

117TH CONGRESS
1ST SESSION

S. 2491

To amend the Homeland Security Act of 2002 to establish the National Cyber Resilience Assistance Fund, to improve the ability of the Federal Government to assist in enhancing critical infrastructure cyber resilience, to improve security in the national cyber ecosystem, to address Systemically Important Critical Infrastructure, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 27, 2021

Mr. KING (for himself, Mr. ROUNDS, and Mr. SASSE) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To amend the Homeland Security Act of 2002 to establish the National Cyber Resilience Assistance Fund, to improve the ability of the Federal Government to assist in enhancing critical infrastructure cyber resilience, to improve security in the national cyber ecosystem, to address Systemically Important Critical Infrastructure, 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,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Defense of United States Infrastructure Act of 2021”.

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

Sec. 1. Short title; table of contents.

TITLE I—INVESTING IN CYBER RESILIENCY IN CRITICAL
INFRASTRUCTURE

Sec. 101. Establishment of the National Cyber Resilience Assistance Fund.

TITLE II—IMPROVING THE ABILITY OF THE FEDERAL GOVERN-
MENT TO ASSIST IN ENHANCING CRITICAL INFRASTRUCTURE
CYBER RESILIENCE

Sec. 201. Institute a 5-year term for the cybersecurity and infrastructure secu-
rity director.

Sec. 202. Create a joint collaborative environment.

Sec. 203. Designate three critical technology security centers.

TITLE III—IMPROVING SECURITY IN THE NATIONAL CYBER
ECOSYSTEM

Sec. 301. Establish a National Cybersecurity Certification and Labeling Au-
thority.

Sec. 302. Establish the Bureau of Cybersecurity Statistics.

Sec. 303. Secure foundational internet protocols.

TITLE IV—SYSTEMICALLY IMPORTANT CRITICAL
INFRASTRUCTURE

Sec. 401. Definitions.

Sec. 402. Systemically Important Critical Infrastructure.

Sec. 403. Plan for enhancement of Systemically Important Critical Infrastruc-
ture methodology and capability.

TITLE V—ENABLING THE NATIONAL CYBER DIRECTOR

Sec. 501. Establishment of hiring authorities for the Office of the National
Cyber Director.

1 **TITLE I—INVESTING IN CYBER**
2 **RESILIENCY IN CRITICAL IN-**
3 **FRASTRUCTURE**

4 **SEC. 101. ESTABLISHMENT OF THE NATIONAL CYBER RE-**
5 **SILIENCE ASSISTANCE FUND.**

6 (a) SENSE OF CONGRESS.—It is the sense of Con-
7 gress that—

8 (1) the United States now operates in a cyber
9 landscape that requires a level of data security, resil-
10 ience, and trustworthiness that neither the United
11 States Government nor the private sector alone is
12 currently equipped to provide;

13 (2) the United States must deny benefits to ad-
14 versaries who have long exploited cyberspace to their
15 advantage, to the disadvantage of the United States,
16 and at little cost to themselves;

17 (3) this new approach requires securing critical
18 networks in collaboration with the private sector to
19 promote national resilience and increase the security
20 of the cyber ecosystem;

21 (4) reducing the vulnerabilities adversaries can
22 target denies them opportunities to attack the inter-
23 ests of the United States through cyberspace;

1 (5) the public and private sectors struggle to
2 coordinate cyber defenses, leaving gaps that decrease
3 national resilience and create systemic risk;

4 (6) new technology continues to emerge that
5 further compounds these challenges;

6 (7) while the Homeland Security Grant Pro-
7 gram and resourcing for national preparedness
8 under the Federal Emergency Management Agency
9 are well-established, the United States Government
10 has no equivalent for cybersecurity preparation or
11 prevention;

12 (8) the lack of a consistent, resourced fund for
13 investing in resilience in key areas inhibits the
14 United States Government from conveying its under-
15 standing of risk into strategy, planning, and action
16 in furtherance of core objectives for the security and
17 resilience of critical infrastructure;

18 (9) Congress has worked diligently to establish
19 the Cybersecurity and Infrastructure Security Agen-
20 cy, creating a new agency that can leverage broad
21 authorities to receive and share information, provide
22 technical assistance to operators, and partner with
23 stakeholders across the executive branch, State and
24 local communities, and the private sector;

1 (10) the Cybersecurity and Infrastructure Secu-
2 rity Agency requires strengthening in its mission to
3 ensure the national resilience of critical infrastruc-
4 ture, promote a more secure cyber ecosystem, and
5 serve as the central coordinating element to support
6 and integrate Federal, State, local, and private-sec-
7 tor cybersecurity efforts; and

8 (11) the Cybersecurity and Infrastructure Secu-
9 rity Agency requires further resource investment and
10 clear authorities to realize its full potential.

11 (b) AMENDMENTS.—Subtitle A of title XXII of the
12 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)
13 is amended—

14 (1) in section 2202(c) (6 U.S.C. 652(c))—

15 (A) in paragraph (11), by striking “and”
16 at the end;

17 (B) in the first paragraph designated as
18 paragraph (12), relating to the Cybersecurity
19 State Coordinator—

20 (i) by striking “section 2215” and in-
21 serting “section 2217”; and

22 (ii) by striking “and” at the end; and

23 (C) by redesignating the second and third
24 paragraphs designated as paragraph (12) as
25 paragraphs (13) and (14), respectively;

1 (2) by redesignating section 2217 (6 U.S.C.
2 665f) as section 2220;

3 (3) by redesignating section 2216 (6 U.S.C.
4 665e) as section 2219;

5 (4) by redesignating the fourth section 2215
6 (relating to Sector Risk Management Agencies) (6
7 U.S.C. 665d) as section 2218;

8 (5) by redesignating the third section 2215 (re-
9 lating to the Cybersecurity State Coordinator) (6
10 U.S.C. 665c) as section 2217;

11 (6) by redesignating the second section 2215
12 (relating to the Joint Cyber Planning Office) (6
13 U.S.C. 665b) as section 2216; and

14 (7) by adding at the end the following:

15 **“SEC. 2220A. NATIONAL CYBER RESILIENCE ASSISTANCE**
16 **FUND.**

17 “(a) DEFINITIONS.—In this section:

18 “(1) CYBERSECURITY RISK.—The term ‘cyber-
19 security risk’ has the meaning given that term in
20 section 2209.

21 “(2) ELIGIBLE ENTITY.—The term ‘eligible en-
22 tity’ means an entity that meets the guidelines and
23 requirements for eligible entities established by the
24 Secretary under subsection (d)(4).

1 “(3) FUND.—The term ‘Fund’ means the Na-
2 tional Cyber Resilience Assistance Fund established
3 under subsection (c).

4 “(4) NATIONAL CRITICAL FUNCTIONS.—The
5 term ‘national critical functions’ means the functions
6 of government and the private sector so vital to the
7 United States that their disruption, corruption, or
8 dysfunction would have a debilitating effect on secu-
9 rity, national economic security, national public
10 health or safety, or any combination thereof.

11 “(b) CREATION OF A CRITICAL INFRASTRUCTURE
12 RESILIENCE STRATEGY AND A NATIONAL RISK MANAGE-
13 MENT CYCLE.—

14 “(1) INITIAL RISK IDENTIFICATION AND AS-
15 SESSMENT.—

16 “(A) IN GENERAL.—The Secretary, acting
17 through the Director, shall establish a process
18 by which to identify, assess, and prioritize risks
19 to critical infrastructure, considering both cyber
20 and physical threats, vulnerabilities, and con-
21 sequences.

22 “(B) CONSULTATION.—In establishing the
23 process required under subparagraph (A), the
24 Secretary shall consult with Sector Risk Man-
25 agement Agencies, critical infrastructure owners

1 and operators, and the National Cyber Direc-
2 tor.

3 “(C) PUBLICATION.—Not later than 180
4 days after the date of enactment of this section,
5 the Secretary shall publish in the Federal Reg-
6 ister procedures for the process established
7 under subparagraph (A).

8 “(D) REPORT.—Not later than 1 year
9 after the date of enactment of this section, the
10 Secretary shall submit to the President, the
11 Committee on Homeland Security and Govern-
12 mental Affairs of the Senate, and the Com-
13 mittee on Homeland Security of the House of
14 Representatives a report on the risks identified
15 by the process established under subparagraph
16 (A).

17 “(2) INITIAL NATIONAL CRITICAL INFRASTRUC-
18 TURE RESILIENCE STRATEGY.—

19 “(A) IN GENERAL.—Not later than 1 year
20 after the date on which the Secretary delivers
21 the report required under paragraph (1)(D),
22 the President shall deliver to majority and mi-
23 nority leaders of the Senate, the Speaker and
24 minority leader of the House of Representa-
25 tives, the Committee on Homeland Security and

1 Governmental Affairs of the Senate, and the
2 Committee on Homeland Security of the House
3 of Representatives a national critical infrastruc-
4 ture resilience strategy designed to address the
5 risks identified by the Secretary.

6 “(B) ELEMENTS.—In the strategy deliv-
7 ered under subparagraph (A), the President
8 shall—

9 “(i) identify, assess, and prioritize
10 areas of risk to critical infrastructure that
11 would compromise, disrupt, or impede the
12 ability of the critical infrastructure to sup-
13 port the national critical functions of na-
14 tional security, economic security, or public
15 health and safety;

16 “(ii) identify and outline current and
17 proposed national-level actions, programs,
18 and efforts to be taken to address the risks
19 identified;

20 “(iii) identify the Federal departments
21 or agencies responsible for leading each na-
22 tional-level action, program, or effort and
23 the relevant critical infrastructure sectors
24 for each;

1 “(iv) outline the budget plan required
2 to provide sufficient resources to success-
3 fully execute the full range of activities
4 proposed or described by the strategy; and

5 “(v) request any additional authorities
6 or resources necessary to successfully exe-
7 cute the strategy.

8 “(C) FORM.—The strategy delivered under
9 subparagraph (A) shall be unclassified, but may
10 contain a classified annex.

11 “(3) CONGRESSIONAL BRIEFING.—Not later
12 than 1 year after the date on which the President
13 delivers the strategy under subparagraph (A), and
14 every year thereafter, the Secretary, in coordination
15 with Sector Risk Management Agencies, shall brief
16 the appropriate congressional committees on the na-
17 tional risk management cycle activities undertaken
18 pursuant to the strategy.

19 “(4) FIVE YEAR RISK MANAGEMENT CYCLE.—

20 “(A) RISK IDENTIFICATION AND ASSESS-
21 MENT.—Under procedures established by the
22 Secretary, the Secretary shall repeat the con-
23 ducting and reporting of the risk identification
24 and assessment required under paragraph (1),

1 in accordance with the requirements in para-
2 graph (1), every 5 years.

3 “(B) STRATEGY.—Under procedures estab-
4 lished by the President, the President shall re-
5 peat the preparation and delivery of the critical
6 infrastructure resilience strategy required under
7 paragraph (2), in accordance with the require-
8 ments in paragraph (2), every 5 years, which
9 shall also include assessing the implementation
10 of the previous national critical infrastructure
11 resilience strategy.

12 “(c) ESTABLISHMENT OF THE NATIONAL CYBER RE-
13 SILIENCE ASSISTANCE FUND.—There is established in the
14 Treasury of the United States a fund, to be known as the
15 ‘National Cyber Resilience Assistance Fund’, which shall
16 be available for the cost of risk-based grant programs fo-
17 cused on systematically increasing the resilience of public
18 and private critical infrastructure against cybersecurity
19 risk, thereby increasing the overall resilience of the United
20 States.

21 “(d) ADMINISTRATION OF GRANTS FROM THE NA-
22 TIONAL CYBER RESILIENCE ASSISTANCE FUND.—

23 “(1) IN GENERAL.—In accordance with this
24 section, the Secretary, acting through the Adminis-
25 trator of the Federal Emergency Management Agen-

1 cy and the Director, shall develop and administer
2 processes to—

3 “(A) establish focused grant programs to
4 address identified areas of cybersecurity risk to,
5 and bolster the resilience of, critical infrastruc-
6 ture;

7 “(B) accept and evaluate applications for
8 each such grant program;

9 “(C) award grants under each such grant
10 program; and

11 “(D) disburse amounts from the Fund.

12 “(2) ESTABLISHMENT OF RISK-FOCUSED
13 GRANT PROGRAMS.—

14 “(A) ESTABLISHMENT.—

15 “(i) IN GENERAL.—The Secretary,
16 acting through the Director and the Ad-
17 ministrator of the Federal Emergency
18 Management Agency, may establish not
19 less than 1 grant program focused on miti-
20 gating an identified category of cybersecu-
21 rity risk identified under the national risk
22 management cycle and critical infrastruc-
23 ture resilience strategy under subsection
24 (b) in order to bolster the resilience of crit-

1 ical infrastructure within the United
2 States.

3 “(ii) SELECTION OF FOCUS AREA.—
4 Before selecting a focus area for a grant
5 program pursuant to this subparagraph,
6 the Director shall ensure—

7 “(I) there is a clearly defined cy-
8 bersecurity risk identified through the
9 national risk management cycle and
10 critical infrastructure resilience strat-
11 egy under subsection (b) to be miti-
12 gated;

13 “(II) market forces do not pro-
14 vide sufficient private-sector incentives
15 to mitigate the risk without Govern-
16 ment investment; and

17 “(III) there is clear Federal
18 need, role, and responsibility to miti-
19 gate the risk in order to bolster the
20 resilience of critical infrastructure.

21 “(B) FUNDING.—

22 “(i) RECOMMENDATION.—Beginning
23 in the first fiscal year following the estab-
24 lishment of the Fund and each fiscal year
25 thereafter, the Director shall—

1 “(I) assess the funds available in
2 the Fund for the fiscal year; and

3 “(II) recommend to the Secretary
4 the total amount to be made available
5 from the Fund under each grant pro-
6 gram established under this sub-
7 section.

8 “(ii) ALLOCATION.—After considering
9 the recommendations made by the Director
10 under clause (i) for a fiscal year, the Di-
11 rector shall allocate amounts from the
12 Fund to each active grant program estab-
13 lished under this subsection for the fiscal
14 year.

15 “(3) USE OF FUNDS.—Amounts in the Fund
16 shall be used to mitigate risks identified through the
17 national risk management cycle and critical infra-
18 structure resilience strategy under subsection (b).

19 “(4) ELIGIBLE ENTITIES.—

20 “(A) GUIDELINES AND REQUIREMENTS.—

21 “(i) IN GENERAL.—In accordance
22 with clause (ii), the Secretary shall submit
23 to the Committee on Homeland Security
24 and Governmental Affairs and the Com-
25 mittee on Appropriations of the Senate

1 and the Committee on Homeland Security
2 and the Committee on Appropriations of
3 the House of Representatives a set of
4 guidelines and requirements for deter-
5 mining the entities that are eligible enti-
6 ties.

7 “(ii) DEADLINES.—The Secretary
8 shall submit the guidelines and require-
9 ments under clause (i)—

10 “(I) not later than 180 days
11 after the date of enactment of this
12 section, and every 2 years thereafter;
13 and

14 “(II) not later than 30 days be-
15 fore the date on which the Secretary
16 implements the guidelines and re-
17 quirements.

18 “(B) CONSIDERATIONS.—In developing
19 guidelines and requirements for eligible entities
20 under subparagraph (A), the Secretary shall
21 consider—

22 “(i) number of employees;

23 “(ii) annual revenue;

24 “(iii) existing entity cybersecurity
25 spending;

1 “(iv) current cyber risk assessments,
2 including credible threats, vulnerabilities,
3 and consequences; and

4 “(v) entity capacity to invest in miti-
5 gating cybersecurity risk absent assistance
6 from the Federal Government.

7 “(5) LIMITATION.—For any fiscal year, an eli-
8 gible entity may not receive more than 1 grant from
9 each grant program established under this sub-
10 section.

11 “(6) GRANT PROCESSES.—The Secretary, act-
12 ing through the Administrator of the Federal Emer-
13 gency Management Agency, shall require the sub-
14 mission of such information as the Secretary deter-
15 mines is necessary to—

16 “(A) evaluate a grant application against
17 the criteria established under this section;

18 “(B) disburse grant funds;

19 “(C) provide oversight of disbursed grant
20 funds; and

21 “(D) evaluate the effectiveness of the fund-
22 ed project in increasing the overall resilience of
23 the United States with respect to cybersecurity
24 risks.

1 “(7) GRANT CRITERIA.—For each grant pro-
2 gram established under this subsection, the Director,
3 in coordination with the Administrator of the Fed-
4 eral Emergency Management Agency, shall develop
5 and publish criteria for evaluating applications for
6 funding, which shall include—

7 “(A) whether the application identifies a
8 clearly defined cybersecurity risk;

9 “(B) whether the cybersecurity risk identi-
10 fied in the grant application poses a substantial
11 threat to critical infrastructure;

12 “(C) whether the application identifies a
13 program or project clearly designed to mitigate
14 a cybersecurity risk;

15 “(D) the potential consequences of leaving
16 the identified cybersecurity risk unmitigated, in-
17 cluding the potential impact to the critical func-
18 tions and overall resilience of the nation; and

19 “(E) other appropriate factors identified
20 by the Director.

21 “(8) EVALUATION OF GRANTS APPLICATIONS.—

22 “(A) IN GENERAL.—Utilizing the criteria
23 established under paragraph (7), the Director,
24 in coordination with the Administrator of the
25 Federal Emergency Management Agency, shall

1 evaluate grant applications made under each
2 grant program established under this sub-
3 section.

4 “(B) RECOMMENDATION.—Following the
5 evaluations required under subparagraph (A),
6 the Director shall recommend to the Secretary
7 applications for approval, including the amount
8 of funding recommended for each such ap-
9 proval.

10 “(9) AWARD OF GRANT FUNDING.—The Sec-
11 retary shall—

12 “(A) review the recommendations of the
13 Director prepared pursuant to paragraph (8);
14 and

15 “(B) provide a final determination of grant
16 awards to the Administrator of the Federal
17 Emergency Management Agency to be dis-
18 bursed and administered under the process es-
19 tablished under paragraph (6).

20 “(e) EVALUATION OF GRANT PROGRAMS UTILIZING
21 THE NATIONAL CYBER RESILIENCE ASSISTANCE
22 FUND.—

23 “(1) EVALUATION.—The Secretary shall estab-
24 lish a process to evaluate the effectiveness and effi-
25 ciency of grants distributed under this section and

1 develop appropriate updates, as needed, to the grant
2 programs.

3 “(2) ANNUAL REPORT.—Not later than 180
4 days after the conclusion of the first fiscal year in
5 which grants are awarded under this section, and
6 every fiscal year thereafter, the Secretary shall sub-
7 mit to the Committee on Homeland Security and
8 Governmental Affairs and the Committee on Appro-
9 priations of the Senate and the Committee on
10 Homeland Security and the Committee on Appro-
11 priations of the House of Representatives a report
12 detailing the grants awarded from the Fund, the
13 status of projects undertaken with the grant funds,
14 any planned changes to the disbursement method-
15 ology of the Fund, measurements of success, and
16 total outlays from the Fund.

17 “(3) GRANT PROGRAM REVIEW.—

18 “(A) ANNUAL ASSESSMENT.—Before the
19 start of the second fiscal year in which grants
20 are awarded under this section, and every fiscal
21 year thereafter, the Director shall assess the
22 grant programs established under this section
23 and determine—

24 “(i) for the coming fiscal year—

1 “(I) whether new grant programs
2 with additional focus areas should be
3 created;

4 “(II) whether any existing grant
5 program should be discontinued; and

6 “(III) whether the scope of any
7 existing grant program should be
8 modified; and

9 “(ii) the success of the grant pro-
10 grams in the prior fiscal year.

11 “(B) SUBMISSION TO CONGRESS.—Not
12 later than 90 days before the start of the sec-
13 ond fiscal year in which grants are awarded
14 under this section, and every fiscal year there-
15 after, the Secretary shall submit to the Com-
16 mittee on Homeland Security and Govern-
17 mental Affairs and the Committee on Appro-
18 priations of the Senate and the Committee on
19 Homeland Security and the Committee on Ap-
20 propriations of the House of Representatives
21 the assessment conducted pursuant to subpara-
22 graph (A) and any planned alterations to the
23 grant program for the coming fiscal year.

24 “(f) LIMITATION ON USE OF GRANT FUNDS.—Funds
25 awarded pursuant to this section—

1 “(1) shall supplement and not supplant State
2 or local funds or, as applicable, funds supplied by
3 the Bureau of Indian Affairs; and

4 “(2) may not be used—

5 “(A) to provide any Federal cost-sharing
6 contribution on behalf of a State or local gov-
7 ernment;

8 “(B) to pay a ransom;

9 “(C) by or for a non-United States entity;

10 or

11 “(D) for any recreational or social purpose.

12 “(g) AUTHORIZATION OF APPROPRIATIONS.—There
13 are authorized to be appropriated to carry out this section
14 \$75,000,000 for each of fiscal years 2022 through 2026.

15 “(h) TRANSFERS AUTHORIZED.—During a fiscal
16 year, the Secretary or the head of any component of the
17 Department that administers the State and Local Cyber-
18 security Grant Program may transfer not more than 5
19 percent of the amounts appropriated pursuant to sub-
20 section (g) or other amounts appropriated to carry out the
21 National Cyber Resilience Assistance Fund for that fiscal
22 year to an account of the Department for salaries, ex-
23 penses, and other administrative costs incurred for the
24 management, administration, or evaluation of this sec-
25 tion.”.

1 (c) TECHNICAL AND CONFORMING AMENDMENTS.—

2 (1) TABLE OF CONTENTS.—The table of con-
 3 tents in section 1(b) of the Homeland Security Act
 4 of 2002 (Public Law 107–296; 116 Stat. 2135) is
 5 amended by striking the item relating to section
 6 2214 and all that follows through the item relating
 7 to section 2217 and inserting the following:

“Sec. 2214. National Asset Database.

“Sec. 2215. Duties and authorities relating to .gov internet domain.

“Sec. 2216. Joint Cyber Planning Office.

“Sec. 2217. Cybersecurity State Coordinator.

“Sec. 2218. Sector Risk Management Agencies.

“Sec. 2219. Cybersecurity Advisory Committee.

“Sec. 2220. Cybersecurity education and training programs.

“Sec. 2220A. National Cyber Resilience Assistance Fund.”.

8 (2) ADDITIONAL TECHNICAL AMENDMENT.—

9 (A) AMENDMENT.—Section 904(b)(1) of
 10 the DOTGOV Act of 2020 (title IX of division
 11 U of Public Law 116–260) is amended, in the
 12 matter preceding subparagraph (A), by striking
 13 “Homeland Security Act” and inserting
 14 “Homeland Security Act of 2002”.

15 (B) EFFECTIVE DATE.—The amendment
 16 made by subparagraph (A) shall take effect as
 17 if enacted as part of the DOTGOV Act of 2020
 18 (title IX of division U of Public Law 116–260).

1 **TITLE II—IMPROVING THE ABIL-**
2 **ITY OF THE FEDERAL GOV-**
3 **ERNMENT TO ASSIST IN EN-**
4 **HANCING CRITICAL INFRA-**
5 **STRUCTURE CYBER RESIL-**
6 **IENCE**

7 **SEC. 201. INSTITUTE A 5-YEAR TERM FOR THE CYBERSECU-**
8 **RITY AND INFRASTRUCTURE SECURITY DI-**
9 **RECTOR.**

10 (a) IN GENERAL.—Subsection (b)(1) of section 2202
11 of the Homeland Security Act of 2002 (6 U.S.C. 652),
12 is amended by inserting “The Director shall be appointed
13 for a term of 5 years.” after “who shall report to the Sec-
14 retary.”.

15 (b) TRANSITION RULES.—The amendment made by
16 subsection (a) shall take effect on the earlier of—

17 (1) the first appointment of an individual to the
18 position of Director of the Cybersecurity and Infra-
19 structure Protection Agency of the Department of
20 Homeland Security, by and with the advice and con-
21 sent of the Senate, that is made on or after the date
22 of enactment of this Act; or

23 (2) January 1, 2022.

1 **SEC. 202. CREATE A JOINT COLLABORATIVE ENVIRON-**
2 **MENT.**

3 (a) IN GENERAL.—The Director of the Cybersecurity
4 and Infrastructure Security Agency shall establish a joint,
5 cloud-based, information sharing environment to—

6 (1) integrate the Federal Government’s unclas-
7 sified and classified cyber threat information,
8 malware forensics, and data related to cybersecurity
9 risks (as defined in section 2209 of the Homeland
10 Security Act of 2002 (6 U.S.C. 659)) that is derived
11 from network sensor programs;

12 (2) enable cross-correlation of threat data at
13 the speed and scale necessary for rapid detection
14 and identification;

15 (3) enable query and analysis by appropriate
16 operators across the Federal Government;

17 (4) facilitate a whole-of-Government, com-
18 prehensive understanding of the cyber threats to the
19 resilience of the Federal Government and national
20 critical infrastructure networks;

21 (5) enable and support the private-public cyber-
22 security collaboration efforts of the Federal Govern-
23 ment, whose successes will be directly dependent on
24 the accuracy, comprehensiveness, and timeliness of
25 threat information collected and held by the Federal
26 Government; and

1 (6) enable data curation for artificial intel-
2 ligence models and provide an environment to enable
3 the Federal Government to curate data and build
4 applications.

5 (b) DEVELOPMENT.—

6 (1) INITIAL EVALUATION.—Not later than 180
7 days after the date of enactment of this Act, the Di-
8 rector of the Cybersecurity and Infrastructure Secu-
9 rity Agency, in coordination with the Director
10 shall—

11 (A) identify all Federal sources of classi-
12 fied and unclassified cyber threat information;

13 (B) evaluate all programs, applications, or
14 platforms of the Federal Government that are
15 intended to detect, identify, analyze, or monitor
16 cyber threats against the resiliency of the Fed-
17 eral Government or critical infrastructure; and

18 (C) submit a recommendation to the Presi-
19 dent identifying Federal programs to be des-
20 ignated and required to participate in the Infor-
21 mation Sharing Environment, including—

22 (i) Government network-monitoring
23 and intrusion detection programs;

24 (ii) cyber threat indicator-sharing pro-
25 grams and Government-sponsored network

1 sensors or network-monitoring programs
2 for the private sector or for State, local,
3 tribal, and territorial governments;

4 (iii) incident response and cybersecu-
5 rity technical assistance programs; and

6 (iv) malware forensics and reverse-en-
7 gineering programs.

8 (2) DESIGNATION OF PARTICIPATING PRO-
9 GRAMS.—Not later than 60 days after completion of
10 the evaluation required under paragraph (1), the
11 President shall issue a determination designating the
12 departments, agencies, Federal programs, and cor-
13 responding systems and assets that are required to
14 be a part of the Information Sharing Environment.

15 (3) DESIGN.—Not later than 1 year after com-
16 pletion of the evaluation required under paragraph
17 (1), the Director of the Cybersecurity and Infra-
18 structure Security Agency, in consultation with the
19 Director, shall design the structure of a common
20 platform for sharing and fusing existing Government
21 information, insights, and data related to cyber
22 threats and threat actors, which, at a minimum,
23 shall—

24 (A) account for appropriate data standards
25 and interoperability requirements;

1 (B) enable integration of existing applica-
2 tions, platforms, data, and information, to in-
3 clude classified information;

4 (C) ensure access by such Federal depart-
5 ments and agencies as the Director of the Cy-
6 bersecurity and Infrastructure Security Agency
7 determines necessary;

8 (D) account for potential private sector
9 participation and partnerships;

10 (E) enable unclassified data to be inte-
11 grated with classified data;

12 (F) anticipate the deployment of analytic
13 tools across classification levels to leverage all
14 relevant data sets, as appropriate;

15 (G) identify tools and analytical software
16 that can be applied and shared to manipulate,
17 transform, and display data and other identified
18 needs;

19 (H) anticipate the integration of new tech-
20 nologies and data streams, including data re-
21 lated to cybersecurity risks derived from Gov-
22 ernment-sponsored voluntary network sensors
23 or network-monitoring programs for the private
24 sector or for State, local, Tribal, and territorial
25 governments; and

1 (I) appropriately account for departments,
2 agencies, programs, and systems and assets de-
3 termined to be required to participate by the
4 President under paragraph (2) in the Informa-
5 tion Sharing Environment.

6 (c) OPERATION.—The Information Sharing Environ-
7 ment shall be managed by the Director of the Cybersecu-
8 rity and Infrastructure Security Agency.

9 (d) POST-DEPLOYMENT ASSESSMENT.—Not later
10 than 1 year after the date on which the Information Shar-
11 ing Environment is established, the Director of the Cyber-
12 security and Infrastructure Security Agency and the Di-
13 rector shall assess the means by which the Information
14 Sharing Environment may be expanded to include the pri-
15 vate sector and critical infrastructure information sharing
16 organizations and, to the maximum extent practicable,
17 begin the process of such expansion.

18 (e) PRIVATE SECTOR SHARING INFORMATION SHAR-
19 ING PROTECTIONS.—To the extent any private entity
20 shares cyber threat indicators and defensive measures
21 through or with the Information Sharing Environment
22 and in a manner that is consistent with all requirements
23 under section 1752 of the William M. (Mac) Thornberry
24 National Defense Authorization Act for Fiscal Year 2021
25 (6 U.S.C. 1500), the Cybersecurity Information Sharing

1 Act of 2015 (6 U.S.C. 1501 et seq.), and any applicable
2 guidelines promulgated under subsection (f), such activi-
3 ties shall be considered to be authorized by and in accord-
4 ance with section 1752 of the William M. (Mac) Thorn-
5 berry National Defense Authorization Act for Fiscal Year
6 2021 and the Cybersecurity Information Sharing Act of
7 2015.

8 (f) PRIVACY AND CIVIL LIBERTIES.—

9 (1) GUIDELINES OF ATTORNEY GENERAL.—Not
10 later than 60 days after the date of enactment of
11 this Act, the Secretary of Homeland Security (acting
12 through the Director of the Cybersecurity and Infra-
13 structure Security Agency) and the Attorney Gen-
14 eral, shall jointly, and in coordination with heads of
15 the appropriate Federal entities and in consultation
16 with officers designated under section 1062 of the
17 National Security Intelligence Reform Act of 2004
18 (42 U.S.C. 2000ee–1), develop, submit to Congress,
19 and make available to the public interim guidelines
20 relating to privacy and civil liberties which shall gov-
21 ern the receipt, retention, use, and dissemination of
22 cyber threat indicators by a Federal entity obtained
23 in connection with activities authorized in this sec-
24 tion.

25 (2) FINAL GUIDELINES.—

1 (A) IN GENERAL.—Not later than 180
2 days after the date of enactment of this Act,
3 the Secretary of Homeland Security (acting
4 through the Director of the Cybersecurity and
5 Infrastructure Security Agency) and the Attor-
6 ney General, shall jointly, in coordination with
7 heads of the appropriate Federal entities and in
8 consultation with officers designated under sec-
9 tion 1062 of the National Security Intelligence
10 Reform Act of 2004 (42 U.S.C. 2000ee–1) and
11 such private entities with industry expertise as
12 the Secretary and the Attorney General con-
13 sider relevant, promulgate final guidelines relat-
14 ing to privacy and civil liberties which shall gov-
15 ern the receipt, retention, use, and dissemina-
16 tion of cyber threat indicators by a Federal en-
17 tity obtained in connection with activities au-
18 thorized in this section.

19 (B) PERIODIC REVIEW.—The Secretary of
20 Homeland Security (acting through the Direc-
21 tor of the Cybersecurity and Infrastructure Se-
22 curity Agency) and the Attorney General, shall
23 jointly, in coordination with heads of the appro-
24 priate Federal entities and in consultation with
25 officers and private entities described in sub-

1 paragraph (A), periodically, but not less fre-
2 quently than once every 2 years, review the
3 guidelines promulgated under subparagraph
4 (A).

5 (3) CONTENT.—The guidelines required by
6 paragraphs (1) and (2) shall, consistent with the
7 need to bolster the resilience of information systems
8 and mitigate cybersecurity threats—

9 (A) limit the effect on privacy and civil lib-
10 erties of activities by the Federal Government
11 under this section;

12 (B) limit the receipt, retention, use, and
13 dissemination of cyber threat indicators con-
14 taining personal information or information
15 that identifies specific persons, including by es-
16 tablishing—

17 (i) a process for the timely destruction
18 of such information that is known not to
19 be directly related to uses authorized under
20 this section; and

21 (ii) specific limitations on the length
22 of any period in which a cyber threat indi-
23 cator may be retained;

24 (C) include requirements to safeguard
25 cyber threat indicators containing personal in-

1 formation or information that identifies specific
2 persons from unauthorized access or acquisi-
3 tion, including appropriate sanctions for activi-
4 ties by officers, employees, or agents of the
5 Federal Government in contravention of such
6 guidelines;

7 (D) include procedures for notifying enti-
8 ties and Federal entities if information received
9 pursuant to this subsection is known or deter-
10 mined by a Federal entity receiving such infor-
11 mation not to constitute a cyber threat indi-
12 cator;

13 (E) protect the confidentiality of cyber
14 threat indicators containing personal informa-
15 tion or information that identifies specific per-
16 sons to the greatest extent practicable and re-
17 quire recipients to be informed that such indica-
18 tors may only be used for purposes authorized
19 under this section; and

20 (F) include steps that may be needed so
21 that dissemination of cyber threat indicators is
22 consistent with the protection of classified and
23 other sensitive national security information.

24 (g) OVERSIGHT OF GOVERNMENT ACTIVITIES.—

1 (1) BIENNIAL REPORT ON PRIVACY AND CIVIL
2 LIBERTIES.—Not later than 2 years after the date
3 of enactment of this Act, and not less frequently
4 than once every year thereafter, the Privacy and
5 Civil Liberties Oversight Board shall submit to Con-
6 gress and the President a report providing—

7 (A) an assessment of the effect on privacy
8 and civil liberties by the type of activities car-
9 ried out under this section; and

10 (B) an assessment of the sufficiency of the
11 guidelines established pursuant to subsection (f)
12 in addressing concerns relating to privacy and
13 civil liberties.

14 (2) BIENNIAL REPORT BY INSPECTORS GEN-
15 ERAL.—

16 (A) IN GENERAL.—Not later than 2 years
17 after the date of enactment of this Act, and not
18 less frequently than once every 2 years there-
19 after, the Inspector General of the Department
20 of Homeland Security, the Inspector General of
21 the Intelligence Community, the Inspector Gen-
22 eral of the Department of Justice, the Inspector
23 General of the Department of Defense, and the
24 Inspector General of the Department of Energy
25 shall, in consultation with the Council of In-

1 spectors General on Integrity and Efficiency,
2 jointly submit to Congress a report on the re-
3 ceipt, use, and dissemination of cyber threat in-
4 dicators and defensive measures that have been
5 shared with Federal entities under this section.

6 (B) CONTENTS.—Each report submitted
7 under subparagraph (A) shall include the fol-
8 lowing:

9 (i) A review of the types of cyber
10 threat indicators shared with Federal enti-
11 ties.

12 (ii) A review of the actions taken by
13 Federal entities as a result of the receipt
14 of such cyber threat indicators.

15 (iii) A list of Federal entities receiving
16 such cyber threat indicators.

17 (iv) A review of the sharing of such
18 cyber threat indicators among Federal en-
19 tities to identify inappropriate barriers to
20 sharing information.

21 (3) RECOMMENDATIONS.—Each report sub-
22 mitted under this subsection may include such rec-
23 ommendations as the Privacy and Civil Liberties
24 Oversight Board, with respect to a report submitted
25 under paragraph (1), or the Inspectors General re-

1 ferred to in paragraph (2)(A), with respect to a re-
2 port submitted under paragraph (2), may have for
3 improvements or modifications to the authorities
4 under this section.

5 (4) FORM.—Each report required under this
6 subsection shall be submitted in unclassified form,
7 but may include a classified annex.

8 (h) AUTHORIZATION OF APPROPRIATIONS.—There
9 are authorized to be appropriated to carry out this section
10 \$100,000,000 for each of fiscal years 2022 through 2026.

11 (i) DEFINITIONS.—In this section:

12 (1) CRITICAL INFRASTRUCTURE.—The term
13 “critical infrastructure” has the meaning given that
14 term in section 1016(e) of the Critical Infrastruc-
15 ture Protection Act of 2001 (42 U.S.C. 5195c(e)).

16 (2) DIRECTOR.—The term “Director” means
17 the National Cyber Director.

18 (3) INFORMATION SHARING ENVIRONMENT.—
19 The term “Information Sharing Environment”
20 means the information sharing environment estab-
21 lished under subsection (a).

1 **SEC. 203. DESIGNATE THREE CRITICAL TECHNOLOGY SE-**
2 **CURITY CENTERS.**

3 (a) IN GENERAL.—Section 307(b)(3) of the Home-
4 land Security Act of 2002 (6 U.S.C. 187(b)(3)), is amend-
5 ed—

6 (1) in the matter preceding subparagraph (A),
7 by inserting “national laboratories,” before “and
8 universities”;

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

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

13 (4) by adding at the end the following:

14 “(E) establish not less than 1, and not
15 more than 3, cybersecurity-focused critical tech-
16 nology security centers, in order to bolster the
17 overall resilience of the networks and critical in-
18 frastructure of the United States, to perform—

19 “(i) network technology security test-
20 ing, to test the security of cyber-related
21 hardware and software;

22 “(ii) connected industrial control sys-
23 tem security testing, to test the security of
24 connected programmable data logic con-
25 trollers, supervisory control and data ac-

1 quisition servers, and other cyber con-
2 nected industrial equipment; and

3 “(iii) open source software security
4 testing, to test and coordinate efforts to fix
5 vulnerabilities in open-source software.”.

6 (b) AUTHORIZATION OF APPROPRIATIONS.—There
7 are authorized to be appropriated to carry out the amend-
8 ments made by this section \$15,000,000 for each of fiscal
9 years 2022 through 2026.

10 **TITLE III—IMPROVING SECU-**
11 **RITY IN THE NATIONAL**
12 **CYBER ECOSYSTEM**

13 **SEC. 301. ESTABLISH A NATIONAL CYBERSECURITY CER-**
14 **TIFICATION AND LABELING AUTHORITY.**

15 (a) DEFINITIONS.—In this section:

16 (1) ACCREDITED CERTIFYING AGENT.—The
17 term “accredited certifying agent” means any person
18 who is accredited by the Authority as a certifying
19 agent for the purposes of certifying a specific class
20 of critical information and communications tech-
21 nology.

22 (2) AUTHORITY.—The term “Authority” means
23 the National Cybersecurity Certification and Label-
24 ing Authority established under subsection (b)(1).

1 (3) CERTIFICATION.—The term “certification”
2 means a seal or symbol provided by the Authority or
3 an accredited certifying agent, that results from pas-
4 sage of a comprehensive evaluation of an informa-
5 tion and communications technology that establishes
6 the extent to which a particular design and imple-
7 mentation meets a set of specified security stand-
8 ards.

9 (4) CRITICAL INFORMATION AND COMMUNICA-
10 TIONS TECHNOLOGY.—The term “critical informa-
11 tion and communications technology” means infor-
12 mation and communications technology that is in
13 use in critical infrastructure sectors and that under-
14 pins the resilience of national critical functions, as
15 determined by the Secretary.

16 (5) CRITICAL INFRASTRUCTURE.—The term
17 “critical infrastructure” has the meaning given that
18 term in section 1016(e) of the Critical Infrastruc-
19 ture Protection Act of 2001 (42 U.S.C. 5195c(e)).

20 (6) LABEL.—The term “label” means a clear,
21 visual, and easy to understand symbol or list that
22 conveys specific information about a product’s secu-
23 rity attributes, characteristics, functionality, compo-
24 nents, or other features.

1 (7) PROGRAM.—The term “Program” means
2 the program administered under subsection (b)(1).

3 (8) SECRETARY.—The term “Secretary” means
4 the Secretary of Homeland Security.

5 (b) NATIONAL CYBERSECURITY CERTIFICATION AND
6 LABELING AUTHORITY.—

7 (1) ESTABLISHMENT.—There is established a
8 National Cybersecurity Certification and Labeling
9 Authority for the purpose of establishing and admin-
10 istering a voluntary national cybersecurity certifi-
11 cation and labeling program for critical information
12 and communications technology in order to bolster
13 the resilience of the networks and critical infrastruc-
14 ture of the United States.

15 (2) PROGRAMS.—

16 (A) ACCREDITATION OF CERTIFYING
17 AGENTS.—As part of the Program, the Author-
18 ity shall define and publish a process whereby
19 governmental and nongovernmental entities
20 may apply to become accredited certifying
21 agents for the certification of specific critical in-
22 formation and communications technology, in-
23 cluding—

24 (i) smartphones;

25 (ii) tablets;

- 1 (iii) laptop computers;
- 2 (iv) operating systems;
- 3 (v) routers;
- 4 (vi) software-as-a-service;
- 5 (vii) infrastructure-as-a-service;
- 6 (viii) platform-as-a-service;
- 7 (ix) programmable logic controllers;
- 8 (x) intelligent electronic devices; and
- 9 (xi) programmable automation con-
- 10 trollers.

11 (B) IDENTIFICATION OF STANDARDS,
12 FRAMEWORKS, AND BENCHMARKS.—As part of
13 the Program, the Authority shall work in co-
14 ordination with accredited certifying agents, the
15 Secretary, and subject matter experts from the
16 Federal Government, academia, nongovern-
17 mental organizations, and the private sector to
18 identify and harmonize common security stand-
19 ards, frameworks, and benchmarks against
20 which the security of critical information and
21 communications technologies may be measured.

22 (C) PRODUCT CERTIFICATION.—As part of
23 the Program, the Authority, in consultation
24 with the Secretary and other experts from the
25 Federal Government, academia, nongovern-

1 mental organizations, and the private sector,
2 shall—

3 (i) develop, and disseminate to accred-
4 ited certifying agents, guidelines to stand-
5 ardize the presentation of certifications to
6 communicate the level of security for crit-
7 ical information and communications tech-
8 nologies;

9 (ii) develop, or permit accredited certi-
10 fying agents to develop, certification cri-
11 teria for critical information and commu-
12 nications technologies based on identified
13 security standards, frameworks, and
14 benchmarks, through the work conducted
15 under subparagraph (B);

16 (iii) issue, or permit accredited certi-
17 fying agents to issue, certifications for crit-
18 ical information and communications tech-
19 nology that meet and comply with security
20 standards, frameworks, and benchmarks
21 identified through the work conducted
22 under subparagraph (B);

23 (iv) permit a manufacturer or dis-
24 tributor of critical information and commu-
25 nications technology to display a certificate

1 reflecting the extent to which the critical
2 information and communications tech-
3 nology meets security standards, frame-
4 works, and benchmarks identified through
5 the work conducted under subparagraph
6 (B);

7 (v) remove the certification of a crit-
8 ical information and communications tech-
9 nology as a critical information and com-
10 munications technology certified under the
11 Program if the manufacturer of the cer-
12 tified critical information and communica-
13 tions technology falls out of conformity
14 with the benchmarks security standards,
15 frameworks, or benchmarks identified
16 through the work conducted under sub-
17 paragraph (B) for the critical information
18 and communications technology;

19 (vi) work to enhance public awareness
20 of the certification and labeling efforts of
21 the Authority and accredited certifying
22 agents, including through public outreach,
23 education, research and development, and
24 other means; and

1 (vii) publicly display a list of labels
2 and certified critical information and com-
3 munications technology, along with their
4 respective certification information.

5 (D) CERTIFICATIONS.—

6 (i) IN GENERAL.—A certification shall
7 remain valid for 1 year from the date of
8 issuance.

9 (ii) CLASSES OF CERTIFICATION.—In
10 developing the guidelines and criteria re-
11 quired under subparagraph (C)(i), the Au-
12 thority shall designate at least 3 classes of
13 certifications, including the following:

14 (I) For critical information and
15 communications technology which the
16 product manufacturer or service pro-
17 vider attests meets the criteria for a
18 certification, attestation-based certifi-
19 cation.

20 (II) For critical information and
21 communications technology products
22 and services that have undergone
23 third-party accreditation of criteria
24 for certification, accreditation-based
25 certification.

1 (III) For critical information and
2 communications technology that has
3 undergone a security evaluation and
4 testing process by a qualifying third
5 party, as determined by the Authority,
6 test-based certification.

7 (E) PRODUCT LABELING.—The Authority,
8 in consultation with the Secretary and other ex-
9 perts from the Federal Government, academia,
10 nongovernmental organizations, and the private
11 sector, shall—

12 (i) collaborate with the private sector
13 to standardize language and define a label-
14 ing schema to provide transparent infor-
15 mation on the security characteristics and
16 constituent components of a software or
17 hardware product; and

18 (ii) establish a mechanism by which
19 product developers can provide this infor-
20 mation for both product labeling and pub-
21 lic posting.

22 (3) ENFORCEMENT.—

23 (A) IN GENERAL.—It shall be unlawful for
24 a product manufacturer, distributor, or seller
25 to—

1 (i) falsely attest to, or falsify an audit
2 or test for, a security standard, framework,
3 or benchmark for certification;

4 (ii) intentionally mislabel a product;
5 or

6 (iii) fail to maintain the security
7 standard, framework, or benchmark to
8 which the manufacturer, distributor, or
9 seller attested.

10 (B) ENFORCEMENT BY FEDERAL TRADE
11 COMMISSION.—

12 (i) UNFAIR OR DECEPTIVE ACTS OR
13 PRACTICES.—A violation of subparagraph
14 (A) shall be treated as an unfair and de-
15 ceptive act or practice in violation of a reg-
16 ulation under section 18(a)(1)(B) of the
17 Federal Trade Commission Act (15 U.S.C.
18 57a(a)(1)(B)) regarding unfair or decep-
19 tive acts or practices.

20 (ii) POWERS OF COMMISSION.—

21 (I) IN GENERAL.—The Federal
22 Trade Commission shall enforce this
23 paragraph in the same manner, by the
24 same means, and with the same juris-
25 diction, powers, and duties as though

1 all applicable terms and provisions of
2 the Federal Trade Commission Act
3 (15 U.S.C. 41 et seq.) were incor-
4 porated into and made a part of this
5 paragraph.

6 (II) PRIVILEGES AND IMMUNI-
7 TIES.—Any person who violates this
8 paragraph shall be subject to the pen-
9 alties and entitled to the privileges
10 and immunities provided in the Fed-
11 eral Trade Commission Act (15
12 U.S.C. 41 et seq.).

13 (c) SELECTION OF THE AUTHORITY.—

14 (1) SELECTION.—The Secretary shall issue a
15 notice of funding opportunity and select, on a com-
16 petitive basis, a nonprofit, nongovernmental organi-
17 zation to serve as the Authority for a period of 5
18 years.

19 (2) ELIGIBILITY FOR SELECTION.—The Sec-
20 retary may only select an organization to serve as
21 the Authority if such organization—

22 (A) is a nongovernmental, nonprofit orga-
23 nization that is—

1 (i) exempt from taxation under sec-
2 tion 501(a) of the Internal Revenue Code
3 of 1986; and

4 (ii) described in sections 501(c)(3)
5 and 170(b)(1)(A)(vi) of that Code;

6 (B) has a demonstrable track record of
7 work on cybersecurity and information security
8 standards, frameworks, and benchmarks; and

9 (C) possesses requisite staffing and exper-
10 tise, with demonstrable prior experience in tech-
11 nology security or safety standards, frame-
12 works, and benchmarks, as well as certification.

13 (3) APPLICATION.—The Secretary shall estab-
14 lish a process by which a nonprofit, nongovern-
15 mental organization that seeks to be selected as the
16 Authority may apply for consideration.

17 (4) PROGRAM EVALUATION.—Not later than
18 the date that is 4 years after the initial selection
19 pursuant paragraph (1), and every 4 years there-
20 after, the Secretary shall—

21 (A) assess the effectiveness of the labels
22 and certificates produced by the Authority, in-
23 cluding—

24 (i) assessing the costs to businesses
25 that manufacture critical information and

1 communications technology participating in
2 the Program;

3 (ii) evaluating the level of participa-
4 tion in the Program by businesses that
5 manufacture critical information and com-
6 munications technology; and

7 (iii) assessing the level of public
8 awareness and consumer awareness of the
9 label;

10 (B) audit the impartiality and fairness of
11 the Authority's activities conducted under this
12 section;

13 (C) issue a public report on the assessment
14 most recently carried out under subparagraph
15 (A) and the audit most recently carried out
16 under subparagraph (B); and

17 (D) brief Congress on the findings of the
18 Secretary with respect to the most recent as-
19 sessment under subparagraph (A) and the most
20 recent audit under subparagraph (B).

21 (5) RENEWAL.—After the initial selection pur-
22 suant to paragraph (1), the Secretary shall, every 5
23 years—

1 (A) accept applications from nonprofit,
 2 nongovernmental organizations seeking selection
 3 as the Authority; and

4 (B) following competitive consideration of
 5 all applications—

6 (i) renew the selection of the organiza-
 7 tion serving as the Authority; or

8 (ii) select another applicant organiza-
 9 tion to serve as the Authority.

10 (d) AUTHORIZATION OF APPROPRIATIONS.—There
 11 are authorized to be appropriated to carry out this section
 12 \$25,000,000 for each of fiscal years 2022 through 2026.

13 **SEC. 302. ESTABLISH THE BUREAU OF CYBERSECURITY**
 14 **STATISTICS.**

15 (a) DEFINITIONS.—In this section:

16 (1) BUREAU.—The term “Bureau” means the
 17 Bureau of Cybersecurity Statistics established under
 18 subsection (b).

19 (2) COVERED ENTITY.—The term “covered en-
 20 tity” means any nongovernmental organization, cor-
 21 poration, trust, partnership, sole proprietorship, un-
 22 incorporated association, or venture (without regard
 23 to whether it is established for profit) that is en-
 24 gaged in or affecting interstate commerce and that

1 provides cybersecurity incident response services or
2 cybersecurity insurance products.

3 (3) CYBER INCIDENT.—The term cyber incident
4 includes each of the following:

5 (A) Unauthorized access to an information
6 system or network that leads to loss of con-
7 fidentiality, integrity, or availability of that in-
8 formation system or network.

9 (B) Disruption of business operations due
10 to a distributed denial of service attack against
11 an information system or network.

12 (C) Unauthorized access or disruption of
13 business operations due to loss of service facili-
14 tated through, or caused by a cloud service pro-
15 vider, managed service provider, or other data
16 hosting provider.

17 (D) Fraudulent or malicious use of a cloud
18 service account, data hosting account, internet
19 service account, or any other digital service.

20 (4) DIRECTOR.—The term “Director” means
21 the Director of the Bureau.

22 (5) STATISTICAL PURPOSE.—The term “statistical
23 purpose”—

24 (A) means the description, estimation, or
25 analysis of the characteristics of groups, with-

1 out identifying the individuals or organizations
2 that comprise such groups; and

3 (B) includes the development, implementa-
4 tion, or maintenance of methods, technical or
5 administrative procedures, or information re-
6 sources that support the purposes described in
7 subsection (e).

8 (b) ESTABLISHMENT.—There is established within
9 the Department of Homeland Security a Bureau of Cyber-
10 security Statistics.

11 (c) DIRECTOR.—

12 (1) IN GENERAL.—The Bureau shall be headed
13 by a Director, who shall—

14 (A) report to the Secretary of Homeland
15 Security; and

16 (B) be appointed by the President.

17 (2) AUTHORITY.—The Director shall—

18 (A) have final authority for all cooperative
19 agreements and contracts awarded by the Bu-
20 reau;

21 (B) be responsible for the integrity of data
22 and statistics collected or issued by the Bureau;
23 and

24 (C) protect against improper or illegal use
25 or disclosure of information furnished for exclu-

1 sively statistical purposes under this section,
2 consistent with the requirements of subsection
3 (f).

4 (3) QUALIFICATIONS.—The Director—

5 (A) shall have experience in statistical pro-
6 grams; and

7 (B) shall not—

8 (i) engage in any other employment;

9 or

10 (ii) hold any office in, or act in any
11 capacity for, any organization, agency, or
12 institution with which the Bureau makes
13 any contract or other arrangement under
14 this section.

15 (4) DUTIES AND FUNCTIONS.—The Director
16 shall—

17 (A) collect and analyze information con-
18 cerning cybersecurity, including data related to
19 cyber incidents, cyber crime, and any other area
20 the Director determines appropriate;

21 (B) collect and analyze data that will serve
22 as a continuous and comparable national indi-
23 cation of the prevalence, incidents, rates, ex-
24 tent, distribution, and attributes of all relevant
25 cyber incidents, as determined by the Director,

1 in support of national policy and decision mak-
2 ing;

3 (C) compile, collate, analyze, publish, and
4 disseminate uniform national cyber statistics
5 concerning any area that the Director deter-
6 mines appropriate;

7 (D) in coordination with the National In-
8 stitute of Standards and Technology, rec-
9 ommend national standards, metrics, and meas-
10 urement criteria for cyber statistics and for en-
11 suring the reliability and validity of statistics
12 collected pursuant to this subsection;

13 (E) conduct or support research relating to
14 methods of gathering or analyzing cyber statis-
15 tics;

16 (F) enter into cooperative agreements or
17 contracts with public agencies, institutions of
18 higher education, or private organizations for
19 purposes related to this subsection;

20 (G) provide appropriate information to the
21 President, the Congress, Federal agencies, the
22 private sector, and the general public on cyber
23 statistics;

24 (H) maintain liaison with State and local
25 governments concerning cyber statistics;

1 (I) confer and cooperate with Federal sta-
2 tistical agencies as needed to carry out the pur-
3 poses of this section, including by entering into
4 cooperative data sharing agreements in con-
5 formity with all laws and regulations applicable
6 to the disclosure and use of data; and

7 (J) request from any person or entity in-
8 formation, data, and reports as may be required
9 to carry out the purposes of this subsection.

10 (d) FURNISHMENT OF INFORMATION, DATA, OR RE-
11 PORTS BY FEDERAL DEPARTMENTS AND AGENCIES.—
12 Federal departments and agencies requested by the Direc-
13 tor to furnish information, data, or reports pursuant to
14 subsection (c)(4)(J) shall provide to the Bureau such in-
15 formation as the Director determines necessary to carry
16 out the purposes of this section.

17 (e) FURNISHMENT OF CYBER INCIDENT INFORMA-
18 TION, DATA, OR REPORTS TO THE BUREAU BY THE PRI-
19 VATE SECTOR.—

20 (1) IN GENERAL.—Not later than 180 days
21 after the date of enactment of this Act, and every
22 180 days thereafter, each covered entity shall submit
23 to the Bureau a report containing such data and in-
24 formation as the Director determines necessary to
25 carry out the purposes of this section.

1 (2) DETERMINATION OF DATA AND INFORMA-
2 TION NECESSARY TO CARRY OUT THE PURPOSES OF
3 THIS SECTION.—Not later than 90 days after the
4 date of enactment of this Act, and annually there-
5 after, the Director shall publish a list of data and
6 information determined necessary to carry out the
7 purposes of this section, including individual descrip-
8 tions of cyber incidents, which shall include—

9 (A) identification of the affected databases,
10 information systems, or devices that were, or
11 are reasonably believed to have been accessed
12 by an unauthorized person;

13 (B) where applicable, a description of the
14 vulnerabilities, tactics, techniques, and proce-
15 dures used;

16 (C) where applicable, any identifying infor-
17 mation related to the malicious actors who per-
18 petrated the incident;

19 (D) where applicable any cybersecurity
20 controls implemented by the victim organiza-
21 tion; and

22 (E) the industrial sectors, regions, and size
23 of affected entities (as determined by number of
24 employees) without providing any information

1 that can reasonably be expected to identify such
2 entities.

3 (3) STANDARDS FOR SUBMISSION OF INFORMA-
4 TION AND DATA.—Not later than 180 days after the
5 date of enactment of this Act, the Director shall, in
6 consultation with covered entities, develop standard-
7 ized procedures for the submission of data and infor-
8 mation the Director determines necessary to carry
9 out the purposes of this section.

10 (4) PRIVATE SECTOR REPORTING.—Not later
11 than 90 days after the date on which the Director
12 develops the standards required under paragraph
13 (3), the Director shall—

14 (A) publish the processes for submission of
15 information, data, and reports by covered enti-
16 ties; and

17 (B) begin accepting reporting required
18 under paragraph (1).

19 (5) REGULATORY USE.—Information disclosed
20 to the Bureau under this section that is not other-
21 wise available, shall not be used by the Federal Gov-
22 ernment or any State, local, tribal, or territorial gov-
23 ernment to sanction or otherwise punish the entity
24 disclosing the information, or the entity in which the
25 cyber incident initially occurred.

1 (6) PRESERVATION OF PRIVILEGE.—Disclosure
2 of information pursuant to this section or by a cov-
3 ered entity to the Bureau shall not waive any other-
4 wise applicable privilege, immunity, or protection
5 provided by law.

6 (7) PRESERVATION OF EXISTING OBLIGA-
7 TIONS.—Nothing in this section shall modify, pre-
8 vent, or abrogate any notice or notification obliga-
9 tions under Federal contracts, enforceable agree-
10 ments with the government, or other Federal law.

11 (8) ENFORCEMENT.—

12 (A) UNFAIR OR DECEPTIVE ACTS OR PRAC-
13 TICES.—Compliance with the requirements im-
14 posed under this subsection by covered entities
15 shall be enforced by the Federal Trade Com-
16 mission under the Federal Trade Commission
17 Act (15 U.S.C. 41 et seq.). For the purpose of
18 the exercise by the Federal Trade Commission
19 of its functions and powers under the Federal
20 Trade Commission Act, a violation of any re-
21 quirement or prohibition imposed under this
22 subsection shall be treated as an unfair and de-
23 ceptive act or practice in violation of a regula-
24 tion under section 18(a)(1)(B) of the Federal
25 Trade Commission Act (15 U.S.C.

1 57a(a)(1)(B)) regarding unfair or deceptive
2 acts or practices.

3 (B) POWERS OF COMMISSION.—Subject to
4 subparagraph (C), the Federal Trade Commis-
5 sion shall enforce this subsection in the same
6 manner, by the same means, and with the same
7 jurisdiction, powers, and duties as though all
8 applicable terms and provisions of the Federal
9 Trade Commission Act (15 U.S.C. 41 et seq.)
10 were incorporated into and made a part of this
11 subsection.

12 (C) ADDITIONAL ENTITIES.—

13 (i) IN GENERAL.—Notwithstanding
14 sections 4, 5(a)(2), or 6 of the Federal
15 Trade Commission Act (15 U.S.C. 44,
16 45(a)(2), 46) or any jurisdictional limita-
17 tion of the Federal Trade Commission, the
18 Federal Trade Commission shall also en-
19 force this subsection, in the same manner
20 provided in subparagraph (A) of this para-
21 graph, with respect to—

22 (I) organizations not organized to
23 carry on business for their own profit
24 or that of their members; and

1 (II) common carriers subject to
2 the Communications Act of 1934 (47
3 U.S.C. 151 et seq.).

4 (ii) COORDINATION AND NOTICE.—
5 The Federal Trade Commission shall—

6 (I) coordinate with the Federal
7 Communications Commission regard-
8 ing enforcement of this subsection
9 with respect to common carriers sub-
10 ject to the Communications Act of
11 1934 (47 U.S.C. 151 et seq.);

12 (II) notify the Bureau of Con-
13 sumer Financial Protection regarding
14 enforcement of this subsection with
15 respect to information associated with
16 the provision of financial products or
17 services by an entity that provides a
18 consumer financial product or service
19 (as defined in section 1002 of the
20 Consumer Financial Protection Act of
21 2010 (12 U.S.C. 5481)); and

22 (III) for enforcement of this sub-
23 section with respect to matters impli-
24 cating the jurisdiction or authorities

1 of another Federal agency, notify that
2 agency as appropriate.

3 (D) PRIVILEGES AND IMMUNITIES.—Any
4 covered entity that violates the requirements
5 imposed under this subsection shall be subject
6 to the penalties and entitled to the privileges
7 and immunities provided in the Federal Trade
8 Commission Act (15 U.S.C. 41 et seq.).

9 (E) CONSTRUCTION.—Nothing in this
10 paragraph shall be construed to limit the au-
11 thority of the Federal Trade Commission under
12 any other provision of law.

13 (f) PROTECTION OF INFORMATION.—

14 (1) IN GENERAL.—No officer or employee of
15 the Federal Government or agent of the Federal
16 Government may, without the consent of the indi-
17 vidual, entity, agency, or other person who is the
18 subject of the submission or provides the submis-
19 sion—

20 (A) use any submission that is furnished
21 for exclusively statistical purposes under this
22 section for any purpose other than the statis-
23 tical purposes for which the submission is fur-
24 nished;

1 (B) make any publication or media trans-
2 mittal of the data contained in a submission de-
3 scribed in subparagraph (A) that permits infor-
4 mation concerning individual entities or indi-
5 vidual incidents to be reasonably inferred by ei-
6 ther direct or indirect means; or

7 (C) permit anyone other than a sworn offi-
8 cer, employee, agent, or contractor of the Bu-
9 reau to examine an individual submission de-
10 scribed in subsection (e).

11 (2) IMMUNITY FROM LEGAL PROCESS.—Any
12 submission (including any data derived from the
13 submission) that is collected and retained by the Bu-
14 reau, or an officer, employee, agent, or contractor of
15 the Bureau, for exclusively statistical purposes under
16 this section shall be immune from the legal process
17 and shall not, without the consent of the individual,
18 entity, agency, or other person who is the subject of
19 the submission or provides the submission, be admit-
20 ted as evidence or used for any purpose in any ac-
21 tion, suit, or other judicial or administrative pro-
22 ceeding.

23 (3) RULE OF CONSTRUCTION.—Nothing in this
24 subsection shall be construed to provide immunity
25 from the legal process for a submission (including

1 any data derived from the submission) if the submis-
2 sion is in the possession of any person, agency, or
3 entity other than the Bureau or an officers, em-
4 ployee, agent, or contractor of the Bureau, or if the
5 submission is independently collected, retained, or
6 produced for purposes other than the purposes of
7 this section.

8 (g) AUTHORIZATION OF APPROPRIATION.—There are
9 authorized to be appropriated such sums as may be nec-
10 essary to carry out this section. Such funds shall remain
11 available until expended.

12 **SEC. 303. SECURE FOUNDATIONAL INTERNET PROTOCOLS.**

13 (a) DEFINITIONS.—In this section:

14 (1) BORDER GATEWAY PROTOCOL.—The term
15 “border gateway protocol” means a protocol de-
16 signed to optimize routing of information exchanged
17 through the internet.

18 (2) DOMAIN NAME SYSTEM.—The term “do-
19 main name system” means a system that stores in-
20 formation associated with domain names in a dis-
21 tributed database on networks.

22 (3) INFORMATION AND COMMUNICATIONS
23 TECHNOLOGY INFRASTRUCTURE PROVIDERS.—The
24 term “information and communications technology
25 infrastructure providers” means all systems that en-

1 able connectivity and operability of internet service,
2 backbone, cloud, web hosting, content delivery, do-
3 main name system, and software-defined networks
4 and other systems and services.

5 (b) CREATION OF A STRATEGY TO SECURE
6 FOUNDATIONAL INTERNET PROTOCOLS.—

7 (1) PROTOCOL SECURITY STRATEGY.—In order
8 to secure foundational internet protocols, not later
9 than December 31, 2021, the National Tele-
10 communications and Information Administration
11 and the Department of Homeland Security shall
12 submit to Congress a strategy to secure the border
13 gateway protocol and the domain name system.

14 (2) STRATEGY REQUIREMENTS.—The strategy
15 required under paragraph (1) shall—

16 (A) articulate the security and privacy ben-
17 efits of implementing security for the border
18 gateway protocol and the domain name system
19 and the burdens of implementation and the en-
20 tities on whom those burdens will most likely
21 fall;

22 (B) identify key United States and inter-
23 national stakeholders;

24 (C) outline identified security measures
25 that could be used to secure or provide authen-

1 tication for the border gateway protocol and the
2 domain name system;

3 (D) identify any barriers to implementing
4 security for the border gateway protocol and the
5 domain name system at scale;

6 (E) propose a strategy to implement iden-
7 tified security measures at scale, accounting for
8 barriers to implementation and balancing bene-
9 fits and burdens, where feasible; and

10 (F) provide an initial estimate of the total
11 cost to the Government and implementing enti-
12 ties in the private sector of implementing secu-
13 rity for the border gateway protocol and the do-
14 main name system and propose recommenda-
15 tions for defraying these costs, if applicable.

16 (3) CONSULTATION.—In developing the strat-
17 egy required under paragraph (1) the National Tele-
18 communications and Information Administration
19 and the Department of Homeland Security shall
20 consult with information and communications tech-
21 nology infrastructure providers, civil society organi-
22 zations, relevant nonprofit organizations, and aca-
23 demic experts.

1 **TITLE IV—SYSTEMICALLY IM-**
2 **PORTANT CRITICAL INFRA-**
3 **STRUCTURE**

4 **SEC. 401. DEFINITIONS.**

5 In this title:

6 (1) **APPROPRIATE CONGRESSIONAL COMMIT-**
7 **TEES.**—The term “appropriate congressional com-
8 mittees” means the Committee on Homeland Secu-
9 rity and Governmental Affairs of the Senate and the
10 Committee on Homeland Security of the House of
11 Representatives.

12 (2) **CRITICAL INFRASTRUCTURE.**—The term
13 “critical infrastructure” has the meaning given that
14 term in section 1016(e) of the Critical Infrastruc-
15 ture Protection Act of 2001 (42 U.S.C. 5195c(e)).

16 (3) **DEPARTMENT.**—The term “Department”
17 means the Department of Homeland Security.

18 (4) **ENTITY.**—The term “entity” means a non-
19 Federal entity and a private entity, as such terms
20 are defined under section 102 of the Cybersecurity
21 Information Sharing Act of 2015 (6 U.S.C. 1501).

22 (5) **NATIONAL CRITICAL FUNCTIONS.**—The
23 term “national critical functions” means functions of
24 government and the private sector so vital to the
25 United States that their disruption, corruption, or

1 dysfunction would have a debilitating effect on secu-
2 rity, national economic security, national public
3 health or safety, or any combination thereof.

4 (6) SECRETARY.—The term “Secretary” means
5 the Secretary of Homeland Security.

6 (7) STAKEHOLDERS.—The term “stakeholders”
7 means persons or groups whose consultation may aid
8 the Secretary in exercising the authority of the Sec-
9 retary under this title, including—

10 (A) Sector Coordinating Councils within
11 the Critical Infrastructure Partnership Advisory
12 Council, established under section 871 of the
13 Homeland Security Act of 2002 (6 U.S.C. 451);

14 (B) the State, Local, Tribal and Territorial
15 Government Coordinating Council, within the
16 Critical Infrastructure Partnership Advisory
17 Council, established under section 871 of the
18 Homeland Security Act of 2002 (6.U.S.C. 451);

19 (C) the Cybersecurity Advisory Committee
20 established under section 2219 of the Homeland
21 Security Act of 2002 (6 U.S.C. 665e), as so re-
22 designated by section 101 of this Act;

23 (D) the National Security Telecommuni-
24 cations Advisory Committee established pursu-

1 ant to Executive Order 12382 (47 Fed. Reg.
2 40531); and

3 (E) the National Infrastructure Advisory
4 Council, established pursuant to Executive
5 Order 13231 (66 Fed. Reg. 53063).

6 (8) SYSTEMICALLY IMPORTANT CRITICAL IN-
7 FRASTRUCTURE.—The term “Systemically Impor-
8 tant Critical Infrastructure” means an entity that
9 has been designated as such by the Secretary
10 through the process and procedures established
11 under section 402.

12 **SEC. 402. SYSTEMICALLY IMPORTANT CRITICAL INFRA-**
13 **STRUCTURE.**

14 (a) IN GENERAL.—The Secretary may designate en-
15 tities as Systemically Important Critical Infrastructure.

16 (b) ESTABLISHMENT OF METHODOLOGY AND CRI-
17 TERIA.—Prior to designating any entities as Systemically
18 Important Critical Infrastructure, the Secretary, in con-
19 sultation with the National Cyber Director, Sector Risk
20 Management Agencies, and appropriate stakeholders shall
21 develop—

22 (1) a methodology for identifying Systemically
23 Important Critical Infrastructure; and

1 (2) criteria for determining whether an entity
2 qualifies as Systemically Important Critical Infra-
3 structure.

4 (c) CONSIDERATIONS.—In establishing criteria for
5 determining whether an entity qualifies as Systemically
6 Important Critical Infrastructure, the Secretary shall con-
7 sider—

8 (1) the likelihood that disruption to or com-
9 promise of such an entity could cause a debilitating
10 effect on national security, economic security, public
11 health or safety, or any combination thereof;

12 (2) the extent to which damage, disruption, or
13 unauthorized access to such an entity either sepa-
14 rately or collectively, will disrupt the reliable oper-
15 ation of other critical infrastructure assets, or im-
16 pede provisioning of one or more national critical
17 functions;

18 (3) the extent to which national cybersecurity
19 resilience would be enhanced by deeper risk manage-
20 ment integration between Systemically Important
21 Critical Infrastructure entities and the Federal Gov-
22 ernment; and

23 (4) the extent to which compromise or unau-
24 thorized access of such an entity could separately or
25 collectively create widespread compromise of the

1 cyber ecosystem, significant portions of critical infra-
2 structure, or multiple critical infrastructure sectors.

3 (d) LIST.—

4 (1) IN GENERAL.—Not later than 1 year after
5 the date of enactment of this Act, the Secretary
6 shall complete an initial list of entities designated as
7 Systemically Important Critical Infrastructure.

8 (2) MAINTENANCE OF LIST.—The Secretary
9 shall maintain a comprehensive list of entities des-
10 ignated as Systemically Important Critical Infra-
11 structure, which shall be updated within 7 days of
12 a change in whether an entity qualifies as System-
13 ically Important Critical Infrastructure.

14 (e) ENTITY NOTIFICATIONS.—Not later than 90 days
15 after designating an entity as Systemically Important
16 Critical Infrastructure or removing the designation of an
17 entity as Systemically Important Critical Infrastructure,
18 the Secretary shall notify the entity.

19 (f) CONGRESSIONAL NOTIFICATIONS.—The Sec-
20 retary shall—

21 (1) not later than 30 days after the date of any
22 addition, modification, or removal of an entity from
23 the list of Significantly Important Critical Infra-
24 structure maintained under subsection (d), notify
25 the appropriate Congressional committees; and

1 (2) at least every 2 years, submit to the appro-
2 priate Congressional committees an updated com-
3 prehensive list of entities designated as Systemically
4 Important Critical Infrastructure, in conjunction
5 with each plan required pursuant to section 403.

6 **SEC. 403. PLAN FOR ENHANCEMENT OF SYSTEMICALLY IM-**
7 **PORTANT CRITICAL INFRASTRUCTURE**
8 **METHODOLOGY AND CAPABILITY.**

9 (a) IN GENERAL.—Not later than 180 days after the
10 date of enactment of this Act, and every 2 years thereafter
11 for 10 years, the Secretary, in consultation with Sector
12 Risk Management Agencies and appropriate stakeholders,
13 shall develop and submit to the appropriate congressional
14 committees a plan for enhancing the methodology of the
15 Department for identifying Systemically Important Crit-
16 ical Infrastructure, including a discussion of the progress
17 of the Department as of the date of submission of the plan
18 in implementing the plan.

19 (b) CONTENTS OF PLAN.—

20 (1) IN GENERAL.—The plan required under
21 subsection (a) shall include—

22 (A) the methodology and criteria used for
23 identifying and determining entities that qualify
24 as Systemically Important Critical Infrastruc-
25 ture as described in section 402(b) and the

1 analysis used to establish such methodology and
2 criteria;

3 (B) a proposed timeline for enhancing the
4 capabilities of the Department to expand the
5 list beyond the designated entities to also in-
6 clude facilities, systems, assets, or other rel-
7 evant units of critical infrastructure that may
8 further enhance the ability to manage risk of
9 Systemically Important Critical Infrastructure;

10 (C) information regarding the outreach by
11 the Department to stakeholders and other Sec-
12 tor Risk Management Agencies on such efforts,
13 including mechanisms for incorporation of in-
14 dustry feedback;

15 (D) information regarding the efforts of
16 the Department, and the associated challenges
17 with such efforts, to access information from
18 stakeholders and other Sector Risk Manage-
19 ment Agencies to identify Systemically Impor-
20 tant Critical Infrastructure;

21 (E) information regarding other critical in-
22 frastructure entity identification programs with-
23 in the Department and how they are being in-
24 corporated into the overarching process to iden-
25 tify Systemically Important Critical Infrastruc-

1 ture, which shall include the efforts of the De-
2 partment under section 9 of Executive Order
3 13636 (78 Fed. Reg. 11739), the National In-
4 frastructure Prioritization Program, and section
5 4 of Executive Order 14028 (86 Fed. Reg.
6 26633);

7 (F) any identified gaps in authorities or
8 resources required to successfully carry out the
9 process of identifying Systemically Important
10 Critical Infrastructure, including facilities, sys-
11 tems, assets, or other relevant units of critical
12 infrastructure, as well as legislative proposals to
13 address such gaps;

14 (G) an assessment of potential benefits for
15 entities designated as Systemically Important
16 Critical Infrastructure, which shall include an
17 assessment of—

18 (i) enhanced intelligence support and
19 information sharing;

20 (ii) prioritized Federal technical as-
21 sistance;

22 (iii) liability protection for entities
23 designated as Systemically Important Crit-
24 ical Infrastructure that conform to identi-
25 fied security standards for damages or

- 1 harm directly or indirectly caused by a
2 cyber incident;
- 3 (iv) prioritized emergency planning;
- 4 (v) benefits described in the final re-
5 port of the U.S. Cyberspace Solarium
6 Commission, dated March 2020; and
- 7 (vi) additional authorizations or re-
8 sources necessary to implement the bene-
9 fits assessed under this subparagraph; and
- 10 (H) an assessment of potential mecha-
11 nisms to improve the security of entities des-
12 ignated as Systemically Important Critical In-
13 frastructure, which shall include an assessment
14 of—
- 15 (i) risk-based cybersecurity perform-
16 ance standards for all Systemically Impor-
17 tant Critical Infrastructure entities, incor-
18 porating, to the greatest extent possible,
19 existing industry best practices, standards,
20 and guidelines;
- 21 (ii) sector-specific performance stand-
22 ards;
- 23 (iii) additional regulations to enhance
24 the security of Systemically Important
25 Critical Infrastructure against cyber risks,

1 including how to prevent duplicative re-
2 quirements for already regulated sectors;

3 (iv) cyber incident reporting require-
4 ments for entities designated as System-
5 ically Important Critical Infrastructure;
6 and

7 (v) additional authorizations or re-
8 sources necessary to implement the mecha-
9 nisms to improve the security of System-
10 ically Important Critical Infrastructure as-
11 sessed under this subparagraph.

12 (2) INITIAL PLAN.—The initial plan submitted
13 under this section shall include a detailed description
14 of the capabilities of the Department with respect to
15 identifying Systemically Important Critical Infra-
16 structure as they were on the date of enactment of
17 this Act.

18 (c) CLASSIFIED ANNEX.—The plan shall be in un-
19 classified form, but may include a classified annex, as the
20 Secretary determines necessary.

21 (d) PUBLICATION.—Not later than 30 days after the
22 date on which the Secretary submits a plan to Congress,
23 the Secretary shall make the plan available to relevant
24 stakeholders.

1 (e) RESTRICTION.—Subchapter I of chapter 35 of
2 title 44, United States Code, shall not apply to any action
3 to implement this section or to any exercise of the author-
4 ity of the Secretary pursuant to this section.

5 **TITLE V—ENABLING THE**
6 **NATIONAL CYBER DIRECTOR**

7 **SEC. 501. ESTABLISHMENT OF HIRING AUTHORITIES FOR**
8 **THE OFFICE OF THE NATIONAL CYBER DI-**
9 **RECTOR.**

10 Section 1752 of the William M. (Mac) Thornberry
11 National Defense Authorization Act for Fiscal Year 2021
12 (Public Law 116–283) is amended—

13 (1) in subsection (e)—

14 (A) in paragraph (1), by inserting “and in
15 accordance with paragraphs (3) through (7) of
16 this subsection,” after “and classification
17 laws,”;

18 (B) in paragraph (2), by inserting “not-
19 withstanding paragraphs (3) through (7) of this
20 subsection,” before “employ experts”;

21 (C) by redesignating paragraphs (3)
22 through (8) as paragraphs (8) through (13), re-
23 spectively; and

24 (D) by inserting after paragraph (2) the
25 following:

1 “(3) establish, as positions in the excepted serv-
2 ice, such qualified positions in the Office as the Di-
3 rector determines necessary to carry out the respon-
4 sibilities of the Office, appoint an individual to a
5 qualified position (after taking into consideration the
6 availability of preference eligibles for appointment to
7 the position), and, subject to the requirements of
8 paragraphs (4) and (5), fix the compensation of an
9 individual for service in a qualified position;

10 “(4) fix the rates of basic pay for any qualified
11 position established under paragraph (3) in relation
12 to the rates of pay provided for employees in com-
13 parable positions in the Office, in which the em-
14 ployee occupying the comparable position performs,
15 manages, or supervises functions that execute the
16 mission of the Office, and, subject to the same limi-
17 tations on maximum rates of pay and consistent
18 with section 5341 of title 5, United States Code,
19 adopt such provisions of that title to provide for pre-
20 vailing rate systems of basic pay and apply those
21 provisions to qualified positions for employees in or
22 under which the Office may employ individuals de-
23 scribed by section 5342(a)(2)(A) of such title;

24 “(5) employ an officer or employee of the
25 United States or member of the Armed Forces de-

1 tailed to the staff of the Office on a non-reimburs-
2 able basis—

3 “(A) as jointly agreed to by the heads of
4 the receiving and detailing elements, for a pe-
5 riod not to exceed 3 years;

6 “(B) which shall not be construed to limit
7 any other source of authority for reimbursable
8 or non-reimbursable details; and

9 “(C) which shall not be considered an aug-
10 mentation of the appropriations of the receiving
11 element of the Office;

12 “(6) provide—

13 “(A) employees in qualified positions com-
14 pensation (in addition to basic pay), including
15 benefits, incentives, and allowances, consistent
16 with, and not in excess of the level authorized
17 for, comparable positions authorized by title 5,
18 United States Code; and

19 “(B) employees in a qualified position
20 whose rate of basic pay is fixed under para-
21 graph (4) an allowance under section 5941 of
22 title 5, United States Code, on the same basis
23 and to the same extent as if the employee was
24 an employee covered by such section, including

1 eligibility conditions, allowance rates, and all
2 other terms and conditions in law or regulation;

3 “(7) establish a fellowship program to facilitate
4 a talent exchange program between the private sec-
5 tor and the Office to arrange, with the agreement of
6 a private sector organization and the consent of the
7 employee, for the temporary assignment of an em-
8 ployee to the private sector organization, or from the
9 private sector organization to the Office;” and

10 (2) in subsection (g)—

11 (A) by redesignating paragraphs (3)
12 through (6) as paragraphs (4) through (7), re-
13 spectively;

14 (B) by inserting after paragraph (2) the
15 following:

16 “(3) The term ‘excepted service’ has the mean-
17 ing given that term in section 2103 of title 5, United
18 States Code.”; and

19 (3) by adding at the end the following:

20 “(8) The term ‘preference eligible’ has the
21 meaning given that term in section 2108(3) of title
22 5, United States Code.

23 “(9) The term ‘qualified position’ means a posi-
24 tion, designated by the Director for the purpose of
25 this section, in which the individual occupying such

- 1 position performs, manages, or supervises functions
- 2 that execute the responsibilities of the Office.”.

