Calendar No. 129

118TH CONGRESS *1st Session*	SENATE	REPORT 118–47

IMPROVING DIGITAL IDENTITY ACT OF 2023

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 884

TO ESTABLISH A GOVERNMENT–WIDE APPROACH TO IMPROVING DIGITAL IDENTITY, AND FOR OTHER PURPOSES

JULY 11, 2023.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
ALEX PADILLA, California	RICK SCOTT, Florida
JON OSSOFF, Georgia	JOSH HAWLEY, Missouri
RICHARD BLUMENTHAL, Connecticut	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
LENA C. CHANG, *Director of Governmental Affairs*
CARTER A. HIRSCHHORN, *Research Assistant*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
ANDREW J. HOPKINS, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 129

118TH CONGRESS *1st Session* | SENATE | REPORT 118–47

IMPROVING DIGITAL IDENTITY ACT OF 2023

JULY 11, 2023.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 884]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 884) to establish a Government-wide approach to improving digital identity, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 884, the *Improving Digital Identity Act of 2023*, would establish an Improving Digital Identity Task Force with intergovernmental, public, and private representatives. The Task Force would coordinate and issue recommendations relating to federal, state, and private-sector efforts to develop and adopt digital identity tools, and ensure federal agencies implement relevant recommendations.[1]

[1] On September 28, 2022, the Committee approved S. 4528, the Improving Digital Identity Act of 2022. That bill, as reported, is substantially similar to S. 884. Accordingly, this committee report is, in many respects, similar to the committee report for S. 4528. *See* S. Rept. 117–238.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Enhancing digital identity across federal, state, and local governments, in coordination with the private sector, to avert fraud, prevent identity theft, and enable individuals to verify their identities online more easily and reliably can result in a more secure online environment.[2] In 2016, the Commission on Enhancing National Cybersecurity, established to strengthen cybersecurity in both the public and private sectors, recommended the creation of an interagency task force to "find secure, user-friendly, privacy centric ways" to validate identity attributes in the broader identity market.[3] Since then, more data breaches have occurred in the country and across the world. Given the scale and frequency of recent data breaches—including successful attacks against consumer credit reporting agencies, financial institutions, telecommunication providers, and government entities—cybercriminals have access to countless Americans' personal identifiers traditionally used to verify identity. Data breaches result in severe financial losses and privacy harms for consumers and facilitate high levels of fraud against governments and private entities alike.[4] In 2022, Javelin Strategy and Research estimated roughly 15.4 million U.S. adults were victims of traditional identity fraud, and Javelin's report estimates this could account for roughly $20 billion in losses of traditional identity fraud.[5] During the COVID–19 pandemic, federal and state benefits programs similarly experienced a surge of fraudulent claims, in large part due to governments' inability to differentiate between authorized and unauthorized uses of individuals' identifying information on online application portals.[6]

Upgrading identity verification technologies and providing individuals with the choice to adopt innovative digital identity tools is critical to tackling these and related challenges.[7] Government entities, as authoritative issuers of identity in the United States, are uniquely positioned to work with the private sector to facilitate this transition. For instance, some states, including Arizona, Arkansas, Colorado, Connecticut, Delaware, Louisiana, Maryland, Mississippi,

---

[2] See, e.g., *Blockchain for digital identity and credentials*, IBM (https://www.ibm.com/blockchain-identity) (accessed May 16, 2023).

[3] Commission on enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Dec. 1, 2016).

[4] See, e.g., *Personal information of members of Congress exposed in health data breach*, NPR (Mar. 11, 2023) (https://www.npr.org/2023/03/09/1162191035/personal-information-of-u-s-house-members-exposed-in-health-data-breach); *Data of 143 million Americans exposed in hack of credit reporting agency Equifax*, Washington Post (Sep. 7, 2017) (https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html); *Data of 40 million plus exposed in latest T-Mobile breach*, AP News (Aug. 18, 2021) (https://apnews.com/article/technology-business-f23cf2ea885f1089571ee45837c81382).

[5] Javelin Strategy and Research, *2023 Identity Fraud Study: The Butterfly Effect* (2023) (https://javelinstrategy.com/research/2023-identity-fraud-study-butterfly-effect). Javelin collects this information in the following way: "Javelin surveys 5,000 U.S. adults, then qualifies each respondent by categorizing each reported loss. Javelin then extrapolates population information from the U.S. Census Bureau, which then permits a best-effort estimation of identity fraud impact across the entire U.S. adult population. It is reasonable to see vast differences in the research findings of various agencies and companies." For example, the Federal Trade Commission's (FTC) Consumer Sentinel Network reported a little more than a million U.S. reports of identity theft in 2022.

[6] See, e.g., *'A magnet for rip-off artists': Fraud siphoned billions from pandemic unemployment benefits*, Washington Post (May 15, 2022) (www.washingtonpost.com/us-policy/2022/05/15/unemployment-pandemic-fraud-identity-theft).

[7] Government Accountability Office, *Data Protection: Agencies need to Strengthen Online Identity Verification Processes* (GAO–19–288) (May 2019); World Economic Forum, Digital Identity Ecosystems: Unlocking New Value (Sept. 2021) (https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf).

Oklahoma, and Utah have begun offering mobile driver's licenses or mobile IDs to citizens, and nine other states are piloting mobile licenses.[8] These licenses can be more secure than physical driver's licenses and create opportunities to improve convenience for citizens.[9] The Transportation Security Administration now accepts mobile driver's licenses at select airport checkpoints.[10] The private and public sectors are continuing to develop promising digital identity verification techniques.[11]

The Task Force this legislation creates also accounts for risks associated with expanding digital identity usage. Risks for expanding digital ID use include potential accessibility concerns, privacy and security violations, and vendor or technology lock-in.[12] For example, the American Civil Liberties Union (ACLU) has highlighted challenges associated with implementing digital driver's licenses, like personal control over ID data, hacker susceptibility, and forced app installation. Among its duties, the bill requires the Task Force to consider potential exploitation of digital identity tools by malign actors, privacy concerns, and ways to improve access to foundational identity documents.[13] Additionally, the bill specifies that the Task Force may not recommend the creation of a single identity credential provided or mandated by the federal government, a unilateral national identification registry, or a requirement forcing any individual to use digital identity verification for a public purpose.[14] Accounting for these types of challenges and risks would allow federal, state, and local governments, and private entities to more successfully introduce digital IDs.

As high-value private transactions and critical government-citizen interactions move online, establishing digital identity standards is essential to ensuring this activity is secure, private, and efficient. A common set of guidelines can ensure mobile forms of identification, as well as digital identity verification processes, are interoperable from a technical perspective, safe from a cybersecurity perspective, and private and equitable from a civil liberties perspective.[15] S. 884 establishes the Improving Digital Identity Task Force, an interagency and public-private partnership, which would develop recommendations on such matters to increase and improve usage of digital identity verification technologies. In addition, the Task Force would ensure that necessary oversight accompanies the deployment of these tools. Task Force recommendations

---

[8] *Which States Offer Mobile Driver's Licenses: An overview of which states have launched electronic IDs, and which are currently piloting mDLs* (https://idscan.net/mobile-drivers-licenses-mdl-state-adoption/) (accessed Apr. 7, 2023).

[9] *Digital driver's licenses take the sting out of forgetting your wallet. Here's how they work*, The Washington Post (Mar. 24, 2022) (https://www.washingtonpost.com/technology/2021/10/11/digital-drivers-license-mdl/).

[10] See, e.g., Transportation Security Administration, *TSA enables Maryland residents to use mobile driver's license or state ID for verification at Baltimore/Washington International and Reagan National Airports* (May, 25, 2022); *Maryland begins issuing digital driver's licenses, ID cards,* The Washington Post (May 25, 2022) (https://www.washingtonpost.com/transportation/2022/05/25/maryland-digital-drivers-licenses/).

[11] See, e.g., *New features from Google make Android phones better wallet replacements*, The Washington Post (June 1, 2023) (https://www.washingtonpost.com/technology/2023/06/01/google-wallet-drivers-license-cards/).

[12] *Creating a good ID system presents risks and challenges, but there are common success factors*, The World Bank (https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors) (accessed May 17, 2023).

[13] Improving Digital Identity Act of 2023, Sec. 4(g)(9).

[14] *Id.*, Sec. (4)(h).

[15] The White House, *National Cybersecurity Strategy* (March 2023).

would aim to help agencies prevent fraud and ensure future protection of citizens' privacy and data.

III. LEGISLATIVE HISTORY

Senator Kyrsten Sinema (I–AZ) introduced S. 884, the *Improving Digital Identity Act*, on March 21, 2023, with original cosponsor Senator Cynthia Lummis (R–WY). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 884 at a business meeting on March 29, 2023. At the business meeting, S. 884 was reported favorably by roll call vote of 11 yeas to 1 nay, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Lankford, Romney, Scott, and Hawley voting in the affirmative, and with Senator Paul voting in the negative. Senators Carper, Johnson, and Marshall voted yea by proxy, for the record only.

Consistent with Committee Rule 3(G), the Committee reports the bill with a technical amendment by mutual agreement of the Chairman and Ranking Member.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section establishes the short title of the bill as the "Improving Digital Identity Act of 2023."

Section 2. Findings

This section discusses the need for the legislation. It highlights the prevalence of identity theft and fraud, and how the inadequacy of current digital identity solutions degrades security and privacy. The section explains how governmental entities are uniquely positioned to work with the private sector and other nongovernmental stakeholders to address deficiencies in our nation's digital identity infrastructure. Finally, this section finds that the Federal government should use its authorities and capabilities to support consent-based digital identity solutions that enable Americans to better prove who they are online and facilitate trusted transactions.

Section 3. Definitions

This section defines the terms "appropriate notification entities," "digital identity verification," "Director," "Federal agency," "identity attribute," "identity credential," "Secretary," and "Task Force."

Section 4. Improving Digital Identity Task Force

Subsection (a) establishes the Improving Digital Identity Task Force within the Executive Office of the President.

Subsection (b) provides that the purpose of the Task Force is to establish and coordinate a government-wide effort to develop enhanced security between physical and digital identity credentials. Developing digital versions of physical credentials, like passports and driver's licenses, can help reduce identity theft, increase trust in digital transactions, and ensure equity across identity verification systems.

Subsection (c) specifies that the Director of the Task Force must be appointed by the President and outlines the Director's required pay, qualifications, and term of service.

Subsection (d) describes that membership of the Task Force shall include the following: (1) Representatives from the following 11 agencies: the Department of Homeland Security, the Department of the Treasury, the National Institute of Standards and Technology, the Financial Crimes Enforcement Network, the Social Security Administration, the Department of State, the General Services Administration, the Office of Management and Budget (OMB), the United States Postal Service, the Office of the National Cyber Director, the Department of Justice, and any other Federal agency determined by the President; (2) six State, local, Tribal, or Territorial members representing agencies that issue identity credentials; and (3) five nongovernmental members with civil liberties, identity verification, and cybersecurity experience and expertise.

Subsections (e) and (f) relate to various administrative matters regarding Task Force meetings. The Director is required to organize members into working groups, and the Task Force must provide opportunities for public comment.

Subsection (g) describes the duties of the Task Force. The Task Force must identify and assess the use of current Federal, State, local, Tribal, and Territorial agencies that use or hold identity credentials. Additionally, the Task Force will put forth several recommendations for agencies, including a strategy proposal for delivering digital identify verification services, principles for promoting shared identity verification across agencies, and funding models to support governmental and non-governmental identity verification systems. The Task Force must also consider matters including the potential exploitation of digital identity tools by malign actors, privacy concerns, and ways to improve access to foundational identity documents.

Subsection (h) ensures that the Task Force respects privacy and civil liberties by specifying that the Task Force may not recommend the creation of a single identity credential provided or mandated by the Federal government, a unilateral national identification registry, or a requirement forcing any individual to use digital identity verification for a public purpose.

Subsection (i) requires the Task Force to consult with the Department of Education, other appropriate Federal entities, State, local, Tribal, and Territorial governments (including departments of motor vehicles and vital records bureaus), digital privacy and civil liberties experts, technology and cybersecurity experts, users of verification services, experts from academia and advocacy organizations, industry representatives, and fraud prevention experts.

Subsection (j) establishes various reporting and publication requirements for the Task Force. The Task Force is required to publish at least three reports, made available to the public on a centralized website. The first report includes an update on the Task Force's activities and recommendations; the second report includes updates on many of the Task Force's duties described in subsection (g); and the final report, occurring after two and a half years, will make recommendations for the President and Congress on matters related to the Task Force.

Subsection (k) specifies that the Task Force must conclude business 3 years after the date of enactment.

Section 5. Security enhancements to Federal systems

Subsection (a) requires the Director of OMB to issue guidance to Federal agencies for the purpose of implementing appropriate recommendations contained in the Task Force's initial report.

Subsection (b) instructs each Federal agency to produce an annual report on its implementation of the guidance required under subsection (a). It further requires OMB to annually publish a report that includes the digital identity verification services offered by Federal agencies, the volume of digital identity verifications performed by each agency, and the effectiveness of Federal digital identity efforts. Additionally, this subsection requires OMB, in consultation with the Cybersecurity and Infrastructure Security Agency, to submit a report to Congress describing Federal agencies' implementation of digital identity capabilities.

Subsection (c) ensures that updates regarding the matters covered by OMB's initial report to Congress are subsequently incorporated into other reports annually required to be submitted to Congress.

Section 6. GAO report

This section instructs the Government Accountability Office to submit a report to Congress estimating the potential savings that would result from the increased adoption and widespread usage of digital identification tools. This report would specifically outline the potential cost savings to the Federal government from averted fraud, including the theft of government benefits, and the savings to the economy of the United States as a whole, including from averted consumer identity theft.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

S. 884, Improving Digital Identity Act of 2023
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 29, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	*	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	*	*	*
Spending Subject to Appropriation (Outlays)	*	4	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2034?	No	Statutory pay-as-you-go procedures apply?	Yes
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 884 would establish a task force to coordinate federal, state, and private-sector efforts to develop digital identity credentials, such as driver's licenses, passports, and birth certificates. The task force would identify best practices and publish guidelines for federal and state agencies to consider when implementing digital identity programs. Under the bill, the task force would submit periodic reports to the Congress on its findings and would terminate three years after enactment. The bill also would require the Office of Management and Budget to issue guidance to federal agencies on implementing digital identity programs and would require the Government Accountability Office to report on the costs and benefits of adopting digital identities.

The task force would consist of representatives from federal agencies, state governments, and private entities. Using information about the cost of similar efforts, CBO estimates that implementing S. 884 would cost $4 million over the 2023–2028 period for staff salaries, travel, and other administrative expenses to operate the task force. CBO also estimates that satisfying the reporting requirements of S. 884 would cost less than $500,000. Such spending would be subject to the availability of appropriated funds.

Enacting the bill could affect direct spending by some federal agencies that are allowed to use fees, receipts from the sale of goods, and other collections to cover operating costs. CBO estimates that any net changes in direct spending by those agencies would be negligible because most of them can adjust amounts collected to reflect changes in operating costs.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Chad Chirico, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation would make no change in existing law, within the meaning of clauses (a) and (b) of subparagraph 12 of rule XXVI of the Standing Rules of the Senate, because this legislation would not repeal or amend any provision of current law.

○