II

117TH CONGRESS
1ST SESSION

S. 2547

To improve the procedures for the authentication and the secure and tamper-evident delivery and transmission of certain court orders.

IN THE SENATE OF THE UNITED STATES

JULY 29, 2021

Mr. WYDEN (for himself, Mr. TILLIS, and Mr. WHITEHOUSE) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To improve the procedures for the authentication and the secure and tamper-evident delivery and transmission of certain court orders.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Digital Authenticity for Court Orders Act of 2021''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) In recent years, criminals have created counterfeit court orders which they have used to

trick telecommunications and technology companies into performing illegal wiretaps and removing online content.

(2) Counterfeit court orders threaten public trust in the courts, and undermine the privacy of the people of the United States and their rights under the First Amendment to the Constitution of the United States.

(3) Secure digital signature technology has existed for decades that solves this problem. Digital signatures enable recipients of a digital document to verify that it was issued by an authorized entity and that it has not been tampered with or modified since it was digitally signed.

(4) Since 1994, the National Institute of Standards and Technology has published Federal Information Processing Standard 186–4, which is the official standard for digital signatures for the Federal Government.

(5) Since 1998, the Government Paperwork Elimination Act (title XVII of division C of Public Law 105–277; 112 Stat. 2681–749) and the amendments made by that Act have required Federal executive branch agencies use digital signatures to conduct official business with the public.

(6) Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), as amended by section 1716 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, requires that subpoenas issued by the Cybersecurity and Infrastructure Security Agency be ''authenticated with a cryptographic digital signature'' and that subpoenas lacking such a digital signature ''shall not be considered to be valid by the recipient of such subpoena''.

(7) The legislative branch has also embraced digital signatures. Every bill posted to congress.gov is digitally signed by the Government Publishing Office.

(8) Federal, State, and Tribal courts have not kept pace with the adoption of digital signature technology by other branches of government.

(9) Illegal wiretaps by their nature involve the interception of private communications that flow over means or instrumentalities of interstate or foreign commerce.

(10) Content and data delivered over the internet is a thing in interstate or foreign commerce. To the extent that a counterfeit court order would result in that content being removed from the internet,

that counterfeit order affects things in interstate and foreign commerce. Congress may therefore take steps to ensure the authenticity of orders purporting to require the removal of online content in interstate or foreign commerce.

(11) Consumers will not continue to do business with telecommunications and technology companies if those companies facilitate surveillance of their private communications or remove their content in response to fraudulent court orders.

(12) The absence of digital signatures from court orders places an unreasonable economic burden on telecommunications and technology companies. These companies must either expend significant effort and resources to manually verify the legitimacy of each court order they receive or bear the risk of significant reputational and financial harm.

(13) The absence of verifiable digital signatures on court orders therefore creates an unreasonable burden on interstate or foreign commerce of the United States, which Congress has the power to remedy.

(14) The adoption of digital signature technology by Federal courts alone will not address the threat of counterfeiting. Criminals have created and

passed off counterfeit State court orders and will continue to do so.

(15) As such, the legitimacy of and public trust in the courts depends upon every court, Federal, State, and Tribal, adopting digital signature technology.

SEC. 3. DEFINITIONS.

In this Act—

(1) the term ''appropriate committees of Congress'' means—

(A) the Committee on the Judiciary and the Committee on Appropriations of the Senate; and

(B) the Committee on the Judiciary and the Committee on Appropriations of the House of Representatives;

(2) the term ''authorized court officer or employee'' means an officer or employee of a Federal, State, or Tribal court that is authorized by the Federal, State, or Tribal court to digitally sign covered orders;

(3) the term ''contains an authentic digital signature'', with respect to a covered order, means that the covered order contains a digital signature—

(A) by an authorized court officer or employee of the Federal, State, or Tribal court issuing the covered order;

(B) that—

(i) complies with the standards certified and promulgated by the Director of the Administrative Office of the United States Courts under section 4(a)(1)(A)(ii); or

(ii) if the Director of the Administrative Office of the United States Courts promulgates updated standards under section 4(a)(1)(B)(ii), on and after the date that is 1 year after the date on which the Director of the Administrative Office of the United States Courts promulgates a set of updated standards, complies with such set of updated standards; and

(C) that confirms that the covered order is authentic;

(4) the term ''covered order'' means an order—

(A) directed to a person other than a party to the proceedings in which the order is entered; and

(B) that is—

(i) an order authorizing or approving the interception of a wire communication, oral communication, or electronic communication under chapter 119 of title 18, United States Code, or under an equivalent State law;

(ii) an order authorizing or approving the installation and use of a pen register or a trap and trace device under chapter 206 of title 18, United States Code, or under an equivalent State law;

(iii) an order for the installation of a mobile tracking device under section 3117 of title 18, United States Code;

(iv) an order for disclosure under chapter 121 of title 18, United States Code;

(v) a search or seizure warrant issued using the procedures described in the Federal Rules of Criminal Procedure or in the case of a State or Tribal court, issued using State or Tribal warrant procedures;

(vi) in the case of a court-martial or other proceeding under chapter 47 of title 10, United States Code (Uniform Code of

Military Justice), a warrant or order issued under section 846 of that title;

(vii) an order under section 1651 of title 28, United States Code;

(viii) an order for third party assistance under section 2518(4) or section 3124 of title 18, United States Code;

(ix) an order to enforce the assistance capability and capacity requirements under section 2522 of title 18, United States Code;

(x) an order under section 2705(b) of title 18, United States Code, prohibiting notifying other persons;

(xi) an order authorizing electronic surveillance issued under section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805);

(xii) an order authorizing a physical search issued under section 304 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824);

(xiii) an order requiring the production of tangible things issued under section

501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861);

(xiv) an order authorizing an acquisition or targeting that is issued under title VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.);

(xv) an order issued under section 512(j) of title 17, United States Code;

(xvi) an order requiring the removal or blocking of content published on the internet;

(xvii) an order that permanently or temporarily seizes a domain name, including by requiring the change of the registrar of record for the domain name or preventing the domain name from resolving to a particular internet protocol address; or

(xviii) any other type of order for which the Judicial Conference of the United States determines that the use of digital signatures would result in increased trust in the courts and reduce the risk and

impact of fraudulent efforts to impersonate court orders;

(5) the term ''digital signature'' has the meaning given the term in section 850.103 of title 5, Code of Federal Regulations, or any successor thereto;

(6) the term ''digital signature technology'' means cryptographic technology that allows a recipient of a covered court order to determine that the covered order—

(A) was issued by a Federal, State, or Tribal court; and

(B) has not been tampered with or modified since it was issued by the court;

(7) the term ''Indian Tribe'' has the meaning given such term in section 102 of the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5130);

(8) the term ''provider'' means an electronic communication service provider, as defined in section 701(b) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881(b));

(9) the term ''State'' means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, American

Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the United States Virgin Islands; and

(10) the term ''Tribal'' means of or pertaining to an Indian Tribe.

SEC. 4. ENSURING AUTHENTICITY AND INTEGRITY OF COURT ORDERS AFFECTING INTERSTATE COMMERCE.

(a) STANDARDIZED TECHNOLOGY FOR DIGITAL SIGNATURES.—

(1) INITIAL STANDARDS.—

(A) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, and in accordance with paragraph (2)—

(i) the Director of the National Institute of Standards and Technology shall develop proposed standards for the use of digital signature technology for covered orders, which shall—

(I) be based on open standards; and

(II) facilitate audits to enable courts to identify whether cryptographic keys, or an equally secure successor technology, used to digitally

authenticate covered orders have been lost, stolen, or misused; and

(ii) on the basis of the proposed standards developed under clause (i), the Director of the Administrative Office of the United States Courts shall certify and promulgate standards for the use of digital signature technology for covered orders.

(B) UPDATING.—In accordance with paragraph (2)—

(i) not later than 5 years after developing proposed standards for the use of digital signature technology for covered orders under subparagraph (A)(i), and every 5 years thereafter, the Director of the National Institute of Standards and Technology shall update such standards; and

(ii) not later than 6 months after receiving standards updated under clause (i), and on the basis of such standards, the Director of the Administrative Office of the United States Courts shall certify and promulgate updated standards for the use of digital signature technology for covered orders.

(2) CONSULTATION.—In developing or updating proposed standards and certifying and promulgating standards under paragraph (1), the Director of the National Institute of Standards and Technology and the Director of the Administrative Office of the United States Courts shall each consult with—

(A) the Attorney General;

(B) the Director of the Cybersecurity and Infrastructure Security Agency;

(C) the Administrator of General Services;

(D) the Director of the Government Publishing Office;

(E) the National Center for State Courts;

(F) the National American Indian Court Judges Association;

(G) independent experts in cybersecurity;

(H) providers;

(I) private entities offering electronic case management software; and

(J) the Archivist of the United States.

(3) IMPLEMENTATION ASSISTANCE.—

(A) DIGITAL SIGNATURE SERVICE.—

(i) IN GENERAL.—Notwithstanding any limitations on the authority of the General Services Administration to provide

services to State or Tribal entities, the Administrator of General Services shall offer a managed digital signature service to each Federal, State, or Tribal court that will allow the court to digitally sign covered orders without the court having to hold and secure the long-term cryptographic keys used to digitally authenticate the covered orders, or an equally secure successor technology.

(ii) CONSULTATION.—The digital signature service offered under clause (i) shall be developed and implemented in consultation with the Administrative Office of United States Courts, the National Center for State Courts, the National American Indian Court Judges Association, the Government Publishing Office, and the Director of the Cybersecurity and Infrastructure Security Agency.

(iii) REQUIREMENTS.—The digital signature service offered under clause (i) shall be designed to—

(I) permit an authorized court officer or employee of a Federal, State,

or Tribal court to digitally sign covered orders from a court office and while teleworking; and

(II) be continuously available for use.

(B) USE.—If a Federal, State, or Tribal court elects to use the managed digital signature service offered under subparagraph (A), the General Services Administration shall provide an online service, available both through a publicly-documented and publicly-available application programming interface and through secure and public websites, that enable authorized court officers and employees to digitally sign a covered order and recipients of a covered order and other third parties to verify that the covered order has a valid digital signature at no cost to the recipient or third party.

(C) NO COST TO COURTS.—The Administrator of General Services shall provide the managed digital signature service to Federal, State, and Tribal courts under this paragraph at no cost to the court.

(D) REIMBURSEMENT.—The Attorney General shall reimburse the Administrator of

General Services for the costs of building, operating, and maintaining the managed digital signature service for Federal, State, and Tribal courts.

(b) DIGITAL SIGNATURE REQUIREMENTS FOR FEDERAL COURT ORDERS.—

(1) IN GENERAL.—

(A) PILOTING THE USE OF DIGITAL SIGNATURES.—Beginning not later than 2 years after the date on which the standards are certified and promulgated by the Director of the Administrative Office of the United States Courts under subsection (a)(1)(A)(ii), not less than 1 district court of the United States in each Federal judicial circuit shall use digital signature technology that complies with the standards to authenticate all covered orders issued by that court.

(B) REQUIRED USE OF DIGITAL SIGNATURE TECHNOLOGY.—

(i) IN GENERAL.—Beginning not later than 4 years after the date on which the standards are certified and promulgated by the Director of the Administrative Office of the United States Courts under sub-

section (a)(1)(A)(ii), each Federal court shall use digital signature technology that complies with the standards to authenticate all covered orders issued by the court.

(ii) UPDATES.—Not later than 1 year after the date on which updated standards are certified and promulgated by the Director of the Administrative Office of the United States Courts under subsection (a)(1)(B)(ii), each Federal court system shall update the digital signature technology used by the court to comply with the updated standards.

(C) PLAN FOR LOSS OR THEFT.—Each Federal court using digital signature technology shall develop, and update not less frequently than every 2 years, a written plan to respond to the loss or theft of the encryption keys, access credentials, or any successor technology used to digitally sign covered orders.

(2) MANDATORY USE OF DIGITAL SIGNATURES.—Except as provided in subsections (d) and (i), on and after the date that is 6 years after the date on which standards are certified and promul-

gated by the Director of the Administrative Office of the United States Courts under subsection (a)(1)(A)(ii), a Federal court may not issue a covered order unless the covered order contains an authentic digital signature.

(c) DIGITAL SIGNATURE REQUIREMENTS FOR STATE AND TRIBAL COURT ORDERS.—

(1) FULL FAITH AND CREDIT REQUIREMENTS.—Section 1738 of title 28, United States Code, is amended—

(A) by inserting ''(a)'' before ''The Acts'';

(B) by inserting ''(b)'' before ''The records'';

(C) by striking ''Such Acts,'' and inserting ''(c)(1) Except as provided in paragraph (2), such Acts,''; and

(D) in subsection (c), as so designated, by adding at the end the following:

''(2)(A) In this paragraph, the terms 'contains an authentic digital signature', 'covered order', 'digital signature', 'State', and 'Tribal' have the meanings given such terms in section 3 of the Digital Authenticity for Court Orders Act of 2021.

''(B) A document purporting to be a covered order issued by a State or Tribal court shall be entitled to full faith and credit only if—

''(i)(I) the document contains an authentic digital signature;

''(II) the document was served with a certificate of authenticity in accordance with section 4(d)(1) of the Digital Authenticity for Court Orders Act of 2021; or

''(III) the document was issued pursuant to a waiver under section 4(d)(2) of the Digital Authenticity for Court Orders Act of 2021; and

''(ii) the State or Tribal court includes with the document a statement certifying that the court has (and has updated on or after the date that is 2 years before the date on which the covered order is issued) a written plan to respond to the loss or theft of the encryption keys, access credentials, or any successor technology used to digitally sign covered orders.''.

(2) WIRETAPPING.—Section 2516(2) of title 18, United States Code, is amended by striking ''The principal prosecuting attorney of any State'' and inserting ''If a State requires that an order described in this subsection issued by the State court

contains an authentic digital signature (as defined in section 3 of the Digital Authenticity for Court Orders Act of 2021), the principal prosecuting attorney of that State''.

(3) STORED COMMUNICATIONS REQUIREMENTS.—Chapter 121 of title 18, United States Code, is amended—

(A) in section 2703, by inserting ''and containing an authentic digital signature (as defined in section 3 of the Digital Authenticity for Court Orders Act of 2021)'' after ''warrant procedures'' each place it appears; and

(B) in section 2711(3)(B), by inserting '', if the court requires that each covered order issued by the court contains an authentic digital signature (as such terms are defined in section 3 of the Digital Authenticity for Court Orders Act of 2021)'' after ''search warrants''.

(4) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 3122(a)(2) of title 18, United States Code, is amended by inserting ''and if the State requires that such an order issued by the State court contains an authentic digital signature (as defined in section 3 of the Digital Authenticity

for Court Orders Act of 2021),'' after ''prohibited by State law,''.

(5) EFFECTIVE DATE.—Except as provided in subsection (i), the amendments made by paragraphs (1) through (4) shall take effect on the date that is 6 years after the date on which the Director of the Administrative Office of the United States Courts certifies and promulgates standards for the use of digital signature technology for covered orders under subsection (a)(1)(A)(ii).

(d) FAILURE OF DIGITAL SIGNATURE TECHNOLOGY.—

(1) INDIVIDUAL COURTS.—If the digital signature technology of a Federal, State, or Tribal court is not operational, upon request by an officer or employee of the Federal, State, or Tribal court who is authorized to digitally sign covered orders, and if the Attorney General determines that a covered court order is authentic, the Attorney General may serve on the provider by personal service the covered court order and a certification stating that the covered court order is authentic.

(2) WIDESPREAD OUTAGE.—

(A) IN GENERAL.—If the digital signature technology of not less than 5 Federal, State, or

Tribal courts is not operational, the Chief Justice of the United States may issue a waiver for a period of not more than 30 days that waives the application of each of the following:

(i) The requirements under subsection (b)(2) with respect to Federal courts.

(ii) The limits on full faith and credit for covered orders issued by State and Tribal courts under paragraph (2) of section 1738(c) of title 28, United States Code, as added by subsection (c) of this section.

(B) RENEWALS.— A waiver described in subparagraph (A) may be renewed for additional periods of not more than 30 days.

(C) NOTICE.—The Chief Justice of the United States shall submit to the appropriate committees of Congress and make publicly available on the website of the Supreme Court of the United States notice of each waiver and renewal of a waiver under this paragraph.

(3) SUBSEQUENT SERVICE OF DIGITALLY SIGNED ORDER BY FEDERAL COURTS.—If a covered order of a Federal, State, or Tribal court is served on a provider under paragraph (1) or pursuant to a

waiver under paragraph (2), after the digital signature technology of the Federal, State, or Tribal court is operational, the party who obtained the initial order shall obtain and serve on the provider an identical covered order that meets the requirements under subsection (b)(2) or paragraph (2) of section 1738(c) of title 28, United States Code, as applicable.

(4) INFORMATION REGARDING FAILURE OF DIGITAL SIGNATURE TECHNOLOGY.—

(A) PUBLIC LIST OF NONOPERATIONAL SYSTEMS.—The Attorney General shall make publicly available on the website of the Department of Justice a list of each Federal, State, or Tribal court for which the digital signature technology is not operational, which shall include—

(i) the period during which the Attorney General approved 1 or more covered court orders of the Federal, State, or Tribal court under paragraph (1); and

(ii) information indicating the measures a provider can take to verify that a covered court order and certification served under paragraph (1) are authentic.

(B) NOTICE TO CONGRESS.—If the digital signature technology of a Federal, State, or Tribal court is not operational for a period of not less than 10 days, the Attorney General shall notify the appropriate committees of Congress.

(e) LIMIT ON IMMUNITY PROVISIONS.—

(1) IN GENERAL.—Except as provided in subsection (i), on and after the date that is 6 years after the date on which the standards are certified and promulgated by the Director of the Administrative Office of the United States Courts under subsection (a)(1)(A)(ii), the provisions of law described in paragraph (2) of this subsection shall only apply with respect to the provision of documents, data, or other information by a provider that removes content or makes available documents, data, or other information in response to a document purporting to be a covered order issued by a Federal, State, or Tribal court if—

(A) the document contains an authentic digital signature;

(B)(i) the document was served with a certificate of authenticity in accordance with subsection (d)(1); and

(ii) the provider—

(I) verified that the court that issued the order is listed on the website of the Department of Justice as having non-operational digital signature technology; and

(II) takes the measures listed by the Attorney General to verify that a covered court order and certification served under subsection (d)(1) are authentic; or

(C) the document was issued pursuant to a waiver under subsection (d)(2).

(2) PROVISIONS OF LAW.—The provisions of law described in this paragraph are the following:

(A) Section 512 of title 17, United States Code.

(B) Section 2520(d)(1) of title 18, United States Code.

(C) Section 2707(e) of title 18, United States Code.

(D) Section 105(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(i)).

(E) Section 402(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842(f)).

(F) Section 702(i)(3) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(i)(3)).

(G) Section 703(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881b(e)).

(H) Title VIII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1885 et seq.).

(f) GRANTS.—The Administrative Office of United States Courts may make grants to State and Tribal courts for the cost of implementing digital signature technology, including to develop and implement training and educational resources, in accordance with this Act.

(g) IMMUNITY.—

(1) IN GENERAL.—Except as provided in subsection (i), on and after the date that is 6 years after the date on which the Director of the Administrative Office of the United States Courts certifies and promulgates standards for the use of digital signature technology for covered orders under subsection (a)(1)(A)(ii), a person may not be held liable

in any Federal, State, or Tribal administrative, civil, or criminal proceeding, including for contempt of court, for failing to comply with a covered order issued by a Federal, State, or Tribal court, respectively, if the covered order does not meet one of the following requirements:

(A) The covered order contains an authentic digital signature.

(B) The covered order was served with a certificate of authenticity in accordance with subsection (d)(1).

(C) The covered order was issued pursuant to a waiver under subsection (d)(2).

(2) COSTS.—In any action brought to enforce compliance with a covered order that, except as provided in subsection (i), was issued on or after the date that is 6 years after the date on which the Director of the Administrative Office of the United States Courts certifies and promulgates standards for the use of digital signature technology for covered orders under subsection (a)(1)(A)(ii), if the court finds that the covered order does not meet the requirements described in subparagraph (A), (B), or (C) of paragraph (1) of this subsection, the court shall award to the person against whom the action

was brought costs of litigation (including reasonable attorney fees).

(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this Act, including for the Administrative Office of United States Courts to make grants under subsection (f) and to upgrade the Case Management/Electronic Case Files System of the Federal Courts.

(i) DELAY OF EFFECTIVE DATE.—The Judicial Conference of the United States may delay the effective dates under subsection (b)(2), subsection (c)(3), subsection (e)(1) and subsection (g) to be the date that is 8 years after the date on which the Director of the Administrative Office of the United States Courts certifies and promulgates standards for the use of digital signature technology for covered orders under subsection (a)(1)(A)(ii).

SEC. 5. PREEMPTION.

This Act and the amendments made by this Act shall preempt any State or Tribal law to the extent that such State law is inconsistent with a provision of this Act or an amendment made by this Act.

SEC. 6. SEVERABILITY.

If any provision of this Act, an amendment made by this Act, or the application of such a provision or amendment to any person or circumstance, is held to be uncon-

stitutional, the remaining provisions of and amendments made by this Act, and the application of the provision or amendment held to be unconstitutional to any other person or circumstance, shall not be affected thereby.

○