

118TH CONGRESS  
2D SESSION

**S.** \_\_\_\_\_

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

---

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

---

**A BILL**

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the  
5 “Health Infrastructure Security and Accountability Act of  
6 2024”.

7 (b) TABLE OF CONTENTS.—The table of contents for  
8 this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I-STRENGTHENING AND INCREASING OVERSIGHT OF, AND  
COMPLIANCE WITH, SECURITY STANDARDS FOR HEALTH IN-  
FORMATION

Sec. 101. Security requirements.

Sec. 102. Security risk management, reporting requirements, and audits for  
covered entities and business associates.

Sec. 103. Increased civil penalties for failure to comply with security standards  
and requirements for health information.

Sec. 104. User fee to support data security oversight and enforcement activi-  
ties.

TITLE II-MEDICARE ASSISTANCE TO ADDRESS CYBERSECURITY  
INCIDENTS

201. Medicare safe cybersecurity practices adoption program for eligible hos-  
pitals and critical access hospitals.

202. Medicare accelerated and advanced payments in response to cybersecurity  
incidents.

1 **TITLE I—STRENGTHENING AND**  
2 **INCREASING OVERSIGHT OF,**  
3 **AND COMPLIANCE WITH, SE-**  
4 **CURITY STANDARDS FOR**  
5 **HEALTH INFORMATION**

6 **SEC. 101. SECURITY REQUIREMENTS.**

7 (a) IN GENERAL.—Section 1173(d)(1) of the Social  
8 Security Act (42 U.S.C. 1320d–2(d)(1)) is amended—

9 (1) in subparagraph (A), by redesignating  
10 clauses (i) through (v) as subclauses (I) through (V)  
11 respectively and indenting appropriately;

12 (2) by redesignating subparagraphs (A) and  
13 (B) as clauses (i) and (ii) respectively and indenting  
14 appropriately;

1           (3) by striking “SECURITY STANDARDS.—The  
2     Secretary” and inserting the following: “MINIMUM  
3     SECURITY STANDARDS.—

4                     “(A) IN GENERAL.—The Secretary”;

5           (4) in subparagraph (A), as added by para-  
6     graph (3)—

7                     (A) in clause (i)(V), by striking “and” at  
8     the end;

9                     (B) in clause (ii), by striking the period at  
10    the end and inserting “; and”; and

11                    (C) by adding at the end the following new  
12    clause:

13                             “(iii) include minimum and enhanced  
14                             security requirements adopted under sub-  
15                             paragraph (B)”;

16           (5) by adding at the end the following new sub-  
17     paragraph:

18                             “(B) MINIMUM AND ENHANCED SECURITY  
19     REQUIREMENTS.—

20                             “(i) ADOPTION.—Subject to clauses  
21                             (iii) and (iv), in order to protect health in-  
22                             formation, protect patient safety, and en-  
23                             sure the availability and resiliency of  
24                             health care information systems and health

1 care transactions, the Secretary shall  
2 adopt—

3 “(I) minimum security require-  
4 ments for covered entities and busi-  
5 ness associates; and

6 “(II) enhanced security require-  
7 ments for covered entities and busi-  
8 ness associates that—

9 “(aa) are of systemic impor-  
10 tance, as determined by the Sec-  
11 retary; or

12 “(bb) are important to na-  
13 tional security, as determined by  
14 the Secretary, in consultation  
15 with the Director of Cybersecu-  
16 rity and Infrastructure Security  
17 Agency and the Director of Na-  
18 tional Intelligence.

19 “(ii) APPLICATION OF ENHANCED SE-  
20 CURITY REQUIREMENTS.—

21 “(I) NOTIFICATION.—The Sec-  
22 retary shall, at a time and in a man-  
23 ner determined appropriate by the  
24 Secretary, notify each covered entity  
25 and business associate that is subject

1 to the enhanced security requirements  
2 under clause (i)(II).

3 “(II) LIMITATION ON REVIEW.—

4 There shall be no administrative or  
5 judicial review under section 1869,  
6 1878, or otherwise of the methodology  
7 the Secretary uses to determine  
8 whether a covered entity or business  
9 associate is subject to the enhanced  
10 security requirements under clause  
11 (i)(II).

12 “(iii) FACTORS.—In addition to the  
13 factors described in subparagraph (A)(i),  
14 in developing—

15 “(I) the minimum security re-  
16 quirements under clause (i)(I), the  
17 Secretary shall, in consultation with  
18 the Director of Cybersecurity and In-  
19 frastructure Security Agency and the  
20 Director of National Intelligence, de-  
21 sign the requirements to prevent—

22 “(aa) cyber incidents uti-  
23 lizing the tools and strategies  
24 used to target covered entities or  
25 business associates;

1                   “(bb) the potential harms,  
2                   as defined by the Secretary, to  
3                   national security that could re-  
4                   sult from a cyber incident involv-  
5                   ing a covered entity or business  
6                   associate;

7                   “(cc) the potential harms, as  
8                   defined by the Secretary, to pa-  
9                   tients that could result from a  
10                  cyber incident involving a covered  
11                  entity or business associate; and

12                  “(dd) other potential harms  
13                  from cyber incidents, as deter-  
14                  mined appropriate by the Sec-  
15                  retary; and

16                  “(II) the enhanced security re-  
17                  quirements under clause (i)(II), the  
18                  Secretary shall, in consultation with  
19                  the Director of the Cybersecurity and  
20                  Infrastructure Security Agency and  
21                  the Director of National Intelligence,  
22                  design the requirements to prevent  
23                  the potential harms described in sub-  
24                  clause (I) and protect against the spe-  
25                  cific threats the covered entities and

1 business associates described in such  
2 clause face.

3 “(iv) REVIEW AND UPDATE OF RE-  
4 QUIREMENTS.—The Secretary shall review  
5 and update the minimum and enhanced se-  
6 curity requirements adopted under clause  
7 (i) not less frequently than every 2 years.

8 “(v) EFFECTIVE DATE AND RULE-  
9 MAKING.—

10 “(I) EFFECTIVE DATE.—The re-  
11 quirements under this subparagraph  
12 shall take effect on the date that is 2  
13 years after the date of enactment of  
14 this subparagraph.

15 “(II) RULEMAKING.—Not later  
16 than 18 months after the date of en-  
17 actment of this subparagraph, the  
18 Secretary shall promulgate regulations  
19 to carry out this subparagraph.

20 “(vi) DEFINITIONS.—For purposes of  
21 this subsection:

22 “(I) BUSINESS ASSOCIATE.—The  
23 term ‘business associate’ has the  
24 meaning given such term in section  
25 160.103 of title 45, Code of Federal

1 Regulations (or a successor regula-  
2 tion).

3 “(II) COVERED ENTITY.—The  
4 term ‘covered entity’ has the meaning  
5 given that term in section 160.103 of  
6 title 45, Code of Federal Regulations  
7 (or a successor regulation).

8 “(III) SYSTEMIC IMPORTANCE.—  
9 The term ‘systemic importance’  
10 means, with respect to a covered enti-  
11 ty or business associate, that the fail-  
12 ure of, or a disruption to, such entity  
13 or associate would have a debilitating  
14 impact on access to health care or the  
15 stability of the health care system of  
16 the United States (as determined by  
17 the Secretary).”.

18 (b) AVAILABILITY OF HEALTH INFORMATION.—Sec-  
19 tion 1173(d)(2)(A) of the Social Security Act (42 U.S.C.  
20 1320d–2(d)(2)(A)) is amended by striking “the integrity  
21 and confidentiality” and inserting “the availability, integ-  
22 rity, and confidentiality.



1 **SEC. 102. SECURITY RISK MANAGEMENT, REPORTING RE-**  
2 **QUIREMENTS, AND AUDITS FOR COVERED**  
3 **ENTITIES AND BUSINESS ASSOCIATES.**

4 (a) SECURITY RISK MANAGEMENT AND REPORT-  
5 ING.—Section 1173(d) of the Social Security Act (42  
6 U.S.C. 1320d–2(d)) is amended by adding at the end the  
7 following new paragraph:

8 “(3) SECURITY RISK MANAGEMENT AND RE-  
9 PORTING.—

10 “(A) IN GENERAL.—Each covered entity  
11 and business associate shall at a minimum, on  
12 an annual basis—

13 “(i) conduct and document a security  
14 risk analysis, including information regard-  
15 ing the manner and extent to which such  
16 entity or associate is exposed to risk  
17 through its business associates;

18 “(ii) document a plan for a rapid and  
19 orderly resolution in the event of a natural  
20 disaster, disruptive cyber incident, or other  
21 technological failure to its information sys-  
22 tems or those of its business associates;

23 “(iii) conduct a stress test to evaluate  
24 whether such entity or associate has the  
25 capabilities and planning necessary to re-  
26 cover essential functions, such as patient

1 care operations and transactions described  
2 in subsection (a)(2), following a cyber inci-  
3 dent, a natural disaster, or other substan-  
4 tial threat to health care operations, as de-  
5 termined by the Secretary;

6 “(iv) document whether, based upon  
7 the results of the stress test described in  
8 clause (iii), the covered entity or business  
9 associate revised the most recent plan de-  
10 scribed in clause (ii);

11 “(v) provide a written statement  
12 signed by the chief executive officer and  
13 chief information security officer (or equiv-  
14 alent thereof) stating that the covered enti-  
15 ty or business associate is in compliance  
16 with security requirements adopted under  
17 part 160 of title 45, Code of Federal Regu-  
18 lations, and subparts A and C of part 164  
19 of title 45, Code of Federal Regulations (or  
20 a successor regulation), including the ap-  
21 plicable security requirements adopted  
22 under paragraph (1)(B); and

23 “(vi) publish on a publicly accessible  
24 website—

## 11

1                   “(I) whether the covered entity  
2                   or business associate has received a  
3                   notification from the Secretary pursu-  
4                   ant to paragraph (1)(B)(ii)(I);

5                   “(II) whether the covered entity  
6                   or business associate meets the min-  
7                   imum security requirements and, if  
8                   applicable, the enhanced security re-  
9                   quirements under paragraph (1)(B);  
10                  and

11                  “(III) a copy of each statement  
12                  provided under clause (v) with respect  
13                  to each year in a machine-readable  
14                  format.

15                  “(B) STRESS TEST METHODOLOGY.—The  
16                  Secretary shall provide for not less than 2 dif-  
17                  ferent sets of conditions under which the test  
18                  described in subparagraph (A)(iii) is to be con-  
19                  ducted.

20                  “(C) WAIVER AUTHORITY.—The Secretary  
21                  may waive the requirements of this paragraph  
22                  with respect to a covered entity or business as-  
23                  sociate if the burden on the entity or associate  
24                  significantly outweighs the benefits, taking into  
25                  account the revenue of the entity or associate,

1 the volume of protected health information or  
2 health care transactions processed by the entity  
3 or associate, and such other factors as the Sec-  
4 retary determines appropriate.

5 “(D) REPORTING.—

6 “(i) IN GENERAL.—Subject to clause  
7 (ii), each covered entity and business asso-  
8 ciate shall submit the documentation re-  
9 quired under subparagraph (A) at such  
10 time, in such form, and containing such in-  
11 formation as the Secretary may require.

12 “(ii) ANNUAL REPORTING FOR COV-  
13 ERED ENTITIES AND BUSINESS ASSOCI-  
14 ATES SUBJECT TO ENHANCED SECURITY  
15 REQUIREMENTS.—Each covered entity and  
16 business associate that is subject to en-  
17 hanced security requirements shall submit  
18 the documentation required under subpara-  
19 graph (A) to the Secretary not less fre-  
20 quently than on an annual basis.

21 “(E) DEFINITIONS.—For purposes of this  
22 subsection:

23 “(i) CYBER INCIDENT.—The term  
24 ‘cyber incident’ has the meaning given the  
25 term ‘incident’ in section 2200(12) of the

1 Homeland Security Act of 2002 (6 U.S.C.  
2 650(12)).

3 “(ii) MACHINE-READABLE.—The term  
4 ‘machine-readable’ has the meaning given  
5 such term in section 3502 of title 44,  
6 United States Code.

7 “(iii) STRESS TEST.—The term ‘stress  
8 test’ means an extensive real-world simula-  
9 tion intended to test the operational resil-  
10 ience of the health care operations of a  
11 covered entity or business associate in re-  
12 sponse to a substantial interruption in in-  
13 formation systems, including the ability  
14 to—

15 “(I) continue to provide essential  
16 care and services during and in the  
17 recovery period from such substantial  
18 interruption; and

19 “(II) timely rebuild the informa-  
20 tion systems (as defined in section  
21 2200(14) of the Homeland Security  
22 Act of 2002 (6 U.S.C. 650(14))) of  
23 such covered entity or business asso-  
24 ciate.

1           “(F) EFFECTIVE DATE.—The require-  
2           ments under this paragraph shall take effect on  
3           the date that is 3 years after the date of enact-  
4           ment of this paragraph.”.

5           (b) INDEPENDENT SECURITY COMPLIANCE AU-  
6           DITS.—Section 1173(d) of the Social Security Act (42  
7           U.S.C. 1320d–2(d)), as amended by subsection (a), is  
8           amended by adding at the end the following new para-  
9           graph:

10           “(4) INDEPENDENT SECURITY COMPLIANCE AU-  
11           DITS.—

12           “(A) IN GENERAL.—Each covered entity  
13           and business associate must—

14           “(i) contract with an independent  
15           auditor that meets such requirements for  
16           independence and technical expertise as  
17           the Inspector General of the Department  
18           of Health and Human Services may estab-  
19           lish to conduct an annual audit in accord-  
20           ance with subparagraph (B); and

21           “(ii) document the findings of each  
22           audit conducted under clause (i).

23           “(B) AUDIT REQUIREMENTS.—An audit  
24           conducted under subparagraph (A)(i) shall—

1 “(i) assess compliance of the covered  
2 entity or business associate with—

3 “(I) during the period prior to  
4 the effective date of the requirements  
5 under paragraph (1)(B), the  
6 Healthcare and Public Health Sector  
7 Cybersecurity Performance Goals as  
8 described in the report published by  
9 the Department of Health and  
10 Human Services as of the date of en-  
11 actment of this paragraph, and titled  
12 ‘Healthcare and Public Health Sector-  
13 Specific Cybersecurity Performance  
14 Goals: Strengthening the Cybersecu-  
15 rity of the Healthcare Sector and  
16 Keeping Patients Safe and Secure’;  
17 and

18 “(II) on or after the effective  
19 date of the requirements under para-  
20 graph (1)(B), the minimum and en-  
21 hanced security requirements adopted  
22 under such paragraph, as applicable;

23 “(ii) identify any areas in which the  
24 covered entity or business associate did not

1 meet such goals or requirements, as appli-  
2 cable; and

3 “(iii) certify that the covered entity or  
4 business associate—

5 “(I) has resolved any areas of  
6 noncompliance; or

7 “(II) is implementing an appro-  
8 priate plan to resolve such areas of  
9 noncompliance in a timely manner.

10 “(C) WAIVER AUTHORITY.—The Secretary  
11 may waive the requirements of this paragraph  
12 with respect to a covered entity or business as-  
13 sociate if the burden on the entity or associate  
14 significantly outweighs the benefits, taking into  
15 account the revenue of the entity or associate,  
16 the volume of protected health information or  
17 health care transactions processed by the entity  
18 or associate, and such as other factors as the  
19 Secretary determines appropriate.

20 “(D) REPORTING.—

21 “(i) IN GENERAL.—Subject to clause  
22 (ii), each covered entity and business asso-  
23 ciate shall submit the documentation re-  
24 quired under subparagraph (A)(ii) at such



1 time, in such form, and containing such in-  
2 formation as the Secretary may require.

3 “(ii) ANNUAL REPORTING FOR ENTI-  
4 TIES AND ASSOCIATES SUBJECT TO EN-  
5 HANCED SECURITY REQUIREMENTS.—Each  
6 covered entity and business associate that  
7 is subject to enhanced security require-  
8 ments shall submit the documentation re-  
9 quired under subparagraph (A)(ii) to the  
10 Secretary not less frequently than on an  
11 annual basis.

12 “(E) EFFECTIVE DATE.—The require-  
13 ments under this paragraph shall take effect on  
14 the date that is 180 days after the date of en-  
15 actment of this paragraph.”.

16 (c) SECRETARIAL AUDITS OF DATA SECURITY PRAC-  
17 TICES.—Section 1173(d) of the Social Security Act (42  
18 U.S.C. 1320d–2(d)), as amended by subsections (a) and  
19 (b), is amended by adding at the end the following new  
20 paragraph

21 “(5) SECRETARIAL AUDITS OF DATA SECURITY  
22 PRACTICES.—

23 “(A) IN GENERAL.—Each year (beginning  
24 on or after the date this is 4 years after the  
25 date of enactment of this paragraph) the Sec-

1           retary shall conduct an annual audit of the data  
2           security practices of at least 20 covered entities  
3           or business associates under this part. The  
4           Comptroller General of the United States shall  
5           monitor auditing activities conducted under this  
6           paragraph.

7           “(B) CONSIDERATIONS.—In selecting cov-  
8           ered entities or business associates for audit  
9           under subparagraph (A) the Secretary shall  
10          consider—

11                   “(i) whether the covered entity or  
12                   business associate is of systemic impor-  
13                   tance;

14                   “(ii) whether any complaints have  
15                   been made with respect to the data secu-  
16                   rity practices of the covered entity or busi-  
17                   ness associate; and

18                   “(iii) whether the covered entity or  
19                   business associate has a history of previous  
20                   violations.

21           “(C) CORRECTIVE ACTION PLAN AND PEN-  
22           ALTIES.—The findings of an audit under this  
23           paragraph may result in a civil money penalty  
24           based on the failure of a covered entity or busi-  
25           ness associate to submit documentation dem-



1                   “(I) fails to timely submit docu-  
2                   mentation or a report required under  
3                   paragraph (3), (4), or (5),

4                   “(II) fails to comply with an  
5                   audit under paragraph (5); or

6                   “(III) fails to comply with a re-  
7                   sponsibility of a covered entity or a  
8                   business associate under section  
9                   160.310 of title 45, Code of Federal  
10                  Regulations (or a successor regula-  
11                  tion),

12                  shall be subject to a civil money penalty of  
13                  not more than \$5,000 per day for each  
14                  such failure.

15                  “(ii) PROCEDURES.—The provisions  
16                  of section 1128A (other than subsections  
17                  (a), (b), and (d)(1), and the second sen-  
18                  tence of subsection (f)) shall apply to the  
19                  imposition of a civil money penalty under  
20                  this subparagraph in the same manner as  
21                  such provisions apply to the imposition of  
22                  a penalty under such section 1128A.

23                  “(iii) CLARIFICATION.—Any civil  
24                  money penalty under this subparagraph  
25                  with respect to a failure described in clause

1 (i) shall be in lieu of the penalties de-  
2 scribed in section 1176.

3 “(B) CRIMINAL PENALTIES.—In addition  
4 to any penalties imposed under subparagraph  
5 (A), whoever submits, or causes to be sub-  
6 mitted, any documentation or report required of  
7 a covered entity or business associate under  
8 paragraph (3), (4), or (5) knowing that such  
9 documentation or report contains false informa-  
10 tion, or willfully fails to timely submit, or will-  
11 fully causes to not be timely submitted, such a  
12 document or report, shall be guilty of a felony  
13 and upon conviction thereof fined not more  
14 than \$1,000,000 or imprisoned for not more  
15 than 10 years, or both.”.

16 **SEC. 103. INCREASED CIVIL PENALTIES FOR FAILURE TO**  
17 **COMPLY WITH SECURITY STANDARDS AND**  
18 **REQUIREMENTS FOR HEALTH INFORMATION.**

19 (a) INCREASED CIVIL PENALTIES.—Section 1176 of  
20 the Social Security Act (42 U.S.C. 1320d–5) is amend-  
21 ed—

22 (1) in subsection (a)(1), in the matter pre-  
23 ceding subparagraph (A), by striking “subsection  
24 (b)” and inserting “subsections (b) and (d)”;

1           (2) by redesignating subsections (d) and (e) as  
2 subsections (e) and (f); and

3           (3) by inserting after subsection (c) the fol-  
4 lowing new subsection:

5           “(d) SPECIAL RULES FOR FAILURE TO COMPLY  
6 WITH SECURITY STANDARDS AND REQUIREMENTS FOR  
7 HEALTH INFORMATION.—

8           “(1) IN GENERAL.—In the case of a violation of  
9 the security standards and requirements under sec-  
10 tion 1173(d) that occurs after the effective date of  
11 the requirements under paragraph (1)(B) of such  
12 section, the following rules shall apply:

13           “(A) Subsection (a)(1)(A) shall be applied  
14 by substituting ‘that is at least \$500’ for ‘that  
15 is at least the amount described in paragraph  
16 (3)(A) but not to exceed the amount described  
17 in paragraph (3)(D)’.

18           “(B) Subsection (a)(1)(B) shall be applied  
19 by substituting ‘that is at least \$5,000’ for  
20 ‘that is at least the amount described in para-  
21 graph (3)(B) but not to exceed the amount de-  
22 scribed in paragraph (3)(D)’.

23           “(C) Subsection (a)(1)(C)(i) shall be ap-  
24 plied by substituting ‘that is at least \$50,000’  
25 for ‘that is at least the amount described in

1 paragraph (3)(C) but not to exceed the amount  
2 described in paragraph (3)(D)’.

3 “(D) Subsection (a)(1)(C)(ii) shall be ap-  
4 plied by substituting ‘that is at least \$250,000’  
5 for ‘that is at least the amount described in  
6 paragraph (3)(D)’.

7 “(E) In addition to the factors described in  
8 the second sentence of subsection (a)(1), in de-  
9 termining the amount of a penalty under this  
10 section for a violation of the security standards  
11 and requirements under section 1173(d), the  
12 Secretary shall also base such determination  
13 on—

14 “(i) the size of the covered entity or  
15 business associate (as such terms are de-  
16 fined in section 1173(d)(1)(B)(vi)) subject  
17 to the penalty;

18 “(ii) the full compliance history of the  
19 covered entity or business associate,

20 “(iii) good faith efforts to comply with  
21 the security standards and requirements;  
22 and

23 “(iv) such other matters as the Sec-  
24 retary determines appropriate.

25 “(F) Subsection (a)(3) shall not apply.

1           “(2) DISTRIBUTION OF CERTAIN CIVIL MONE-  
2           TARY PENALTIES COLLECTED.—

3           “(A) IN GENERAL.—Subject to the regula-  
4           tion promulgated pursuant to subparagraph  
5           (B), any civil monetary penalty or monetary  
6           settlement collected with respect to a violation  
7           of the security standards and requirements  
8           under section 1173(d) that occurs after the ef-  
9           fective date of such requirements under para-  
10          graph (1)(B) of such section shall be trans-  
11          ferred to the Office for Civil Rights of the De-  
12          partment of Health and Human Services to be  
13          used for the purposes of enforcing the provi-  
14          sions of this part and subparts C and E of part  
15          164 of title 45, Code of Federal Regulations (or  
16          any successor regulation).

17          “(B) ESTABLISHMENT OF METHODOLOGY  
18          TO DISTRIBUTE PERCENTAGE OF CMPS COL-  
19          LECTED TO HARMED INDIVIDUALS.—Not later  
20          than 18 months after the date of the enactment  
21          of this subparagraph, the Secretary shall estab-  
22          lish by regulation a methodology under which  
23          an individual who is harmed by an act that con-  
24          stitutes a violation referred to in subparagraph  
25          (A) may receive a percentage of any civil mone-



1            tary penalty or monetary settlement collected  
2            with respect to such violation.

3            “(C) APPLICATION OF METHODOLOGY.—  
4            The methodology under subparagraph (B) shall  
5            be applied to any civil monetary penalty or  
6            monetary settlement collected with respect to a  
7            violation of the security standards and require-  
8            ments under section 1173(d) that occurs after  
9            the effective date of such requirements under  
10           paragraph (1)(B) of such section.”.

11           (b) STRIKING AMENDMENT TO THE HEALTH INFOR-  
12           MATION TECHNOLOGY FOR ECONOMIC AND CLINICAL  
13           HEALTH ACT RELATED TO FINES AND AUDITS.—

14           (1) IN GENERAL.—Part 1 of subtitle D of the  
15           Health Information Technology for Economic and  
16           Clinical Health Act (42 U.S.C. 17931 et seq.), as  
17           amended by Public Law 116–321, is amended by  
18           striking section 13412.

19           (2) EFFECTIVE DATE.—The amendment made  
20           by this subsection shall take effect on the date of en-  
21           actment of this Act, and apply to determinations  
22           made on or after such date.

1 **SEC. 104. USER FEE TO SUPPORT DATA SECURITY OVER-**  
2 **SIGHT AND ENFORCEMENT ACTIVITIES.**

3 Section 1173(d) of the Social Security Act (42 U.S.C.  
4 1320d–2(d)), as amended by section 102, is amended by  
5 adding at the end the following new paragraph:

6 “(7) USER FEE TO SUPPORT DATA SECURITY  
7 OVERSIGHT AND ENFORCEMENT ACTIVITIES.—

8 “(A) IN GENERAL.—Each covered entity  
9 and business associate shall pay the fee estab-  
10 lished by the Secretary under subparagraph  
11 (B).

12 “(B) AUTHORIZATION.—The Secretary is  
13 authorized to charge a fee to each covered enti-  
14 ty and business associate that is equal to the  
15 pro rata share of the entity or associate (equal  
16 to the ratio, as estimated by the Secretary, of  
17 the revenue of the entity or associate for the  
18 preceding fiscal year to national health expendi-  
19 tures, as determined by the Secretary, for the  
20 preceding fiscal year) of the aggregate amount  
21 of fees which the Secretary is directed to collect  
22 in a fiscal year. Any amounts collected shall be  
23 available without further appropriation to the  
24 Secretary for the purpose of carrying out over-  
25 sight and enforcement activities under this sub-  
26 section.



1 **TITLE II—MEDICARE ASSIST-**  
2 **ANCE TO ADDRESS CYBERSE-**  
3 **CURITY INCIDENTS**

4 **SEC. 201. MEDICARE SAFE CYBERSECURITY PRACTICES**  
5 **ADOPTION PROGRAM FOR ELIGIBLE HOS-**  
6 **PITALS AND CRITICAL ACCESS HOSPITALS.**

7 (a) INCENTIVE PAYMENTS.—Section 1886 of the So-  
8 cial Security Act (42 U.S.C. 1395ww) is amended by add-  
9 ing at the end the following new subsection:

10 “(u) INCENTIVES FOR ADOPTION OF ESSENTIAL AND  
11 ENHANCED CYBERSECURITY PRACTICES.—

12 “(1) INVESTMENT.—

13 “(A) FISCAL YEARS 2027 AND 2028.—For  
14 fiscal years 2027 and 2028, upon request, a  
15 critical access hospital or an eligible high-needs  
16 hospital shall be paid from the Federal Hospital  
17 Insurance Trust Fund established under section  
18 1817 a proportional share (as determined by  
19 the Secretary) of \$800,000,000 to adopt essen-  
20 tial cybersecurity practices.

21 “(B) FISCAL YEARS 2029 AND 2030.—For  
22 fiscal years 2029 and 2030, upon request, a  
23 critical access hospital or an eligible hospital  
24 shall be paid from the Federal Hospital Insur-  
25 ance Trust Fund established under section

1 1817 a proportional share (as determined by  
2 the Secretary) of \$500,000,000 to adopt en-  
3 hanced cybersecurity practices.

4 “(C) FORM OF PAYMENT.—A payment  
5 under this subsection may be in the form of a  
6 single consolidated payment or in the form of  
7 such periodic installments as the Secretary may  
8 specify.

9 “(2) ADOPTION.—

10 “(A) ESSENTIAL CYBERSECURITY PRAC-  
11 TICES.—Beginning in fiscal year 2029 for an  
12 eligible hospital, and in calendar year 2029 for  
13 a critical access hospital, such hospital or crit-  
14 ical access hospital shall be treated as an adopt-  
15 er of essential cybersecurity practices for a pay-  
16 ment year if such hospital or critical access hos-  
17 pital submits information to the Secretary, in a  
18 form and manner specified by the Secretary,  
19 and in addition to the information required by  
20 subsection (n)(3)(A)(iii), attesting to implemen-  
21 tation of essential cybersecurity practices se-  
22 lected by the Secretary for the EHR reporting  
23 period with respect to such year.

24 “(B) ENHANCED CYBERSECURITY PRAC-  
25 TICES.—Beginning in fiscal year 2030 for an

1 eligible hospital, and in calendar year 2030 for  
2 a critical access hospital, such hospital or crit-  
3 ical access hospital shall be treated as an adopt-  
4 er of enhanced cybersecurity practices for a  
5 payment year if such hospital or critical access  
6 hospital submits information to the Secretary,  
7 in a form and manner specified by the Sec-  
8 retary, and in addition to the information re-  
9 quired by subsection (n)(3)(A)(iii), attesting to  
10 implementation of enhanced cybersecurity prac-  
11 tices selected by the Secretary during the EHR  
12 reporting period with respect to such year.

13 “(C) IDENTIFICATION OF ESSENTIAL CY-  
14 BERSECURITY PRACTICES.—Beginning in fiscal  
15 year 2027, the Secretary shall, through notice  
16 and comment rulemaking, identify essential cy-  
17 bersecurity practices for an EHR reporting pe-  
18 riod that address known vulnerabilities to data  
19 infrastructure and patient health information  
20 and ensure patient safety and continuity of pa-  
21 tient care.

22 “(D) IDENTIFICATION OF ENHANCED CY-  
23 BERSECURITY PRACTICES.—Beginning in fiscal  
24 year 2028, the Secretary shall, through notice  
25 and comment rulemaking, identify enhanced cy-



1           pital is an essential or enhanced cybersecurity  
2           practices adopted under paragraph (2)  
3           and the Secretary's determination of  
4           whether or not to apply the hardship ex-  
5           ception to an eligible hospital under sub-  
6           section (b)(3)(B)(xiii)(III); or

7                   “(iii) any alteration by the Secretary  
8           of the requirements specified in paragraph  
9           (2).

10           “(B) POSTING ON WEBSITE.—The Sec-  
11           retary shall post on the Internet website of the  
12           Centers for Medicare & Medicaid Services, in an  
13           easily understandable format, the number by  
14           State of eligible hospitals and critical access  
15           hospitals that are not essential or enhanced cy-  
16           bersecurity adopters as applicable for a year.

17           “(4) DEFINITIONS.—For purposes of this sub-  
18           section:

19                   “(A) EHR REPORTING PERIOD.—The term  
20           ‘EHR reporting period’ means the period deter-  
21           mined by the Secretary under subsection  
22           (n)(6)(A).

23                   “(B) ELIGIBLE HIGH-NEEDS HOSPITAL.—  
24           The term ‘eligible high-needs hospital’ means  
25           an eligible hospital that—



1                   “(i) is a subsection (d) Puerto Rico  
2                   hospital (as defined in subsection  
3                   (d)(9)(A));

4                   “(ii) is operated by the Indian Health  
5                   Service or by an Indian tribe or tribal or-  
6                   ganization (as those terms are defined in  
7                   section 4 of the Indian Health Care Im-  
8                   provement Act);

9                   “(iii) has a disproportionate percent-  
10                  age of Medicare beneficiaries who are du-  
11                  ally eligible for benefits under this title and  
12                  title XIX across all subsection (d) hospitals  
13                  in the baseline period (as specified by the  
14                  Secretary) of at least 75 percent;

15                  “(iv) has a disproportionate percent-  
16                  age of Medicare beneficiaries who are sub-  
17                  sidy eligible individuals (as defined in sec-  
18                  tion 1860D–14(a)(3)) across all subsection  
19                  (d) hospitals in the baseline period (as  
20                  specified by the Secretary) of at least 75  
21                  percent (as determined by the Secretary  
22                  under subsection (d)(5)(F)(vi));

23                  “(v) is located in a rural area (as de-  
24                  fined in subsection (d)(2)(D));

1                   “(vi) is classified as a rural referral  
2 center under subsection (d)(5)(C);

3                   “(vii) is a sole community hospital (as  
4 defined in subsection (d)(5)(D)(iii));

5                   “(viii) is a low-volume hospital (as de-  
6 fined in subsection (d)(12)(C)(i)); or

7                   “(ix) is a medicare-dependent, small  
8 rural hospital (as defined in subsection  
9 (d)(5)(G)).

10                  “(C) ELIGIBLE HOSPITAL.—The term ‘eli-  
11 gible hospital’ has the meaning given that term  
12 in subsection (n)(6)(B).

13                  “(D) ENHANCED CYBERSECURITY PRAC-  
14 TICES.—The term ‘enhanced cybersecurity  
15 practices’ means enhanced security require-  
16 ments adopted under section  
17 1173(d)(1)(B)(i)(II) and such additional prac-  
18 tices as the Secretary may select for a year that  
19 are greater than essential cybersecurity prac-  
20 tices.

21                  “(E) ESSENTIAL CYBERSECURITY PRAC-  
22 TICES.—The term ‘essential cybersecurity prac-  
23 tices’ means the minimum security require-  
24 ments adopted under section

1           1173(d)(1)(B)(i)(I) and such additional prac-  
2           tices as the Secretary may select for a year.”.

3           (b) PAYMENT REDUCTIONS FOR FAILURE TO ADOPT  
4 SAFE CYBERSECURITY PRACTICES; SIGNIFICANT HARD-  
5 SHIP EXCEPTION.—

6           (1) HOSPITALS.—Section 1886(b)(3)(B) of the  
7 Social Security Act (42 U.S.C. 1395ww(b)(3)(B)) is  
8 amended by adding at the end the following new  
9 clause:

10                   “(xiii)(I) For purposes of clause (i)—

11                           “(aa) for fiscal year 2029, in the  
12 case of an eligible hospital that is not  
13 an adopter of the essential cybersecu-  
14 rity practices for a payment year (as  
15 determined under subsection  
16 (u)(2)(A)) for an EHR reporting pe-  
17 riod for such year, the applicable per-  
18 centage increase otherwise applicable  
19 under clause (i) (determined without  
20 regard to clause (viii) or (xi)) for such  
21 fiscal year shall be reduced (but not  
22 below zero) by 0.25 percentage point;

23                           “(bb) for fiscal year 2030, in the  
24 case of an eligible hospital that is not  
25 an adopter of the essential cybersecu-

1 rity practices for a payment year (as  
2 determined under subsection  
3 (u)(2)(A)) for an EHR reporting pe-  
4 riod for such year—

5 “(AA) the applicable per-  
6 centage increase otherwise appli-  
7 cable under clause (i) (deter-  
8 mined without regard to clause  
9 (viii) or (xi)) for such fiscal year  
10 shall be reduced (but not below  
11 zero) by 0.50 percentage point;  
12 and

13 “(BB) the base operating  
14 DRG payment amount (as de-  
15 fined in subsection (o)(7)(D)) for  
16 such hospital for each discharge  
17 in such fiscal year shall be re-  
18 duced by 0.25 percent;

19 “(cc) for fiscal year 2031, in the  
20 case of an eligible hospital that is not  
21 an adopter of the enhanced cybersecu-  
22 rity practices for a payment year (as  
23 determined under subsection  
24 (u)(2)(B)) for an EHR reporting pe-  
25 riod for such fiscal year—

1           “(AA) the applicable per-  
2           centage increase otherwise appli-  
3           cable under clause (i) (deter-  
4           mined without regard to clause  
5           (viii) or (xi)) for such fiscal year  
6           shall be reduced (but not below  
7           zero) by 0.75 percentage point;  
8           and

9           “(BB) the base operating  
10          DRG payment amount (as de-  
11          fined in subsection (o)(7)(D)) for  
12          such hospital for each discharge  
13          in such fiscal year shall be re-  
14          duced by 0.50 percent;

15          “(dd) for fiscal year 2032, in the  
16          case of an eligible hospital that is not  
17          an adopter of the enhanced cybersecu-  
18          rity practices for a payment year (as  
19          determined under subsection  
20          (u)(2)(B)) for an EHR reporting pe-  
21          riod for such fiscal year—

22          “(AA) the applicable per-  
23          centage increase otherwise appli-  
24          cable under clause (i) (deter-  
25          mined without regard to clause

1 (viii) or (xi)) for such fiscal year  
2 shall be reduced (but not below  
3 zero) by 1.0 percentage point;  
4 and

5 “(BB) the base operating  
6 DRG payment amount (as de-  
7 fined in subsection (o)(7)(D)) for  
8 such hospital for each discharge  
9 in such fiscal year shall be re-  
10 duced by 0.75 percent; and

11 “(ee) for fiscal year 2033 and  
12 each subsequent fiscal year, in the  
13 case of an eligible hospital that is not  
14 an adopter of the enhanced cybersecu-  
15 rity practices for a payment year (as  
16 determined under subsection  
17 (u)(2)(B)) for an EHR reporting pe-  
18 riod for such fiscal year—

19 “(AA) the applicable per-  
20 centage increase otherwise appli-  
21 cable under clause (i) (deter-  
22 mined without regard to clause  
23 (viii) or (xi)) for such fiscal year  
24 shall be reduced (but not below

1 zero) by 1.0 percentage point;  
2 and

3 “(BB) the base operating  
4 DRG payment amount (as de-  
5 fined in subsection (o)(7)(D)) for  
6 such hospital for each discharge  
7 in such fiscal year shall be re-  
8 duced by 1.0 percent.

9 “(II) A reduction under subclause (I)  
10 shall apply only with respect to the fiscal  
11 year involved, and the Secretary shall not  
12 take into account such reduction in making  
13 payments to a hospital under this section  
14 in a subsequent fiscal year.

15 “(III) The Secretary may, on a case-  
16 by-case basis, except an eligible hospital  
17 from the application of subclause (I) with  
18 respect to a fiscal year if the Secretary de-  
19 termines, subject to annual renewal, that  
20 requiring such hospital to be an essential  
21 or enhanced cybersecurity practices adopt-  
22 er during such fiscal year would result in  
23 a significant hardship, such as in the case  
24 of a natural disaster, a bankruptcy, limited  
25 internet connectivity, an incident (as de-

1            fined in section 2200 of the Homeland Se-  
2            curity Act of 2002) that significantly dis-  
3            rupts medicare claims processing, or any  
4            other similar situation that the Secretary  
5            determines interfered with the ability of  
6            the eligible hospital to meet the require-  
7            ments. An eligible hospital may not be  
8            granted an exemption under this subclause  
9            for more than 5 years, except in cases  
10           where the Secretary determines such hos-  
11           pital has experienced an incident (as so de-  
12           fined) that significantly disrupts medicare  
13           claims processing. The Secretary shall es-  
14           tablish an exception process and post an  
15           application for an exception on the Inter-  
16           net website of the Centers for Medicare &  
17           Medicaid Services. Such process shall re-  
18           quire that the application be submitted to  
19           the Secretary by not later than 6 months  
20           after the conclusion of the EHR reporting  
21           period for the relevant year.

22                    “(IV) In the case of a State for which  
23           the Secretary has waived all or part of this  
24           section under the authority of section  
25           1115A, nothing in this section shall pre-



1           clude such State from implementing an ad-  
2           justment similar to the adjustment under  
3           subclause (I).

4                   “(V) In this clause, the term ‘eligible  
5           hospital’ has the meaning given such term  
6           in subsection (u)(4).”.

7           (2) CRITICAL ACCESS HOSPITALS.—Section  
8           1814(l) of the Social Security Act (42 U.S.C.  
9           1395f(l)) is amended—

10                   (A) by redesignating paragraph (5) as  
11           paragraph (6);

12                   (B) by inserting after paragraph (4) the  
13           following new paragraph:

14                   “(5)(A) Subject to subparagraphs (B) and (C),  
15           for cost reporting periods beginning in—

16                           “(i) fiscal year 2029, in the case of a crit-  
17           ical access hospital that is not an essential cy-  
18           bersecurity practices adopter (as determined  
19           under section 1886(u)(3)(A)) for an EHR re-  
20           porting period with respect to such fiscal year,  
21           the percent described in paragraph (1) shall be  
22           reduced by 0.25 percent;

23                           “(ii) fiscal year 2030, in the case of a crit-  
24           ical access hospital that is not an essential cy-  
25           bersecurity practices adopter (as determined

1 under section 1886(u)(3)(A)) for an EHR re-  
2 porting period with respect to such fiscal year,  
3 the percent described in paragraph (1) shall be  
4 reduced by 0.50 percent;

5 “(iii) fiscal year 2031, in the case of a crit-  
6 ical access hospital that is not an enhanced cy-  
7 bersecurity practices adopter (as determined  
8 under section 1886(u)(3)(B)) for a EHR re-  
9 porting period with respect to such fiscal year,  
10 the percent described in paragraph (1) shall be  
11 reduced by 0.75 percent; and

12 “(iv) fiscal year 2032 or a subsequent fis-  
13 cal year, in the case of a critical access hospital  
14 that is not an enhanced cybersecurity practices  
15 adopter (as determined under section  
16 1886(u)(3)(B)) for a EHR reporting period  
17 with respect to such fiscal year, the percent de-  
18 scribed in paragraph (1) shall be reduced by 1  
19 percent.

20 “(B) The percent described in paragraph (1)  
21 shall be reduced by no more than a total of 1 per-  
22 cent for a fiscal year as the result of the application  
23 of this paragraph and other sections of this title.

24 “(C) The provisions of subclause (III) of sec-  
25 tion 1886(b)(3)(B)(xiii) shall apply with respect to

1       subparagraph (A) for a critical access hospital with  
2       respect to a cost reporting period in the same man-  
3       ner as such subclause applies with respect to sub-  
4       clause (I) of such section for an eligible hospital.”;  
5       and

6               (C) in paragraph (6), as redesignated by  
7       subparagraph (A)—

8               (i) in subparagraph (C), by striking  
9       “and” at the end;

10              (ii) in subparagraph (D), by striking  
11       the period at the end and inserting “;  
12       and”; and

13              (iii) by adding at the end the fol-  
14       lowing new subparagraphs:

15              “(E) the methodology and standards for deter-  
16       mining payment amounts for critical access hospitals  
17       under section 1886(u) and payment adjustments  
18       under paragraph (5);

19              “(F) the methodology and standards for deter-  
20       mining whether a critical access hospital is an essen-  
21       tial or enhanced cybersecurity practices adopter  
22       under section 1886(u)(2) and the Secretary’s deter-  
23       mination of whether or not to apply the hardship ex-  
24       ception under subsection (b)(3)(B)(xiii)(III) to a

1 critical access hospital pursuant to paragraph  
2 (5)(C); or

3 “(G) any alteration by the Secretary of the re-  
4 quirements specified in section 1886(u)(2) with re-  
5 spect to a critical access hospital.”.

6 (c) IMPLEMENTATION FUNDING.—In addition to any  
7 amounts otherwise made available, there is appropriated  
8 to the Centers for Medicare & Medicaid Services Program  
9 Management Account from the Federal Hospital Insur-  
10 ance Trust Fund under section 1817 of the Social Secu-  
11 rity Act (42 U.S.C. 1395i), \$40,000,000 for fiscal year  
12 2025 and \$15,000,000 for each of fiscal years 2027  
13 through 2031, to remain available until expended, to carry  
14 out the amendments made by this section.

15 **SEC. 202. MEDICARE ACCELERATED AND ADVANCE PAY-**  
16 **MENTS IN RESPONSE TO CYBERSECURITY IN-**  
17 **CIDENTS.**

18 (a) PART A.—Section 1815(e)(3) of the Social Secu-  
19 rity Act (42 U.S.C. 1395g(e)(3)) is amended to read as  
20 follows:

21 “(3)(A) Subject to subsection (f), in the case of an  
22 eligible provider of services (as defined in subparagraph  
23 (B)) that has an agreement in effect under section 1866  
24 and that has significant cash flow problems resulting from  
25 operations of its medicare administrative contractor under

1 section 1874A or from unusual circumstances of such pro-  
2 vider’s operation, including significant disruption to Medi-  
3 care claims processing due to a cybersecurity incident (as  
4 defined in subparagraph (C)), the Secretary may make  
5 available appropriate accelerated payments subject to ap-  
6 propriate safeguards against fraud, waste, and abuse de-  
7 termined by the Secretary.

8 “(B) In this paragraph, the term ‘eligible providers  
9 of services’ means—

10 “(i) a subsection (d) hospital or a subsection  
11 (d) Puerto Rico hospital (as defined for purposes of  
12 section 1886);

13 “(ii) a hospital described in any of clauses (i)  
14 through (vi) of section 1886(d)(1)(B);

15 “(iii) a critical access hospital (as defined in  
16 section 1861(mm)(1));

17 “(iv) a rural emergency hospital (as defined in  
18 section 1861(kkk)(2));

19 “(v) a skilled nursing facility (as defined in sec-  
20 tion 1819(a));

21 “(vi) a home health agency (as defined in sec-  
22 tion 1861(o));

23 “(vii) a hospice program (as defined in section  
24 1861(dd)(2));

1           “(viii) a comprehensive outpatient rehabilitation  
2           facility (as defined in section 1861(cc)(2));

3           “(ix) a rural health clinic (as defined in section  
4           1861(aa)(2));

5           “(x) a Federally qualified health center (as de-  
6           fined in section 1861(aa)(4));

7           “(xi) an opioid treatment program (as defined  
8           in section 1861(jjj)(2)); and

9           “(xii) a community mental health center (as de-  
10          fined in section 1861(ff)(3)(B)).

11          “(C) In this paragraph, the term ‘cybersecurity inci-  
12          dent’ has the meaning given the term ‘incident’ in section  
13          2200 of the Homeland Security Act of 2002.

14          “(D) Notwithstanding any other provision of law, the  
15          Secretary may implement the provisions of this paragraph  
16          by program instruction or otherwise.”.

17          (b) PART B.—Section 1835 of the Social Security Act  
18          (42 U.S.C. 1395n) is amended by adding at the end the  
19          following new subsection:

20          “(f)(1) Upon the request of a supplier (as defined in  
21          section 1861(d)) that is participating in the Medicare pro-  
22          gram under this title, that is furnishing items or services  
23          under this part, and that has significant cash flow prob-  
24          lems resulting from operations of its medicare administra-  
25          tive contractor under section 1874A or from unusual cir-

1 cumstances of such supplier’s operation, including signifi-  
2 cant disruption to Medicare claims processing due to a cy-  
3 bersecurity incident (as defined in paragraph (2)), the  
4 Secretary may make available appropriate advance pay-  
5 ments subject to appropriate safeguards against fraud,  
6 waste, and abuse determined by the Secretary.

7 “(2) In this paragraph, the term ‘cybersecurity inci-  
8 dent’ has the meaning given the term ‘incident’ in section  
9 2200 of the Homeland Security Act of 2002.

10 “(3) Notwithstanding any other provision of law, the  
11 Secretary may implement the provisions of this subsection  
12 by program instruction or otherwise.”.

13 (c) PROTECTION OF TRUST FUNDS.—

14 (1) PART A.—Section 1817 of the Social Secu-  
15 rity Act (42 U.S.C. 1395i) is amended by adding at  
16 the end the following new subsection:

17 “(1)(1) Beginning on the date of enactment of this  
18 subsection, there shall be transferred from the General  
19 Fund of the Treasury to the Trust Fund an amount, as  
20 estimated by the Chief Actuary of the Centers for Medi-  
21 care & Medicaid Services, equal to the amount of acceler-  
22 ated payments made for items and services under this  
23 part.

1           “(2) There shall be transferred from the Trust Fund  
2 to the General Fund of the Treasury amounts equivalent  
3 to the sum of—

4           “(A) the amounts by which claims have offset  
5 (in whole or in part) the amount of such payments  
6 described in paragraph (1); and

7           “(B) the amount of such payments that have  
8 been repaid (in whole or in part).

9           “(3) Amounts described in paragraphs (1) and (2)  
10 shall be transferred from time to time as determined ap-  
11 propriate by the Secretary.”.

12           (2) PART B.—Section 1844 of the Social Secu-  
13 rity Act (42 U.S.C. 1395w) is amended by adding  
14 at the end the following new subsection:

15           “(g)(1) Beginning on the date of enactment of this  
16 subsection, there shall be transferred from the General  
17 Fund of the Treasury to the Trust Fund an amount, as  
18 estimated by the Chief Actuary of the Centers for Medi-  
19 care & Medicaid Services, equal to amounts paid in ad-  
20 vance for items and services under this part.

21           “(2) There shall be transferred from the Trust Fund  
22 to the General Fund of the Treasury amounts equivalent  
23 to the sum of—



1           “(A) the amounts by which claims have offset  
2           (in whole or in part) the amount of such payments  
3           described in paragraph (1); and

4           “(B) the amount of such payments that have  
5           been repaid (in whole or in part).

6           “(3) Amounts described in paragraphs (1) and (2)  
7           shall be transferred from time to time as determined ap-  
8           propriate by the Secretary.”.