

Calendar No. 616

117TH CONGRESS }
2d Session }

SENATE

{ REPORT
117-238 }

IMPROVING DIGITAL IDENTITY ACT OF 2022

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

TO ACCOMPANY

S. 4528

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



DECEMBER 12, 2022.—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	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*

ZACHARY I. SCHRAM, *Chief Counsel*

LENA C. CHANG, *Director of Governmental Affairs*

MATTHEW T. CORNELIUS, *Senior Professional Staff Member*

PAMELA THIESSEN, *Minority Staff Director*

SAM J. MULOPULOS, *Minority Deputy Staff Director*

CARA G. MUMFORD, *Minority Director of Governmental Affairs*

LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 616

117TH CONGRESS }
2d Session }

SENATE

{ REPORT
{ 117-238

IMPROVING DIGITAL IDENTITY ACT OF 2022

DECEMBER 12, 2022.—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. 4528]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 4528) to establish a Government-wide approach to improving digital identity, and for other purposes, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	1
III. Legislative History	3
IV. Section-by-Section Analysis of the Bill, as Reported	3
V. Evaluation of Regulatory Impact	6
VI. Congressional Budget Office Cost Estimate	6
VII. Changes in Existing Law Made by the Bill, as Reported	7

I. PURPOSE AND SUMMARY

S. 4528, the *Improving Digital Identity Act*, would establish an interagency and public-private Improving Digital Identity Task Force to 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.

II. BACKGROUND AND NEED FOR THE LEGISLATION

There is an urgent need to enhance digital identity efforts across federal, state, and local governments, in coordination with the pri-

vate sector, to avert fraud, prevent identity theft, and enable individuals to more easily and reliably verify their identities online. Given the scale and frequency of recent data breaches, including successful attacks against consumer credit reporting agencies, financial institutions, telecommunication providers, and even government entities, cybercriminals have access to countless Americans' Social Security numbers, driver's license numbers, and other personal identifiers traditionally used to verify identity. This has not only resulted in severe financial losses and privacy harms for individual consumers, but also facilitated unprecedented levels of fraud against governments and private entities alike. In fact, more than 293,000,000 victims were impacted by data breaches in 2021,¹ and losses from identity fraud totaled \$56,000,000,000 in 2020.² As highlighted by recent reports, federal and state benefits programs similarly experienced a surge of fraudulent claims during the COVID-19 pandemic,³ in large part due to governments' inability to differentiate between authorized and unauthorized uses of individuals' identifying information on online application portals.

Upgrading identity verification technologies and providing individuals with the choice to adopt innovative digital identity tools is critical to tackling these and related challenges. 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, Colorado, Delaware, Florida, Iowa, Louisiana, Maryland, Oklahoma, Utah, and Virginia, have already started to issue mobile driver's licenses to citizens who wish to have them. These licenses not only are more secure than physical driver's licenses, but also create opportunities to improve convenience for citizens, as illustrated by the Transportation Security Administration's acceptance of mobile driver's licenses at select airport checkpoints, as well as next-generation approaches to know-your-customer compliance being considered in the financial industry. There are a variety of other promising digital identity verification techniques also being developed in both the private and public sectors.

More broadly, as high-value private transactions and critical government-citizen interactions move online, establishing digital identity standards is essential to ensuring these transactions and interactions are secure, private, and efficient. There must be a common set of guidelines to 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. By establishing an interagency and public-private Improving Digital Identity Task Force to develop recommendations on such matters, the bill will facilitate the increased and improved usage of digital identity verification technologies, while also ensuring the deployment of these tools is accompanied by necessary oversight. By requiring federal agencies to implement appropriate recommendations of the

¹ Identity Theft Resource Center, *2021 Data Breach Report* (Jan. 24, 2022) (www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf).

² Javelin Strategy and Research, *2021 Identity Fraud Study: Shifting Angles* (2021) (<https://javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud>).

³ 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/).

Task Force, the legislation will also save taxpayer money through fraud prevention and ensure that citizens' privacy and data are better protected when the government engages in identity verification.

III. LEGISLATIVE HISTORY

Senator Kyrsten Sinema (D-AZ) introduced S. 4528, the *Improving Digital Identity Act*, on July 13, 2022, with Senator Cynthia Lummis (R-WY). The bill was referred to the Committee on Homeland Security and Governmental Affairs. Companion legislation was previously introduced in the House of Representatives by Representatives Bill Foster (D-IL-11), John Katko (R-NY-24), James Langevin (D-RI-2), and Barry Loudermilk (R-GA-11).

The Committee considered S. 4528 at a business meeting on September 28, 2022. During the business meeting, an amendment in the nature of a substitute was offered by Senator Sinema. This substitute amendment eliminated language establishing a digital identity innovation grant program and authorizing corresponding appropriations. Instead, the Task Force is required to produce the design for such a grant program. The substitute amendment also created a new mandatory interim reporting requirement for the Task Force and made various technical corrections. The substitute amendment was adopted by voice vote *en bloc*. The bill, as amended, was ordered reported favorably by voice vote *en bloc*. Senators present for the vote were Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley.

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

Section 1. Short title

This section designates the name of the bill as the "Improving Digital Identity Act of 2022."

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 further notes that next-generation solutions are needed that improve security, privacy, equity, and accessibility and that governmental entities, as authoritative issuers of identity in the United States, are uniquely positioned to work with the private sector and other nongovernmental stakeholders to deliver critical components that address deficiencies in our nation's digital identity infrastructure. Finally, this section establishes that it should be the policy of the Federal government to use its authorities and capabilities, in coordination with State, local, Tribal, and Territorial partners and the private sector, 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 shall be to establish and coordinate a government-wide effort to develop secure methods for Federal, State, local, Tribal, and Territorial agencies to improve access and enhance security between physical and digital identity credentials, particularly by promoting the development of digital versions of existing physical identity credentials, including driver's licenses, e-Passports, social security credentials, and birth certificates. Through such activities, the Task Force shall enhance privacy and security, reduce identity theft and fraud, enable trusted transactions, and ensure equitable access to digital identity verification.

Subsection (c) specifies that the Director of the Task Force shall be appointed by the President and serve at his pleasure. It further notes that the Director shall be compensated at the rate of basic pay prescribed for level II of the Executive Schedule and have relevant technical expertise and managerial acumen gained from work in the fields of digital identity management, information security, or benefits administration in academia, advocacy organizations, or the private sector. The Director may not hold his or her role concurrent with another Federal appointment and his or her term shall terminate upon conclusion of the Task Force's work.

Subsection (d) describes the membership of the Task Force. Federal members shall include representatives of 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, the United States Postal Service, the Office of the National Cyber Director, and such other Federal agencies or offices as the President determines appropriate. Six State, local, Tribal, or Territorial members shall also be appointed, representing agencies that issue identity credentials. Finally, there shall be five nongovernmental members, including a privacy and civil liberties expert, technical experts in both identity verification and cybersecurity, and representatives of both an identity verification service provider and a party that relies on effective identity management services.

Subsections (e) and (f) relate to various administrative matters. The Task Force shall be organized into appropriate working groups and shall convene at the call of the Director. The Task Force shall further provide an opportunity for public comment.

Subsection (g) describes the duties of the Task Force. The Task Force shall identify Federal, State, local, Tribal, and Territorial agencies that issue identity credentials or hold information relating to identifying an individual; assess restrictions with respect to the abilities of these agencies to verify identity information for other agencies and nongovernmental organizations; and assess any necessary changes in statutes, regulations, or policy to address such restrictions. It shall also create a standards-based architecture to enable agencies to provide services relating to digital identity verification in a way that complies with safeguards to protect private and civil liberties, promotes interoperability, and enhances shared identity

proofing across public sector agencies. Other responsibilities include identifying funding or other resources needed to enhance digital identity verification, including by designing a Federal grant program to implement the recommendations of the Task Force and facilitate the development and upgrade of State, local, Tribal, and Territorial highly-secure interoperable systems that enable digital identity verification, and recommending funding models to provide digital identity verification to private sector entities. Finally, the Task Force shall determine what other additional steps are necessary to improve digital identity verification and assess related matters, including the potential exploitation of digital identity tools by malign actors, privacy concerns, and ways to improve Americans' 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 for the purposes of verifying identity or associated attributes, a unilateral central national identification registry relating to digital identity verification, or a requirement that any individual be forced to use digital identity verification for a given 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. Not later than 180 days after the date of enactment, the Task Force shall submit an initial report describing recommendations, including with respect to the required standards-based architecture and methods to leverage digital driver's licenses, distributed ledger technology, and other technologies, and initial consultations. 18 months after enactment, the Task Force shall submit a mandatory interim report, which must address a number of statutorily prescribed matters, including the standards-based architecture, the proposed design of the grant program for the development and upgrade of State, local, Tribal, and Territorial digital identity verification systems, and existing restrictions inhibiting related agency action. 180 days before the Task Force's sunset date, the Task Force shall submit a final report. The Task Force may also issue additional reports to educate the public, and all reports shall be made publicly available on a centralized website.

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

Section 5. Security enhancements to Federal systems

Subsection (a) requires the Director of the Office of Management and Budget 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 provides that the Office of Management and Budget shall annually make publicly available a report describing the digital identity verification services offered by Federal agencies, the volume of digital identity verifications performed by each Federal agency, the effectiveness of Federal digital identity efforts, and related recommendations. Such reports shall initially be developed in consultation with the Task Force. Furthermore, not later than 180 days after enactment, the Office of Management and Budget, in consultation with the Cybersecurity and Infrastructure Security Agency, shall submit a report to Congress describing Federal agencies' implementation of the guidelines published by the National Institute of Standards and Technology in the document entitled "Special Publication 800-63" (commonly referred to as the "Digital Identity Guidelines") and the Office of Management and Budget memorandum "M-19-17," as well as other measures that have been taken or will be taken to enhance digital identity verification services offered by Federal agencies.

Subsection (c) ensures that updates regarding the matters covered by the Office of Management and Budget'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 describing the estimated 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 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

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 21, 2022.

Hon. GARY C. PETERS,
Chairman, Committee on Homeland Security and Governmental Affairs,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 4528, the Improving Digital Identity Act of 2022.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 4528, Improving Digital Identity Act of 2022			
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on September 28, 2022			
By Fiscal Year, Millions of Dollars	2023	2023-2027	2023-2032
Direct Spending (Outlays)	*	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	*	*	*
Spending Subject to Appropriation (Outlays)	1	4	not estimated
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 2033?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No
* = between zero and \$500,000.			

S. 4528 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 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. 4528 would cost \$4 million over the 2023–2027 period for staff salaries, travel, and other administrative expenses to operate the task force. 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 Leo Lex, Deputy Director of Budget.

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.

