

118TH CONGRESS
1ST 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 2023”.

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) The inadequacy of current digital identity
19 solutions degrades security and privacy for all people
20 in the United States, and next generation solutions
21 are needed that improve security, privacy, equity,
22 and accessibility.

23 (6) Government entities, as authoritative
24 issuers of identity in the United States, are uniquely
25 positioned to deliver critical components that ad-

1 dress deficiencies in the digital identity infrastruc-
2 ture of the United States and augment private sec-
3 tor digital identity and authentication solutions.

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

10 (8) The public and private sectors should col-
11 laborate to deliver solutions that promote confidence,
12 privacy, choice, equity, accessibility, and innovation.
13 The private sector drives much of the innovation
14 around digital identity in the United States and has
15 an important role to play in delivering digital iden-
16 tity solutions.

17 (9) The bipartisan Commission on Enhancing
18 National Cybersecurity has called for the Federal
19 Government to “create an interagency task force di-
20 rected to find secure, user-friendly, privacy-centric
21 ways in which agencies can serve as 1 authoritative
22 source to validate identity attributes in the broader
23 identity market. This action would enable Govern-
24 ment agencies and the private sector to drive signifi-
25 cant risk out of new account openings and other

1 high-risk, high-value online services, and it would
2 help all citizens more easily and securely engage in
3 transactions online.”.

4 (10) It should be the policy of the Federal Gov-
5 ernment to use the authorities and capabilities of the
6 Federal Government, in coordination with State,
7 local, Tribal, and territorial partners and private
8 sector innovators, to enhance the security, reliability,
9 privacy, equity, accessibility, and convenience of con-
10 sent-based digital identity solutions that support and
11 protect transactions between individuals, government
12 entities, and businesses, and that enable people in
13 the United States to prove who they are online.

14 **SEC. 3. DEFINITIONS.**

15 In this Act:

16 (1) APPROPRIATE NOTIFICATION ENTITIES.—

17 The term “appropriate notification entities”
18 means—

19 (A) the President;

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

22 (C) the Committee on Oversight and Re-
23 form of the House of Representatives.

24 (2) DIGITAL IDENTITY VERIFICATION.—The
25 term “digital identity verification” means a process

1 to verify the identity or an identity attribute of an
2 individual accessing a service online or through an-
3 other electronic means.

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

6 (4) FEDERAL AGENCY.—The term “Federal
7 agency” has the meaning given the term in section
8 102 of the Robert T. Stafford Disaster Relief and
9 Emergency 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 “iden-
15 tity credential” means a document or other evidence
16 of the identity of an individual issued by a govern-
17 ment agency that conveys the identity of the indi-
18 vidual, including 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
23 established under section 4(a).

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

2 (a) ESTABLISHMENT.—There is established in the
3 Executive Office of the President a task force to be known
4 as 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
7 to develop secure methods for Federal, State, local, Tribal,
8 and territorial agencies to improve access and enhance se-
9 curity between physical and digital identity credentials,
10 particularly by promoting the development of digital
11 versions of existing physical identity credentials, including
12 driver’s licenses, e-Passports, social security credentials,
13 and birth 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;
18 and

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

21 (A) reducing identity theft and fraud;

22 (B) enabling trusted transactions; and

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

25 (c) DIRECTOR.—

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

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

5 (3) PAY AND ALLOWANCES.—The Director shall
6 be compensated at the rate of basic pay prescribed
7 for level II of the Executive Schedule under section
8 5313 of title 5, United States Code.

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

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

15 (B) is gained from not less than 1 organi-
16 zation; and

17 (C) includes specific expertise gained from
18 academia, advocacy organizations, or the pri-
19 vate sector.

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

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

1 (d) MEMBERSHIP.—

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

5 (A) The Secretary.

6 (B) The Secretary of the Treasury.

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

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

11 (E) The Commissioner of Social Security.

12 (F) The Secretary of State.

13 (G) The Administrator of General Services.

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

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

18 (J) The National Cyber Director.

19 (K) The Attorney General.

20 (L) The heads of other Federal agencies or
21 offices as the President may designate or invite,
22 as appropriate.

23 (2) STATE, LOCAL, TRIBAL, AND TERRITORIAL
24 GOVERNMENT REPRESENTATIVES.—The Director
25 shall appoint to the Task Force 6 State, local, Trib-

1 al, and territorial government officials who represent
2 agencies that issue identity credentials and who
3 have—

4 (A) experience in identity technology and
5 services;

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

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

11 (3) NONGOVERNMENTAL EXPERTS.—

12 (A) IN GENERAL.—The Director shall ap-
13 point to the Task Force 5 nongovernmental ex-
14 perts.

15 (B) SPECIFIC APPOINTMENTS.—The ex-
16 perts appointed under subparagraph (A) shall
17 include the following:

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

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

22 (iii) A member who is a technical ex-
23 pert in cybersecurity focusing on identity
24 verification services.

1 (iv) A member who represents the
2 identity verification services industry.

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

6 (e) WORKING GROUPS.—The Director shall organize
7 the members of the Task Force into appropriate working
8 groups for the purpose of increasing the efficiency and ef-
9 fectiveness of the Task Force, as appropriate.

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

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

12 (2) provide an opportunity for public comment
13 in accordance with section 1009(a)(3) of title 5,
14 United States Code.

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

17 (1) identify Federal, State, local, Tribal, and
18 territorial agencies that issue identity credentials or
19 hold information relating to identifying an indi-
20 vidual;

21 (2) assess restrictions with respect to the abili-
22 ties of the agencies described in paragraph (1) to
23 verify identity information for other agencies and
24 nongovernmental organizations;

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

4 (4) recommend a strategy, based on existing
5 standards, to enable agencies to provide services re-
6 lating to digital identity verification in a way that—

7 (A) is secure, protects privacy, and pro-
8 tects individuals against unfair and misleading
9 practices;

10 (B) prioritizes equity and accessibility;

11 (C) requires individual consent for the pro-
12 vision of digital identify verification services by
13 a Federal, State, local, Tribal, or territorial
14 agency;

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

19 (E) prioritizes technical standards devel-
20 oped by voluntary consensus standards bodies
21 in accordance with section 12(d) of the Na-
22 tional Technology Transfer and Advancement
23 Act of 1995 (15 U.S.C. 272 note) and guidance
24 under OMB Circular A-119 , entitled “Federal
25 Participation in the Development and Use of

1 Voluntary Consensus Standards and in Con-
2 formity Assessment Activities”, or any suc-
3 cessor thereto.

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

8 (6) identify funding or other resources needed
9 to support the agencies described in paragraph (4)
10 that provide digital identity verification, including
11 recommendations with respect to the need for and
12 the design of a Federal grant program to implement
13 the recommendations of the Task Force and facili-
14 tate the development and upgrade of State, local,
15 Tribal, and territorial highly-secure interoperable
16 systems that enable digital identity verification;

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

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

1 tity solutions that support and protect transactions
2 between individuals, government entities, and busi-
3 nesses; and

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

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

10 (B) privacy implications; and

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

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

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

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

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

23 (i) REQUIRED CONSULTATION.—The Task Force
24 shall closely consult with leaders of Federal, State, local,

1 Tribal, and territorial governments and nongovernmental
2 leaders, which shall include the following:

3 (1) The Secretary of Education.

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

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

11 (4) Digital privacy experts.

12 (5) Civil liberties experts.

13 (6) Technology and cybersecurity experts.

14 (7) Users of identity verification services.

15 (8) Representatives with relevant expertise from
16 academia and advocacy organizations.

17 (9) Industry representatives with experience im-
18 plementing digital identity systems.

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

22 (j) REPORTS.—

23 (1) INITIAL REPORT.—Not later than 180 days
24 after the date of enactment of this Act, the Director
25 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) implementing the strategy pursu-
5 ant to subsection (g)(4); and

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

9 (B) summaries of the input and rec-
10 ommendations of the leaders consulted under
11 subsection (i).

12 (2) INTERIM REPORTS.—

13 (A) IN GENERAL.—The Director may sub-
14 mit to the appropriate notification entities in-
15 terim reports the Director determines necessary
16 to support the work of the Task Force and edu-
17 cate the public.

18 (B) MANDATORY REPORT.—Not later than
19 the date that is 18 months after the date of en-
20 actment of this Act, the Director shall submit
21 to the appropriate notification entities an in-
22 terim report addressing—

23 (i) the matters described in para-
24 graphs (1), (2), (4), and (6) of subsection
25 (g); and

1 (ii) any other matters the Director de-
2 termines necessary to support the work of
3 the Task Force and educate the public.

4 (3) FINAL REPORT.—Not later than 180 days
5 before the date described in subsection (k), the Di-
6 rector shall submit to the appropriate notification
7 entities a final report that includes recommendations
8 for the President and Congress relating to any rel-
9 evant matter within the scope of the duties of the
10 Task Force.

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

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

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

20 (a) GUIDANCE FOR FEDERAL AGENCIES.—Not later
21 than 180 days after the date on which the Director sub-
22 mits the report required under section 4(j)(1), the Direc-
23 tor of the Office of Management and Budget shall issue
24 guidance to Federal agencies for the purpose of imple-
25 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 45 days
15 after the date of the issuance of guidance under
16 subsection (a), and annually thereafter, the Di-
17 rector shall develop and make publicly available
18 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;

1 (iii) information relating to the effec-
2 tiveness of digital identity verification serv-
3 ices by Federal agencies; and

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

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

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

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

24 (B) CONSULTATION.—In developing the
25 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 ccurring after the date described in subsection (b)(3)(A),
14 and annually thereafter, the Director of the Office of Man-
15 agement and Budget, in consultation with the Director of
16 the National Institute of Standards and Technology, shall
17 include in the report required under section 3553(c) of
18 title 44, United States Code—

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

21 (2) associated information collection mecha-
22 nisms.

23 **SEC. 6. GAO REPORT.**

24 (a) **IN GENERAL.**—Not later than 1 year after the
25 date of enactment of this Act, the Comptroller General

1 of the United States shall submit to Congress a report
2 on the estimated potential savings, including estimated an-
3 nual potential savings, due to the increased adoption and
4 widespread use of digital identification, of—

5 (1) the Federal Government from averted
6 fraud, including benefit fraud; and

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

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