

116TH CONGRESS
2D SESSION

H. R. 8214

To direct the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, to direct the Institute to establish a robust program focusing on driving improvements in America’s cybersecurity posture by creating more robust digital identity management standards and guidelines.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 11, 2020

Mr. FOSTER (for himself and Ms. WEXTON) introduced the following bill;
which was referred to the Committee on Science, Space, and Technology

A BILL

To direct the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, to direct the Institute to establish a robust program focusing on driving improvements in America’s cybersecurity posture by creating more robust digital identity management standards and guidelines.

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 “Strengthening Digital
5 Identity Act of 2020”.

1 **SEC. 2. FINDINGS.**

2 Congress finds the following:

3 (1) NIST's work in identity research and stand-
4 ards is unmatched anywhere in the world, with glob-
5 al standards development organizations like the Fi-
6 nancial Action Task Force (FATF) pointing to
7 NIST guidance in its own standards. Given that ad-
8 versaries continue to exploit weaknesses in digital
9 identity systems to conduct successful cyber-attacks,
10 additional NIST resources are needed to help gov-
11 ernment and industry secure identity in cyberspace.

12 (2) The lack of an easy, affordable, and reliable
13 way for organizations and businesses to identify
14 whether an individual is who they claim to be online
15 creates an attack vector that is widely exploited by
16 adversaries in cyberspace and precludes many high
17 value transactions from being available online.

18 (3) According to the identity theft resource cen-
19 ter, incidents of identity theft and identity fraud
20 continue to rise in the United States, where more
21 than 164,000,000 consumer records containing per-
22 sonally identifiable information were breached in
23 2019, increasing the total number of data breaches
24 by 17 percent from the previous year.

1 (4) According to the Insurance Information In-
2 stitute, in 2018, losses resulting from identity fraud
3 amounted to \$16,800,000,000.

4 (5) The inadequacy of current digital identity
5 solutions degrades security and privacy for all Amer-
6 icans, and next generation solutions are needed that
7 improve both security and privacy.

8 (6) Government entities, as authoritative
9 issuers of identity in the United States, are uniquely
10 positioned to deliver critical components that ad-
11 dress deficiencies in our digital identity infrastruc-
12 ture and augment private sector digital identity and
13 authentication solutions.

14 (7) State governments are particularly well
15 suited to play a role in enhancing digital identity so-
16 lutions used by both the public and private sectors,
17 given the role of State governments as the issuers of
18 driver's licenses and other identity documents com-
19 monly used today.

20 (8) It should be the policy of the Government
21 to use the authorities and capabilities of the Govern-
22 ment to enhance the security, reliability, privacy,
23 and convenience of digital identity solutions that
24 support and protect transactions between individ-

1 uals, government entities, and businesses, and that
2 enable Americans to prove who they are online.

3 **SEC. 3. IDENTITY MANAGEMENT RESEARCH AND DEVELOP-**
4 **MENT.**

5 Section 504 of the Cybersecurity Enhancement Act
6 of 2014 (15 U.S.C. 7464) is amended to read as follows:

7 **“SEC. 504. IDENTITY MANAGEMENT RESEARCH AND DEVEL-**
8 **OPMENT.**

9 “(a) IN GENERAL.—The Director shall continue a
10 program to support the development of voluntary and
11 cost-effective technical standards, metrology, testbeds, and
12 conformance criteria, taking into account appropriate user
13 concerns—

14 “(1) to improve interoperability among identity
15 management technologies;

16 “(2) to strengthen identity proofing and au-
17 thentication methods used in identity management
18 systems;

19 “(3) to improve privacy protection in identity
20 management systems, including health information
21 technology systems, through authentication and se-
22 curity protocols; and

23 “(4) to improve the usability and inclusivity of
24 identity management systems.

1 “(b) UPDATES AND INVESTMENT STRATEGY.—The
2 Director, in consultation with other relevant Federal agen-
3 cies and stakeholders from the private sector, shall develop
4 and implement a comprehensive forward-looking invest-
5 ment strategy for identity management research and de-
6 velopment and standards focused on enabling the use and
7 adoption of modern digital identity solutions that align
8 with the four criteria in section (a). This strategy shall:

9 “(1) Identify where additional funding may be
10 needed to execute all elements of the strategy, both
11 in NIST and potentially in other parts of govern-
12 ment.

13 “(2) Be updated not less than every 2 years
14 with reports to the House Science Committee, Sen-
15 ate Commerce Committee, and House and Senate
16 appropriations committees.

17 “(c) ACTIVITIES.—In carrying out the strategy de-
18 scribed under subsection (a), the Director shall give con-
19 sideration to activities that—

20 “(1) accelerate the development, in collabora-
21 tion with the private sector, of standards that ad-
22 dress interoperability and portability of digital iden-
23 tity solutions;

24 “(2) addresses gaps in current private-sector-
25 led identity management research and development

1 and standards work, both for consumer-focused and
2 enterprise-focused identity management;

3 “(3) advances the development of conformance
4 testing performed by the private sector in support of
5 digital identity standardization;

6 “(4) addresses challenges with inclusivity of ex-
7 isting digital identity and identity management tools;
8 and

9 “(5) support, in consultation with other rel-
10 evant Federal agencies and stakeholders from the
11 private sector, the development of appropriate secu-
12 rity frameworks and reference materials, and the
13 identification of best practices, for use by Federal
14 agencies and the private sector to address security
15 and privacy requirements to enable the use and
16 adoption of digital identity services.”.

17 **SEC. 4. DIGITAL IDENTITY STANDARDS.**

18 (a) ESTABLISHMENT OF A STANDARDS FRAME-
19 WORK.—The Director shall develop a framework of stand-
20 ards, methodologies, procedures, and processes (in this
21 section referred to as the “Framework”) as a guide for
22 Federal, State, and local governments to follow when pro-
23 viding services related to digital identity verification.

24 (b) CONSIDERATION.—In developing the Framework,
25 the Director shall consider—

- 1 (1) methods to protect the privacy of individ-
2 uals;
3 (2) security needs; and
4 (3) the needs of potential end-users and individ-
5 uals that will use services related to digital identity
6 verification.

7 (c) CONSULTATION.—In carrying out subsection the
8 Director shall consult with—

- 9 (1) Federal and State agencies;
10 (2) potential end-users and individuals that will
11 use services related to digital identity verification;
12 and
13 (3) experts with relevant experience in the sys-
14 tems that enable digital identity verification, as de-
15 termined by the Director.

16 (d) INTERIM PUBLICATION.—Not later than 240
17 days after the date of the enactment of this Act, the Direc-
18 tor shall publish an interim version of the Framework.

19 (e) FINAL PUBLICATION.—Not later than 1 year
20 after the date of the enactment of this Act, the Director
21 shall publish a final version of the Framework.

22 (f) UPDATES TO THE FRAMEWORK.—The Director
23 shall, from time to time, update the Framework, with con-
24 sideration given to—

1 (1) feedback from Federal, State, and local
2 agencies that provide services related to digital iden-
3 tity verification; and

4 (2) any technological changes to the systems
5 that enable digital identity verification.

6 (g) AUTHORIZATION OF APPROPRIATIONS.—There is
7 authorized to be appropriated to the Secretary
8 \$10,000,000 for each of fiscal years 2021 through 2025
9 to carry out this Act and the amendments made by this
10 Act.

11 **SEC. 5. DEFINITIONS.**

12 For purposes of this Act:

13 (1) BOT.—The term “Bot” means an autono-
14 mous program on an Internet network that can
15 interact with computer systems or users, especially
16 one designed to respond or behave like a human
17 being.

18 (2) DIGITAL IDENTITY VERIFICATION.—The
19 term “digital identity verification” means a process
20 to verify the identity of an individual accessing a
21 service online.

22 (3) DIRECTOR.—The term “Director” means
23 the Director of the National Institute of Standards
24 and Technology.

1 (4) INSTITUTE.—The term “Institute” means
2 the National Institute of Standards and Technology.

3 (5) SECRETARY.—The term “Secretary” means
4 the Secretary of Commerce.

○