

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.

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 “Digital Authenticity  
5 for Court Orders Act of 2021”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

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

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

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

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

15          (4) Since 1994, the National Institute of Stand-  
16      ards and Technology has published Federal Informa-  
17      tion Processing Standard 186-4, which is the official  
18      standard for digital signatures for the Federal Gov-  
19      ernment.

20          (5) Since 1998, the Government Paperwork  
21      Elimination Act (title XVII of division C of Public  
22      Law 105-277; 112 Stat. 2681-749) and the amend-  
23      ments made by that Act have required Federal exec-  
24      utive branch agencies use digital signatures to con-  
25      duct official business with the public.

1           (6) Section 2209 of the Homeland Security Act  
2 of 2002 (6 U.S.C. 659), as amended by section 1716  
3 of the William M. (Mac) Thornberry National De-  
4 fense Authorization Act for Fiscal Year 2021, re-  
5 quires that subpoenas issued by the Cybersecurity  
6 and Infrastructure Security Agency be “authenti-  
7 cated with a cryptographic digital signature” and  
8 that subpoenas lacking such a digital signature  
9 “shall not be considered to be valid by the recipient  
10 of such subpoena”.

11           (7) The legislative branch has also embraced  
12 digital signatures. Every bill posted to congress.gov  
13 is digitally signed by the Government Publishing Of-  
14 fice.

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

18           (9) Illegal wiretaps by their nature involve the  
19 interception of private communications that flow  
20 over means or instrumentalities of interstate or for-  
21 eign commerce.

22           (10) Content and data delivered over the inter-  
23 net is a thing in interstate or foreign commerce. To  
24 the extent that a counterfeit court order would re-  
25 sult in that content being removed from the internet,

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

6 (11) Consumers will not continue to do business  
7 with telecommunications and technology companies  
8 if those companies facilitate surveillance of their pri-  
9 vate communications or remove their content in re-  
10 sponse to fraudulent court orders.

11 (12) The absence of digital signatures from  
12 court orders places an unreasonable economic bur-  
13 den on telecommunications and technology compa-  
14 nies. These companies must either expend significant  
15 effort and resources to manually verify the legit-  
16 imacy of each court order they receive or bear the  
17 risk of significant reputational and financial harm.

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

23 (14) The adoption of digital signature tech-  
24 nology by Federal courts alone will not address the  
25 threat of counterfeiting. Criminals have created and

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

3 (15) As such, the legitimacy of and public trust  
4 in the courts depends upon every court, Federal,  
5 State, and Tribal, adopting digital signature tech-  
6 nology.

7 **SEC. 3. DEFINITIONS.**

8 In this Act—

9 (1) the term “appropriate committees of Con-  
10 gress” means—

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

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

17 (2) the term “authorized court officer or em-  
18 ployee” means an officer or employee of a Federal,  
19 State, or Tribal court that is authorized by the Fed-  
20 eral, State, or Tribal court to digitally sign covered  
21 orders;

22 (3) the term “contains an authentic digital sig-  
23 nature”, with respect to a covered order, means that  
24 the covered order contains a digital signature—

1 (A) by an authorized court officer or em-  
2 ployee of the Federal, State, or Tribal court  
3 issuing the covered order;

4 (B) that—

5 (i) complies with the standards cer-  
6 tified and promulgated by the Director of  
7 the Administrative Office of the United  
8 States Courts under section 4(a)(1)(A)(ii);  
9 or

10 (ii) if the Director of the Administra-  
11 tive Office of the United States Courts  
12 promulgates updated standards under sec-  
13 tion 4(a)(1)(B)(ii), on and after the date  
14 that is 1 year after the date on which the  
15 Director of the Administrative Office of  
16 the United States Courts promulgates a  
17 set of updated standards, complies with  
18 such set of updated standards; and

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

21 (4) the term “covered order” means an order—

22 (A) directed to a person other than a party  
23 to the proceedings in which the order is en-  
24 tered; and

25 (B) that is—

1 (i) an order authorizing or approving  
2 the interception of a wire communication,  
3 oral communication, or electronic commu-  
4 nication under chapter 119 of title 18,  
5 United States Code, or under an equivalent  
6 State law;

7 (ii) an order authorizing or approving  
8 the installation and use of a pen register  
9 or a trap and trace device under chapter  
10 206 of title 18, United States Code, or  
11 under an equivalent State law;

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

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

18 (v) a search or seizure warrant issued  
19 using the procedures described in the Fed-  
20 eral Rules of Criminal Procedure or in the  
21 case of a State or Tribal court, issued  
22 using State or Tribal warrant procedures;

23 (vi) in the case of a court-martial or  
24 other proceeding under chapter 47 of title  
25 10, United States Code (Uniform Code of

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

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

5 (viii) an order for third party assist-  
6 ance under section 2518(4) or section  
7 3124 of title 18, United States Code;

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

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

15 (xi) an order authorizing electronic  
16 surveillance issued under section 105 of  
17 the Foreign Intelligence Surveillance Act of  
18 1978 (50 U.S.C. 1805);

19 (xii) an order authorizing a physical  
20 search issued under section 304 of the  
21 Foreign Intelligence Surveillance Act of  
22 1978 (50 U.S.C. 1824);

23 (xiii) an order requiring the produc-  
24 tion of tangible things issued under section



1           501 of the Foreign Intelligence Surveil-  
2           lance Act of 1978 (50 U.S.C. 1861);

3           (xiv) an order authorizing an acquisi-  
4           tion or targeting that is issued under title  
5           VII of the Foreign Intelligence Surveil-  
6           lance Act of 1978 (50 U.S.C. 1881 et  
7           seq.);

8           (xv) an order issued under section  
9           512(j) of title 17, United States Code;

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

13          (xvii) an order that permanently or  
14          temporarily seizes a domain name, includ-  
15          ing by requiring the change of the reg-  
16          istrar of record for the domain name or  
17          preventing the domain name from resolv-  
18          ing to a particular internet protocol ad-  
19          dress; or

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

1                   impact of fraudulent efforts to impersonate  
2                   court orders;

3                   (5) the term “digital signature” has the mean-  
4                   ing given the term in section 850.103 of title 5,  
5                   Code of Federal Regulations, or any successor there-  
6                   to;

7                   (6) the term “digital signature technology”  
8                   means cryptographic technology that allows a recipi-  
9                   ent of a covered court order to determine that the  
10                  covered order—

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

13                  (B) has not been tampered with or modi-  
14                  fied since it was issued by the court;

15                  (7) the term “Indian Tribe” has the meaning  
16                  given such term in section 102 of the Federally Rec-  
17                  ognized Indian Tribe List Act of 1994 (25 U.S.C.  
18                  5130);

19                  (8) the term “provider” means an electronic  
20                  communication service provider, as defined in section  
21                  701(b) of the Foreign Intelligence Surveillance Act  
22                  of 1978 (50 U.S.C. 1881(b));

23                  (9) the term “State” means each of the several  
24                  States of the United States, the District of Colum-  
25                  bia, the Commonwealth of Puerto Rico, American

1 Samoa, the Commonwealth of the Northern Mariana  
2 Islands, Guam, and the United States Virgin Is-  
3 lands; and

4 (10) the term “Tribal” means of or pertaining  
5 to an Indian Tribe.

6 **SEC. 4. ENSURING AUTHENTICITY AND INTEGRITY OF**  
7 **COURT ORDERS AFFECTING INTERSTATE**  
8 **COMMERCE.**

9 (a) STANDARDIZED TECHNOLOGY FOR DIGITAL SIG-  
10 NATURES.—

11 (1) INITIAL STANDARDS.—

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

15 (i) the Director of the National Insti-  
16 tute of Standards and Technology shall de-  
17 velop proposed standards for the use of  
18 digital signature technology for covered or-  
19 ders, which shall—

20 (I) be based on open standards;  
21 and

22 (II) facilitate audits to enable  
23 courts to identify whether cryp-  
24 tographic keys, or an equally secure  
25 successor technology, used to digitally

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

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

9           (B) UPDATING.—In accordance with para-  
10          graph (2)—

11           (i) not later than 5 years after devel-  
12           oping proposed standards for the use of  
13           digital signature technology for covered or-  
14           ders under subparagraph (A)(i), and every  
15           5 years thereafter, the Director of the Na-  
16           tional Institute of Standards and Tech-  
17           nology shall update such standards; and

18           (ii) not later than 6 months after re-  
19           ceiving standards updated under clause (i),  
20           and on the basis of such standards, the Di-  
21           rector of the Administrative Office of the  
22           United States Courts shall certify and pro-  
23           mulgate updated standards for the use of  
24           digital signature technology for covered or-  
25           ders.

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

7                   (A) the Attorney General;

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

10                  (C) the Administrator of General Services;

11                  (D) the Director of the Government Pub-  
12 lishing Office;

13                  (E) the National Center for State Courts;

14                  (F) the National American Indian Court  
15 Judges Association;

16                  (G) independent experts in cybersecurity;

17                  (H) providers;

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

20                  (J) the Archivist of the United States.

21           (3) IMPLEMENTATION ASSISTANCE.—

22                   (A) DIGITAL SIGNATURE SERVICE.—

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

1 services to State or Tribal entities, the Ad-  
2 ministrators of General Services shall offer  
3 a managed digital signature service to each  
4 Federal, State, or Tribal court that will  
5 allow the court to digitally sign covered or-  
6 ders without the court having to hold and  
7 secure the long-term cryptographic keys  
8 used to digitally authenticate the covered  
9 orders, or an equally secure successor tech-  
10 nology.

11 (ii) CONSULTATION.—The digital sig-  
12 nature service offered under clause (i) shall  
13 be developed and implemented in consulta-  
14 tion with the Administrative Office of  
15 United States Courts, the National Center  
16 for State Courts, the National American  
17 Indian Court Judges Association, the Gov-  
18 ernment Publishing Office, and the Direc-  
19 tor of the Cybersecurity and Infrastructure  
20 Security Agency.

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

24 (I) permit an authorized court of-  
25 ficer or employee of a Federal, State,

1 or Tribal court to digitally sign cov-  
2 ered orders from a court office and  
3 while teleworking; and

4 (II) be continuously available for  
5 use.

6 (B) USE.—If a Federal, State, or Tribal  
7 court elects to use the managed digital signa-  
8 ture service offered under subparagraph (A),  
9 the General Services Administration shall pro-  
10 vide an online service, available both through a  
11 publicly-documented and publicly-available ap-  
12 plication programming interface and through  
13 secure and public websites, that enable author-  
14 ized court officers and employees to digitally  
15 sign a covered order and recipients of a covered  
16 order and other third parties to verify that the  
17 covered order has a valid digital signature at no  
18 cost to the recipient or third party.

19 (C) NO COST TO COURTS.—The Adminis-  
20 trator of General Services shall provide the  
21 managed digital signature service to Federal,  
22 State, and Tribal courts under this paragraph  
23 at no cost to the court.

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

1 General Services for the costs of building, oper-  
2 ating, and maintaining the managed digital sig-  
3 nature service for Federal, State, and Tribal  
4 courts.

5 (b) DIGITAL SIGNATURE REQUIREMENTS FOR FED-  
6 ERAL COURT ORDERS.—

7 (1) IN GENERAL.—

8 (A) PILOTING THE USE OF DIGITAL SIGNA-  
9 TURES.—Beginning not later than 2 years after  
10 the date on which the standards are certified  
11 and promulgated by the Director of the Admin-  
12 istrative Office of the United States Courts  
13 under subsection (a)(1)(A)(ii), not less than 1  
14 district court of the United States in each Fed-  
15 eral judicial circuit shall use digital signature  
16 technology that complies with the standards to  
17 authenticate all covered orders issued by that  
18 court.

19 (B) REQUIRED USE OF DIGITAL SIGNA-  
20 TURE TECHNOLOGY.—

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



1 section (a)(1)(A)(ii), each Federal court  
2 shall use digital signature technology that  
3 complies with the standards to authen-  
4 ticate all covered orders issued by the  
5 court.

6 (ii) UPDATES.—Not later than 1 year  
7 after the date on which updated standards  
8 are certified and promulgated by the Di-  
9 rector of the Administrative Office of the  
10 United States Courts under subsection  
11 (a)(1)(B)(ii), each Federal court system  
12 shall update the digital signature tech-  
13 nology used by the court to comply with  
14 the updated standards.

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

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

1 gated by the Director of the Administrative Office of  
 2 the United States Courts under subsection  
 3 (a)(1)(A)(ii), a Federal court may not issue a cov-  
 4 ered order unless the covered order contains an au-  
 5 thentic digital signature.

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

8 (1) FULL FAITH AND CREDIT REQUIRE-  
 9 MENTS.—Section 1738 of title 28, United States  
 10 Code, is amended—

11 (A) by inserting “(a)” before “The Acts”;

12 (B) by inserting “(b)” before “The  
 13 records”;

14 (C) by striking “Such Acts,” and inserting  
 15 “(c)(1) Except as provided in paragraph (2),  
 16 such Acts,”; and

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

19 “(2)(A) In this paragraph, the terms ‘contains an au-  
 20 thentic digital signature’, ‘covered order’, ‘digital signa-  
 21 ture’, ‘State’, and ‘Tribal’ have the meanings given such  
 22 terms in section 3 of the Digital Authenticity for Court  
 23 Orders Act of 2021.

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

4 “(i)(I) the document contains an authentic dig-  
5 ital signature;

6 “(II) the document was served with a certificate  
7 of authenticity in accordance with section 4(d)(1) of  
8 the Digital Authenticity for Court Orders Act of  
9 2021; or

10 “(III) the document was issued pursuant to a  
11 waiver under section 4(d)(2) of the Digital Authen-  
12 ticity for Court Orders Act of 2021; and

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

21 (2) WIRETAPPING.—Section 2516(2) of title  
22 18, United States Code, is amended by striking  
23 “The principal prosecuting attorney of any State”  
24 and inserting “If a State requires that an order de-  
25 scribed in this subsection issued by the State court

1 contains an authentic digital signature (as defined in  
2 section 3 of the Digital Authenticity for Court Or-  
3 ders Act of 2021), the principal prosecuting attorney  
4 of that State”.

5 (3) STORED COMMUNICATIONS REQUIRE-  
6 MENTS.—Chapter 121 of title 18, United States  
7 Code, is amended—

8 (A) in section 2703, by inserting “and con-  
9 taining an authentic digital signature (as de-  
10 fined in section 3 of the Digital Authenticity for  
11 Court Orders Act of 2021)” after “warrant pro-  
12 cedures” each place it appears; and

13 (B) in section 2711(3)(B), by inserting “,  
14 if the court requires that each covered order  
15 issued by the court contains an authentic digital  
16 signature (as such terms are defined in section  
17 3 of the Digital Authenticity for Court Orders  
18 Act of 2021)” after “search warrants”.

19 (4) PEN REGISTERS AND TRAP AND TRACE DE-  
20 VICES.—Section 3122(a)(2) of title 18, United  
21 States Code, is amended by inserting “and if the  
22 State requires that such an order issued by the  
23 State court contains an authentic digital signature  
24 (as defined in section 3 of the Digital Authenticity

1 for Court Orders Act of 2021),” after “prohibited by  
2 State law,”.

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

11 (d) FAILURE OF DIGITAL SIGNATURE TECH-  
12 NOLOGY.—

13 (1) INDIVIDUAL COURTS.—If the digital signa-  
14 ture technology of a Federal, State, or Tribal court  
15 is not operational, upon request by an officer or em-  
16 ployee of the Federal, State, or Tribal court who is  
17 authorized to digitally sign covered orders, and if the  
18 Attorney General determines that a covered court  
19 order is authentic, the Attorney General may serve  
20 on the provider by personal service the covered court  
21 order and a certification stating that the covered  
22 court order is authentic.

23 (2) WIDESPREAD OUTAGE.—

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

1 Tribal courts is not operational, the Chief Jus-  
2 tice of the United States may issue a waiver for  
3 a period of not more than 30 days that waives  
4 the application of each of the following:

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

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

13 (B) RENEWALS.— A waiver described in  
14 subparagraph (A) may be renewed for addi-  
15 tional periods of not more than 30 days.

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

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

1 waiver under paragraph (2), after the digital signa-  
2 ture technology of the Federal, State, or Tribal  
3 court is operational, the party who obtained the ini-  
4 tial order shall obtain and serve on the provider an  
5 identical covered order that meets the requirements  
6 under subsection (b)(2) or paragraph (2) of section  
7 1738(e) of title 28, United States Code, as applica-  
8 ble.

9 (4) INFORMATION REGARDING FAILURE OF DIG-  
10 ITAL SIGNATURE TECHNOLOGY.—

11 (A) PUBLIC LIST OF NONOPERATIONAL  
12 SYSTEMS.—The Attorney General shall make  
13 publicly available on the website of the Depart-  
14 ment of Justice a list of each Federal, State, or  
15 Tribal court for which the digital signature  
16 technology is not operational, which shall in-  
17 clude—

18 (i) the period during which the Attor-  
19 ney General approved 1 or more covered  
20 court orders of the Federal, State, or Trib-  
21 al court under paragraph (1); and

22 (ii) information indicating the meas-  
23 ures a provider can take to verify that a  
24 covered court order and certification served  
25 under paragraph (1) are authentic.

1           (B) NOTICE TO CONGRESS.—If the digital  
2           signature technology of a Federal, State, or  
3           Tribal court is not operational for a period of  
4           not less than 10 days, the Attorney General  
5           shall notify the appropriate committees of Con-  
6           gress.

7           (e) LIMIT ON IMMUNITY PROVISIONS.—

8           (1) IN GENERAL.—Except as provided in sub-  
9           section (i), on and after the date that is 6 years  
10          after the date on which the standards are certified  
11          and promulgated by the Director of the Administra-  
12          tive Office of the United States Courts under sub-  
13          section (a)(1)(A)(ii), the provisions of law described  
14          in paragraph (2) of this subsection shall only apply  
15          with respect to the provision of documents, data, or  
16          other information by a provider that removes con-  
17          tent or makes available documents, data, or other in-  
18          formation in response to a document purporting to  
19          be a covered order issued by a Federal, State, or  
20          Tribal court if—

21                 (A) the document contains an authentic  
22                 digital signature;

23                 (B)(i) the document was served with a cer-  
24                 tificate of authenticity in accordance with sub-  
25                 section (d)(1); and



1 (ii) the provider—

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

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

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

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

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

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

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

21 (D) Section 105(i) of the Foreign Intel-  
22 ligence Surveillance Act of 1978 (50 U.S.C.  
23 1805(i)).

1           (E) Section 402(f) of the Foreign Intel-  
2           ligence Surveillance Act of 1978 (50 U.S.C.  
3           1842(f)).

4           (F) Section 702(i)(3) of the Foreign Intel-  
5           ligence Surveillance Act of 1978 (50 U.S.C.  
6           1881a(i)(3)).

7           (G) Section 703(e) of the Foreign Intel-  
8           ligence Surveillance Act of 1978 (50 U.S.C.  
9           1881b(e)).

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

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

18          (g) IMMUNITY.—

19           (1) IN GENERAL.—Except as provided in sub-  
20          section (i), on and after the date that is 6 years  
21          after the date on which the Director of the Adminis-  
22          trative Office of the United States Courts certifies  
23          and promulgates standards for the use of digital sig-  
24          nature technology for covered orders under sub-  
25          section (a)(1)(A)(ii), a person may not be held liable

1 in any Federal, State, or Tribal administrative, civil,  
2 or criminal proceeding, including for contempt of  
3 court, for failing to comply with a covered order  
4 issued by a Federal, State, or Tribal court, respec-  
5 tively, if the covered order does not meet one of the  
6 following requirements:

7 (A) The covered order contains an authen-  
8 tic digital signature.

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

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

14 (2) COSTS.—In any action brought to enforce  
15 compliance with a covered order that, except as pro-  
16 vided in subsection (i), was issued on or after the  
17 date that is 6 years after the date on which the Di-  
18 rector of the Administrative Office of the United  
19 States Courts certifies and promulgates standards  
20 for the use of digital signature technology for cov-  
21 ered orders under subsection (a)(1)(A)(ii), if the  
22 court finds that the covered order does not meet the  
23 requirements described in subparagraph (A), (B), or  
24 (C) of paragraph (1) of this subsection, the court  
25 shall award to the person against whom the action

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

3 (h) AUTHORIZATION OF APPROPRIATIONS.—There  
4 are authorized to be appropriated such sums as are nec-  
5 essary to carry out this Act, including for the Administra-  
6 tive Office of United States Courts to make grants under  
7 subsection (f) and to upgrade the Case Management/Elec-  
8 tronic Case Files System of the Federal Courts.

9 (i) DELAY OF EFFECTIVE DATE.—The Judicial Con-  
10 ference of the United States may delay the effective dates  
11 under subsection (b)(2), subsection (c)(3), subsection  
12 (e)(1) and subsection (g) to be the date that is 8 years  
13 after the date on which the Director of the Administrative  
14 Office of the United States Courts certifies and promul-  
15 gates standards for the use of digital signature technology  
16 for covered orders under subsection (a)(1)(A)(ii).

17 **SEC. 5. PREEMPTION.**

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

22 **SEC. 6. SEVERABILITY.**

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

1 stitutional, the remaining provisions of and amendments  
2 made by this Act, and the application of the provision or  
3 amendment held to be unconstitutional to any other per-  
4 son or circumstance, shall not be affected thereby.

○