

Calendar No. 129

118TH CONGRESS
1ST SESSION**S. 884****[Report No. 118–47]**

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

IN THE SENATE OF THE UNITED STATES

MARCH 21, 2023

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

JULY 11, 2023

Reported by Mr. PETERS, with amendments

[Omit the part struck through and insert the part printed in *italie*]**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”.

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 *of the De-*
19 *partment of the Treasury* has stated that the abuse
20 of personally identifiable information and other
21 building blocks of identity is a key enabler behind
22 much of the fraud and cybercrime affecting the
23 United States today.

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

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

3 (6) 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 (7) 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 (8) 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 (9) 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 (10) It should be the policy of the Federal Gov-
10 ernment to use the authorities and capabilities of the
11 Federal Government, in coordination with State,
12 local, Tribal, and territorial partners and private
13 sector innovators, to enhance the security, reliability,
14 privacy, equity, accessibility, and convenience of con-
15 sent-based digital identity solutions that support and
16 protect transactions between individuals, government
17 entities, and businesses, and that enable people in
18 the United States to prove who they are online.

19 **SEC. 3. DEFINITIONS.**

20 In this Act:

21 (1) APPROPRIATE NOTIFICATION ENTITIES.—

22 The term “appropriate notification entities”
23 means—

24 (A) the President;

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

3 (C) the Committee on Oversight and ~~Re-~~
 4 ~~form~~ *Accountability* of the House of Represent-
 5 atives.

6 (2) DIGITAL IDENTITY VERIFICATION.—The
 7 term “digital identity verification” means a process
 8 to verify the identity or an identity attribute of an
 9 individual accessing a service online or through an-
 10 other electronic means.

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

13 (4) FEDERAL AGENCY.—The term “Federal
 14 agency” has the meaning given the term in section
 15 102 of the Robert T. Stafford Disaster Relief and
 16 Emergency Assistance Act (42 U.S.C. 5122).

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

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

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

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

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

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

10 (b) PURPOSE.—The purpose of the Task Force shall
11 be to establish and coordinate a government-wide effort
12 to develop secure methods for Federal, State, local, Tribal,
13 and territorial agencies to improve access and enhance se-
14 curity between physical and digital identity credentials,
15 particularly by promoting the development of digital
16 versions of existing physical identity credentials, including
17 driver’s licenses, e-Passports, social security credentials,
18 and birth certificates, to—

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

21 (2) support reliable, interoperable digital iden-
22 tity verification in the public and private sectors;
23 and

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

- 1 (A) reducing identity theft and fraud;
- 2 (B) enabling trusted transactions; and
- 3 (C) ensuring equitable access to digital
- 4 identity verification.

5 (c) DIRECTOR.—

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

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

10 (3) PAY AND ALLOWANCES.—The Director shall
11 be compensated at the rate of basic pay prescribed
12 for level II of the Executive Schedule under section
13 5313 of title 5, United States Code.

14 (4) QUALIFICATIONS.—The Director shall have
15 substantive technical expertise and managerial acu-
16 men that—

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

20 (B) is gained from not less than 1 organi-
21 zation; and

22 (C) includes specific expertise gained from
23 academia, advocacy organizations, or the pri-
24 vate sector.

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

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

7 (d) MEMBERSHIP.—

8 (1) FEDERAL GOVERNMENT REPRESENTA-
9 TIVES.—The Task Force shall include the following
10 individuals or the designees of such individuals:

11 (A) The Secretary.

12 (B) The Secretary of the Treasury.

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

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

17 (E) The Commissioner of Social Security.

18 (F) The Secretary of State.

19 (G) The Administrator of General Services.

20 (H) The Director of the Office of Manage-
21 ment and Budget.

22 (I) The Postmaster General of the United
23 States Postal Service.

24 (J) The National Cyber Director.

25 (K) The Attorney General.

1 (L) The heads of other Federal agencies or
 2 offices as the President may designate or invite,
 3 as appropriate.

4 (2) STATE, LOCAL, TRIBAL, AND TERRITORIAL
 5 GOVERNMENT REPRESENTATIVES.—The Director
 6 shall appoint to the Task Force 6 State, local, Trib-
 7 al, ~~and~~ *or* territorial government officials who rep-
 8 resent agencies that issue identity credentials and
 9 who have—

10 (A) experience in identity technology and
 11 services;

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

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

17 (3) NONGOVERNMENTAL EXPERTS.—

18 (A) IN GENERAL.—The Director shall ap-
 19 point to the Task Force 5 nongovernmental ex-
 20 perts.

21 (B) SPECIFIC APPOINTMENTS.—The ex-
 22 perts appointed under subparagraph (A) shall
 23 include the following:

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

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

3 (iii) A member who is a technical ex-
4 pert in cybersecurity focusing on identity
5 verification services.

6 (iv) A member who represents the
7 identity verification services industry.

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

11 (e) WORKING GROUPS.—The Director shall organize
12 the members of the Task Force into appropriate working
13 groups for the purpose of increasing the efficiency and ef-
14 fectiveness of the Task Force, as appropriate.

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

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

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

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

22 (1) identify Federal, State, local, Tribal, and
23 territorial agencies that issue identity credentials or
24 hold information relating to identifying an indi-
25 vidual;

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

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

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

11 (A) is secure, protects privacy, and pro-
12 tects individuals against unfair and misleading
13 practices;

14 (B) prioritizes equity and accessibility;

15 (C) requires individual consent for the pro-
16 vision of digital identify verification services by
17 a Federal, State, local, Tribal, or territorial
18 agency;

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

23 (E) prioritizes technical standards devel-
24 oped by voluntary consensus standards bodies
25 in accordance with section 12(d) of the Na-

1 tional Technology Transfer and Advancement
2 Act of 1995 (15 U.S.C. 272 note) and guidance
3 under OMB Circular A-119, entitled “Federal
4 Participation in the Development and Use of
5 Voluntary Consensus Standards and in Con-
6 formity Assessment Activities”, or any suc-
7 cessor thereto;

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

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

21 (7) recommend funding models to provide dig-
22 ital identity verification to private sector entities,
23 which may include fee-based funding models;

24 (8) determine if any additional steps are nec-
25 essary with respect to Federal, State, local, Tribal,

1 and territorial agencies to improve digital identity
2 verification and management processes for the pur-
3 pose of enhancing the security, reliability, privacy,
4 accessibility, equity, and convenience of digital iden-
5 tity solutions that support and protect transactions
6 between individuals, government entities, and busi-
7 nesses; and

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

11 (A) the potential exploitation of digital
12 identity tools or associated products and serv-
13 ices by malign actors;

14 (B) privacy implications; and

15 (C) increasing access to foundational iden-
16 tity documents.

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

19 (1) a single identity credential provided or man-
20 dated by the Federal Government for the purposes
21 of verifying identity or associated attributes;

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

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

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

8 (1) The Secretary of Education.

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

11 (3) State, local, Tribal, and territorial govern-
12 ment officials focused on identity, such as informa-
13 tion technology officials and directors of State de-
14 partments of motor vehicles and vital records bu-
15 reaus.

16 (4) Digital privacy experts.

17 (5) Civil liberties experts.

18 (6) Technology and cybersecurity experts.

19 (7) Users of identity verification services.

20 (8) Representatives with relevant expertise from
21 academia and advocacy organizations.

22 (9) Industry representatives with experience im-
23 plementing digital identity systems.

1 (10) Identity theft and fraud prevention ex-
2 perts, including advocates for victims of identity
3 theft and fraud.

4 (j) REPORTS.—

5 (1) INITIAL REPORT.—Not later than 180 days
6 after the date of enactment of this Act, the Director
7 shall submit to the appropriate notification entities
8 a report on the activities of the Task Force, includ-
9 ing—

10 (A) recommendations on—

11 (i) implementing the strategy pursu-
12 ant to subsection (g)(4); and

13 (ii) methods to leverage digital driv-
14 er's licenses, distributed ledger technology,
15 and other technologies; and

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

19 (2) INTERIM REPORTS.—

20 (A) IN GENERAL.—The Director may sub-
21 mit to the appropriate notification entities in-
22 terim reports the Director determines necessary
23 to support the work of the Task Force and edu-
24 cate the public.

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

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

9 (ii) any other matters the Director de-
10 termines necessary to support the work of
11 the Task Force and educate the public.

12 (3) FINAL REPORT.—Not later than 180 days
13 before the date described in subsection (k), the Di-
14 rector shall submit to the appropriate notification
15 entities a final report that includes recommendations
16 for the President and Congress relating to any rel-
17 evant matter within the scope of the duties of the
18 Task Force.

19 (4) PUBLIC AVAILABILITY.—The Task Force
20 shall make the reports required under this sub-
21 section publicly available on *a* centralized website as
22 an open Government data asset (as defined in sec-
23 tion 3502 of title 44, United States Code).

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

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

5 (a) GUIDANCE FOR FEDERAL AGENCIES.—Not later
 6 than 180 days after the date on which the Director sub-
 7 mits the report required under section 4(j)(1), the Direc-
 8 tor of the Office of Management and Budget shall issue
 9 guidance to Federal agencies for the purpose of imple-
 10 menting any recommendations included in such report de-
 11 termined appropriate by the Director of the Office of Man-
 12 agement and Budget.

13 (b) REPORTS ON FEDERAL AGENCY PROGRESS IM-
 14 PROVING DIGITAL IDENTITY VERIFICATION CAPABILI-
 15 TIES.—

16 (1) ANNUAL REPORT ON GUIDANCE IMPLEMEN-
 17 TATION.—Not later than 1 year after the date of the
 18 issuance of guidance under subsection (a), and an-
 19 nually thereafter, the head of each Federal agency
 20 shall submit to the Director of the Office of Manage-
 21 ment and Budget a report on the efforts of the Fed-
 22 eral agency to implement that guidance.

23 (2) PUBLIC REPORT.—

24 (A) IN GENERAL.—Not later than 45 days
 25 after the date of the issuance of guidance under

1 subsection (a), and annually thereafter, the Di-
2 rector shall develop and make publicly available
3 a report that includes—

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

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

9 (iii) information relating to the effec-
10 tiveness of digital identity verification serv-
11 ices by Federal agencies; and

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

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

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

20 (A) REFORM.—Not later than 180 days
21 after the date of the enactment of this Act, the
22 Director of the Office of Management and
23 Budget, in coordination with the Director of the
24 Cybersecurity and Infrastructure Security
25 Agency, shall submit to the Committee on

1 Homeland Security and Governmental Affairs
2 of the Senate and the Committee on Oversight
3 and ~~Reform~~ *Accountability* of the House of
4 Representatives a report relating to the imple-
5 mentation and effectiveness of the digital iden-
6 tity capabilities of Federal agencies.

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

- 11 (i) consult with the Task Force; and
12 (ii) to the greatest extent practicable,
13 include in the report recommendations of
14 the Task Force.

15 (C) CONTENTS OF REPORT.—The report
16 required under subparagraph (A) shall in-
17 clude—

- 18 (i) an analysis, including metrics and
19 milestones, for the implementation by Fed-
20 eral agencies of—

- 21 (I) the guidelines published by
22 the National Institute of Standards
23 and Technology in the document enti-
24 tled “Special Publication 800–63”
25 (commonly referred to as the “Digital

1 Identity Guidelines”), or any suc-
2 cessor document; and

3 (II) if feasible, any additional re-
4 quirements relating to enhancing dig-
5 ital identity capabilities identified in
6 the document of the Office of Man-
7 agement and Budget entitled “M-19-
8 17” and issued on May 21, 2019, or
9 any successor document;

10 (ii) a review of measures taken to ad-
11 vance the equity, accessibility, cybersecu-
12 rity, and privacy of digital identity
13 verification services offered by Federal
14 agencies; and

15 (iii) any other relevant data, informa-
16 tion, or plans for Federal agencies to im-
17 prove the digital identity capabilities of
18 Federal agencies.

19 (c) ADDITIONAL REPORTS.—On the first March 1 oc-
20 ccurring after the date described in subsection (b)(3)(A),
21 and annually thereafter, the Director of the Office of Man-
22 agement and Budget, in consultation with the Director of
23 the National Institute of Standards and Technology, shall
24 include in the report required under section 3553(c) of
25 title 44, United States Code—

- 1 (1) any additional and ongoing reporting on the
- 2 matters described in subsection (b)(3)(C); and
- 3 (2) associated information collection mecha-
- 4 nisms.

5 **SEC. 6. GAO REPORT.**

6 (a) IN GENERAL.—Not later than 1 year after the

7 date of enactment of this Act, the Comptroller General

8 of the United States shall submit to Congress a report

9 on the estimated potential savings, including estimated an-

10 nual potential savings, due to the increased adoption and

11 widespread use of digital identification, of—

- 12 (1) the Federal Government from averted
- 13 fraud, including benefit fraud; and
- 14 (2) the economy of the United States and con-
- 15 sumers from averted identity theft.

16 (b) CONTENTS.—Among other variables the Comp-

17 troller General of the United States determines relevant,

18 the report required under subsection (a) shall include mul-

19 tiple scenarios with varying uptake rates to demonstrate

20 a range of possible outcomes.

Calendar No. 129

118TH CONGRESS
1ST Session

S. 884

[Report No. 118-47]

A BILL

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

JULY 11, 2023

Reported with amendments