.

1 (B) SPECIFIC APPOINTMENTS.—The ex-
2 perts appointed under subparagraph (A) shall
3 include the following:

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

6 (ii) A member who is a technical ex-
7 pert in identity verification.

8 (iii) A member who is a technical ex-
9 pert in cybersecurity focusing on identity
10 verification services.

11 (iv) A member who represents an in-
12 dustry identity verification service provider.

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

16 (e) WORKING GROUPS.—The Director shall organize
17 the members of the Task Force into appropriate working
18 groups for the purpose of increasing the efficiency and ef-
19 fectiveness of the Task Force, as appropriate.

20 (f) MEETINGS.—The Task Force shall—

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

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

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

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

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

11 (3) assess any necessary changes in statutes,
12 regulations, or policy to address any restrictions as-
13 sessed under paragraph (2);

14 (4) recommend a standards-based architecture
15 to enable agencies to provide services relating to dig-
16 ital identity verification in a way that—

17 (A) is secure, protects privacy, and pro-
18 tects individuals against unfair and misleading
19 practices;

20 (B) prioritizes equity and accessibility;

21 (C) requires individual consent for the pro-
22 vision of digital identify verification services by
23 a Federal, State, local, Tribal, or territorial
24 agency; and

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

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

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

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

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

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

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

7 (B) privacy implications; and

8 (C) increasing access to foundational iden-
9 tity documents.

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

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

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

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

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

24 (1) The Administrator of General Services.

25 (2) The Secretary of Education.

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

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

8 (5) Digital privacy experts.

9 (6) Civil liberties experts.

10 (7) Technology and cybersecurity experts.

11 (8) Users of identity verification services.

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

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

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

19 (j) REPORTS.—

20 (1) INITIAL REPORT.—Not later than 180 days
21 after the date of enactment of this Act, the Director
22 shall submit to the appropriate notification entities
23 a report on the activities of the Task Force, includ-
24 ing—

25 (A) recommendations on—

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

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

7 (iii) methods to leverage digital driv-
8 er's licenses, distributed ledger technology,
9 and other technologies; and

10 (iv) priorities for research and devel-
11 opment in the systems and processes that
12 reduce identity fraud; and

13 (B) summaries of the input and rec-
14 ommendations of the leaders consulted under
15 subsection (i).

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

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

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

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

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

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

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

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

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

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

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

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

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

16 (A) digital identity;

17 (B) cybersecurity;

18 (C) privacy;

19 (D) equity; or

20 (E) accessibility;

21 (3) expend not less than 10 percent of grant
22 funds to provide services that assist individuals with
23 obtaining identity credentials or identity verification
24 services needed to obtain a driver's license or a com-
25 parable identity card; and

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

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

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

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

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

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

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

1 (b) REPORTS ON FEDERAL AGENCY PROGRESS IM-
2 PROVING DIGITAL IDENTITY VERIFICATION CAPABILI-
3 TIES.—

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

11 (2) PUBLIC REPORT.—

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

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

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

22 (iii) information relating to the effec-
23 tiveness of digital identity verification serv-
24 ices by Federal agencies; and

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

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

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

9 (A) IN GENERAL.—Not later than 180
10 days after the date of the enactment of this
11 Act, the Director of the Office of Management
12 and Budget, in coordination with the Director
13 of the Cybersecurity and Infrastructure Secu-
14 rity Agency, shall submit to the Committee on
15 Homeland Security and Governmental Affairs
16 of the Senate and the Committee on Oversight
17 and Reform of the House of Representatives a
18 report relating to the implementation and effec-
19 tiveness of the digital identity capabilities of
20 Federal agencies.

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

25 (i) consult with the Task Force; and

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

4 (C) CONTENTS OF REPORT.—The report
5 required under subparagraph (A) shall in-
6 clude—

7 (i) an analysis, including metrics and
8 milestones, for the implementation by Fed-
9 eral agencies of—

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

17 (II) if feasible, any additional re-
18 quirements relating to enhancing dig-
19 ital identity capabilities identified in
20 the document of the Office of Man-
21 agement and Budget entitled “M–19–
22 17” and issued on May 21, 2019, or
23 any successor document;

24 (ii) a review of measures taken to ad-
25 vance the equity, accessibility, cybersecu-

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

4 (iii) any other relevant data, informa-
5 tion, or plans for Federal agencies to im-
6 prove the digital identity capabilities of
7 Federal agencies.

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

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

15 (2) associated information collection mecha-
16 nisms.

17 **SEC. 7. GAO REPORT.**

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

23 (1) the Federal Government from averted ben-
24 efit fraud; and

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

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