

117TH CONGRESS
1ST SESSION

S. 2666

To address threats relating to ransomware, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 5, 2021

Mr. RUBIO (for himself and Mrs. FEINSTEIN) introduced the following bill;
which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To address threats relating to ransomware, 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.**

4 This Act may be cited as the “Sanction and Stop
5 Ransomware Act of 2021”.

6 **SEC. 2. CYBERSECURITY STANDARDS FOR CRITICAL INFRA-**
7 **STRUCTURE.**

8 (a) IN GENERAL.—Title XXII of the Homeland Se-
9 curity Act of 2002 (6 U.S.C. 651 et seq.) is amended by
10 adding at the end the following:

1 **“Subtitle C—Cybersecurity Stand-**
2 **ards for Critical Infrastructure**

3 **“SEC. 2231. DEFINITION OF CRITICAL INFRASTRUCTURE**
4 **ENTITY.**

5 “In this subtitle, the term ‘critical infrastructure en-
6 tity’ means an owner or operator of critical infrastructure.

7 **“SEC. 2232 CYBERSECURITY STANDARDS.**

8 “(a) IN GENERAL.—The Secretary, in consultation
9 with the Director of the Cybersecurity and Infrastructure
10 Security Agency, shall develop and promulgate mandatory
11 cybersecurity standards for critical infrastructure entities.

12 “(b) HARMONIZATION AND INCORPORATION.—In de-
13 veloping the cybersecurity standards required under sub-
14 section (a), the Secretary shall—

15 “(1) to the greatest extent practicable, ensure
16 the cybersecurity standards are consistent with Fed-
17 eral regulations existing as of the date on enactment
18 of the Sanction and Stop Ransomware Act of 2021;
19 and

20 “(2) in coordination with the Director of the
21 National Institute of Standards and Technology, en-
22 sure that the cybersecurity standards incorporate, to
23 the greatest extent practicable, the standards devel-
24 oped with facilitation and support from the Director
25 of the National Institute of Standards and Tech-

1 nology under section 2(c)(15) of the National Insti-
2 tute of Standards and Technology Act (15 U.S.C.
3 272(c)(15)).

4 “(c) COMPLIANCE ASSESSMENT.—Not less frequently
5 than annually, the Secretary, in coordination with the
6 heads of Sector Risk Management Agencies, shall assess
7 the compliance of each critical infrastructure entity with
8 the cybersecurity standards developed under subsection
9 (a).”.

10 (b) TECHNICAL AND CONFORMING AMENDMENT.—
11 The table of contents in section 1(b) of the Homeland Se-
12 curity Act of 2002 (Public Law 107–296; 116 Stat. 2135)
13 is amended by adding at the end the following:

“Subtitle C—Cybersecurity Standards for Critical Infrastructure

“Sec. 2231. Definition of critical infrastructure entity.

“Sec. 2232. Cybersecurity standards.”.

14 **SEC. 3. REGULATION OF CRYPTOCURRENCY EXCHANGES.**

15 (a) SECRETARY OF THE TREASURY.—Not later than
16 180 days after the date of enactment of this Act, the Sec-
17 retary of the Treasury shall—

18 (1) develop and institute regulatory require-
19 ments for cryptocurrency exchanges operating within
20 the United States to reduce the anonymity of users
21 and accounts suspected of ransomware activity and
22 make records available to the Federal Government in
23 connection with ransomware incidents; and

1 (2) submit to Congress a report with any rec-
2 ommendations that may be necessary regarding
3 cryptocurrency exchanges used in conjunction with
4 ransomware.

5 (b) ATTORNEY GENERAL.—The Attorney General
6 shall determine what information should be preserved by
7 cryptocurrency exchanges to facilitate law enforcement in-
8 vestigations.

9 **SEC. 4. DESIGNATION OF STATE SPONSORS OF**
10 **RANSOMWARE AND REPORTING REQUIRE-**
11 **MENTS.**

12 (a) DESIGNATION OF STATE SPONSORS OF
13 RANSOMWARE.—

14 (1) IN GENERAL.—Not later than 180 days
15 after the date of the enactment of this Act, and an-
16 nually thereafter, the Secretary of State, in consulta-
17 tion with the Director of National Intelligence,
18 shall—

19 (A) designate as a state sponsor of
20 ransomware any country the government of
21 which the Secretary has determined has pro-
22 vided support for ransomware demand schemes
23 (including by providing safe haven for individ-
24 uals engaged in such schemes);

1 (B) submit to Congress a report listing the
2 countries designated under subparagraph (A);
3 and

4 (C) in making designations under subpara-
5 graph (A), take into consideration the report
6 submitted to Congress under section 5(c)(1).

7 (2) SANCTIONS AND PENALTIES.—The Presi-
8 dent shall impose with respect to each state sponsor
9 of ransomware designated under paragraph (1)(A)
10 the sanctions and penalties imposed with respect to
11 a state sponsor of terrorism.

12 (3) STATE SPONSOR OF TERRORISM DE-
13 FINED.—In this subsection, the term “state sponsor
14 of terrorism” means a country the government of
15 which the Secretary of State has determined has re-
16 peatedly provided support for acts of international
17 terrorism, for purposes of—

18 (A) section 1754(c)(1)(A)(i) of the Export
19 Control Reform Act of 2018 (50 U.S.C.
20 4813(c)(1)(A)(i));

21 (B) section 620A of the Foreign Assistance
22 Act of 1961 (22 U.S.C. 2371);

23 (C) section 40(d) of the Arms Export Con-
24 trol Act (22 U.S.C. 2780(d)); or

25 (D) any other provision of law.

1 (b) REPORTING REQUIREMENTS.—

2 (1) SANCTIONS RELATING TO RANSOMWARE RE-
3 PORT.—Not later than 180 days after the date of
4 the enactment of this Act, the Secretary of the
5 Treasury shall submit a report to Congress that de-
6 scribes, for each of the 5 fiscal years immediately
7 preceding the date of such report, the number and
8 geographic locations of individuals, groups, and enti-
9 ties subject to sanctions imposed by the Office of
10 Foreign Assets Control who were subsequently deter-
11 mined to have been involved in a ransomware de-
12 mand scheme.

13 (2) COUNTRY OF ORIGIN REPORT.—The Sec-
14 retary of State, in consultation with the Director of
15 National Intelligence and the Director of the Federal
16 Bureau of Investigation, shall—

17 (A) submit a report, with a classified
18 annex, to the Committee on Foreign Relations
19 of the Senate, the Select Committee on Intel-
20 ligence of the Senate, the Committee on For-
21 eign Affairs of the House of Representatives,
22 and the Permanent Select Committee on Intel-
23 ligence of the House of Representatives that
24 identifies the country of origin of foreign-based
25 ransomware attacks; and

1 (B) make the report described in subpara-
2 graph (A) (excluding the classified annex) avail-
3 able to the public.

4 (3) INVESTIGATIVE AUTHORITIES REPORT.—

5 Not later than 180 days after the date of the enact-
6 ment of this Act, the Comptroller General of the
7 United States shall issue a report that outlines the
8 authorities available to the Federal Bureau of Inves-
9 tigation, the United States Secret Service, the Cy-
10 bersecurity and Infrastructure Security Agency, the
11 Homeland Security Investigations, and the Office of
12 Foreign Assets Control to respond to foreign-based
13 ransomware attacks.

14 **SEC. 5. DEEMING RANSOMWARE THREATS TO CRITICAL IN-**
15 **FRASTRUCTURE AS A NATIONAL INTEL-**
16 **LIGENCE PRIORITY.**

17 (a) CRITICAL INFRASTRUCTURE DEFINED.—In this
18 section, the term “critical infrastructure” has the meaning
19 given such term in subsection (e) of the Critical Infra-
20 structures Protection Act of 2001 (42 U.S.C. 5195c(e)).

21 (b) RANSOMWARE THREATS TO CRITICAL INFRA-
22 STRUCTURE AS NATIONAL INTELLIGENCE PRIORITY.—
23 The Director of National Intelligence, pursuant to the pro-
24 visions of the National Security Act of 1947 (50 U.S.C.
25 3001 et seq.), the Intelligence Reform and Terrorism Pre-

1 vention Act of 2004 (Public Law 108–458), section
2 1.3(b)(17) of Executive Order 12333 (50 U.S.C. 3001
3 note; relating to United States intelligence activities), as
4 in effect on the day before the date of the enactment of
5 this Act, and National Security Presidential Directive–26
6 (February 24, 2003; relating to intelligence priorities), as
7 in effect on the day before the date of the enactment of
8 this Act, shall deem ransomware threats to critical infra-
9 structure a national intelligence priority component to the
10 National Intelligence Priorities Framework.

11 (c) REPORT.—

12 (1) IN GENERAL.—Not later than 180 days
13 after the date of the enactment of this Act, the Di-
14 rector of National Intelligence shall, in consultation
15 with the Director of the Federal Bureau of Inves-
16 tigation, submit to the Select Committee on Intel-
17 ligence of the Senate and the Permanent Select
18 Committee on Intelligence of the House of Rep-
19 resentatives a report on the implications of the
20 ransomware threat to United States national secu-
21 rity.

22 (2) CONTENTS.—The report submitted under
23 paragraph (1) shall address the following:

24 (A) Identification of individuals, groups,
25 and entities who pose the most significant

1 threat, including attribution to individual
2 ransomware attacks whenever possible.

3 (B) Locations from where individuals,
4 groups, and entities conduct ransomware at-
5 tacks.

6 (C) The infrastructure, tactics, and tech-
7 niques ransomware actors commonly use.

8 (D) Any relationships between the individ-
9 uals, groups, and entities that conduct
10 ransomware attacks and their governments or
11 countries of origin that could impede the ability
12 to counter ransomware threats.

13 (E) Intelligence gaps that have, or cur-
14 rently are, impeding the ability to counter
15 ransomware threats.

16 (3) FORM.—The report submitted under para-
17 graph (1) shall be submitted in unclassified form,
18 but may include a classified annex.

19 **SEC. 6. RANSOMWARE OPERATION REPORTING CAPABILI-**
20 **TIES.**

21 (a) IN GENERAL.—Title XXII of the Homeland Se-
22 curity Act of 2002 (6 U.S.C. 651 et seq.), as amended
23 by section 2(a), is amended by adding at the end the fol-
24 lowing:

1 **“Subtitle D—Ransomware**
2 **Operation Reporting Capabilities**

3 **“SEC. 2241. DEFINITIONS.**

4 “In this subtitle:

5 “(1) DEFINITIONS FROM SECTION 2201.—The
6 definitions in section 2201 shall apply to this sub-
7 title, except as otherwise provided.

8 “(2) AGENCY.—The term ‘Agency’ means the
9 Cybersecurity and Infrastructure Security Agency.

10 “(3) APPROPRIATE CONGRESSIONAL COMMIT-
11 TEES.—The term ‘appropriate congressional com-
12 mittees’ means—

13 “(A) the Committee on Homeland Security
14 and Governmental Affairs of the Senate;

15 “(B) the Select Committee on Intelligence
16 of the Senate;

17 “(C) the Committee on the Judiciary of
18 the Senate;

19 “(D) the Committee on Homeland Security
20 of the House of Representatives;

21 “(E) the Permanent Select Committee on
22 Intelligence of the House of Representatives;
23 and

24 “(F) the Committee on the Judiciary of
25 the House of Representatives.

1 “(4) COVERED ENTITY.—The term ‘covered en-
2 tity’ means—

3 “(A) a Federal contractor;

4 “(B) an owner or operator of critical infra-
5 structure;

6 “(C) a non-government entity that pro-
7 vides cybersecurity incident response services;
8 and

9 “(D) any other entity determined appro-
10 priate by the Secretary, in coordination with the
11 head of any other appropriate department or
12 agency.

13 “(5) CRITICAL FUNCTION.—The term ‘critical
14 function’ means any action or operation that is nec-
15 essary to maintain critical infrastructure.

16 “(6) DIRECTOR.—The term ‘Director’ means
17 the Director of the Cybersecurity and Infrastructure
18 Security Agency.

19 “(7) FEDERAL AGENCY.—The term ‘Federal
20 agency’ has the meaning given the term ‘agency’ in
21 section 3502 of title 44, United States Code.

22 “(8) FEDERAL CONTRACTOR.—The term ‘Fed-
23 eral contractor’—

1 “(A) means a contractor or subcontractor
2 (at any tier) of the United States Government;
3 and

4 “(B) does not include a contractor or sub-
5 contractor that is a party only to—

6 “(i) a service contract to provide
7 housekeeping or custodial services; or

8 “(ii) a contract to provide products or
9 services unrelated to information tech-
10 nology that is below the micro-purchase
11 threshold (as defined in section 2.101 of
12 title 48, Code of Federal Regulations, or
13 any successor thereto).

14 “(9) INFORMATION TECHNOLOGY.—The term
15 ‘information technology’ has the meaning given the
16 term in section 11101 of title 40, United States
17 Code.

18 “(10) RANSOMWARE.—The term ‘ransomware’
19 means any type of malicious software that—

20 “(A) prevents the legitimate owner or oper-
21 ator of an information system or network from
22 accessing electronic data, files, systems, or net-
23 works; and

24 “(B) demands the payment of a ransom
25 for the return of access to the electronic data,

1 files, systems, or networks described in sub-
2 paragraph (A).

3 “(11) RANSOMWARE NOTIFICATION.—The term
4 ‘ransomware notification’ means a notification of a
5 ransomware operation.

6 “(12) RANSOMWARE OPERATION.—The term
7 ‘ransomware operation’ means a specific instance in
8 which ransomware affects the information systems
9 or networks owned or operated by—

10 “(A) a covered entity; or

11 “(B) a Federal agency.

12 “(13) SYSTEM.—The term ‘System’ means the
13 ransomware operation reporting capabilities estab-
14 lished under section 2242(b).

15 **“SEC. 2242. ESTABLISHMENT OF RANSOMWARE OPERATION**
16 **REPORTING SYSTEM.**

17 “(a) DESIGNATION.—The Agency shall be the des-
18 ignated agency within the Federal Government to receive
19 ransomware operation notifications from other Federal
20 agencies and covered entities in accordance with this sub-
21 title.

22 “(b) ESTABLISHMENT.—Not later than 180 days
23 after the date of enactment of this subtitle, the Director
24 shall establish ransomware operation reporting capabilities
25 to facilitate the submission of timely, secure, and confiden-

1 tial ransomware notifications by Federal agencies and cov-
2 ered entities to the Agency.

3 “(c) SECURITY ASSESSMENT.—The Director shall—

4 “(1) assess the security of the System not less
5 frequently than once every 2 years; and

6 “(2) as soon as is practicable after conducting
7 an assessment under paragraph (1), make any nec-
8 essary corrective measures to the System.

9 “(d) REQUIREMENTS.—The System shall have the
10 ability—

11 “(1) to accept classified submissions and notifi-
12 cations; and

13 “(2) to accept a ransomware notification from
14 any entity, regardless of whether the entity is a cov-
15 ered entity.

16 “(e) LIMITATIONS ON USE OF INFORMATION.—Any
17 ransomware notification submitted to the System—

18 “(1) shall be exempt from disclosure under—

19 “(A) section 552 of title 5, United States
20 Code (commonly referred to as the “Freedom of
21 Information Act”), in accordance with sub-
22 section (b)(3)(B) of such section 552; and

23 “(B) any State, Tribal, or local law requir-
24 ing the disclosure of information or records;
25 and

1 “(2) may not be—

2 “(A) admitted as evidence in any civil or
3 criminal action brought against the victim of
4 the ransomware operation; or

5 “(B) subject to a subpoena, unless the sub-
6 poena is issued by Congress for congressional
7 oversight purposes.

8 “(f) PRIVACY AND PROTECTION.—

9 “(1) IN GENERAL.—Not later than the date on
10 which the Director establishes the System, Director
11 shall adopt privacy and protection procedures for
12 any information submitted to the System that, at
13 the time of the submission, is known to contain—

14 “(A) the personal information of a specific
15 individual; or

16 “(B) information that identifies a specific
17 individual that is not directly related to a
18 ransomware operation.

19 “(2) MODEL FOR PROTECTIONS.—The Director
20 shall base the privacy and protection procedures
21 adopted under paragraph (1) on the privacy and
22 protection procedures developed for information re-
23 ceived and shared pursuant to the Cybersecurity In-
24 formation Sharing Act of 2015 (6 U.S.C. 1501 et
25 seq.).

1 “(g) ANNUAL REPORTS.—

2 “(1) DIRECTOR REPORTING REQUIREMENT.—

3 Not later than 1 year after the date on which the
4 System is established and once each year thereafter,
5 the Director shall submit to the appropriate congres-
6 sional committees a report on the System, which
7 shall include, with respect to the 1-year period pre-
8 ceding the report—

9 “(A) the number of notifications received
10 through the System; and

11 “(B) the actions taken in connection with
12 the notifications described in subparagraph (A).

13 “(2) SECRETARY REPORTING REQUIREMENT.—

14 Not later than 1 year after the date on which the
15 System is established, and once each year thereafter,
16 the Secretary shall submit to the appropriate con-
17 gressional committees a report on the types of
18 ransomware operation information and incidents in
19 which ransom is requested that are required to be
20 submitted as a ransomware notification, noting any
21 changes from the previous submission.

22 “(3) FORM.—Any report required under this
23 subsection may be submitted in a classified form, if
24 necessary.

1 **“SEC. 2243. REQUIRED NOTIFICATIONS.**

2 “(a) IN GENERAL.—

3 “(1) RANSOMWARE NOTIFICATION.—Not later
4 than 24 hours after the discovery of a ransomware
5 operation that compromises, is reasonably likely to
6 compromise, or otherwise materially affects the per-
7 formance of a critical function by a Federal agency
8 or covered entity, the Federal agency or covered en-
9 tity that discovered the ransomware operation shall
10 submit a ransomware notification to the System.

11 “(2) INCLUSION.—A Federal agency or covered
12 entity shall submit a ransomware notification under
13 paragraph (1) of a ransomware operation discovered
14 by the Federal agency or covered entity even if the
15 ransomware operation does not occur on a system of
16 the Federal agency or covered entity.

17 “(b) REQUIRED UPDATES.—A Federal agency or
18 covered entity that submits a ransomware notification
19 under subsection (a) shall, upon discovery of new informa-
20 tion and not less frequently than once every 5 days until
21 the date on which the ransomware operation is mitigated
22 and any follow-up investigation is completed, submit up-
23 dated ransomware threat information to the System.

24 “(c) PAYMENT DISCLOSURE.—Not later than 24
25 hours after a Federal agency or covered entity issues a
26 ransom payment relating to a ransomware operation, the

1 Federal agency or covered entity shall submit to the Sys-
2 tem details of the ransom payment, including—

3 “(1) the method of payment;

4 “(2) the amount of the payment; and

5 “(3) the recipient of the payment.

6 “(d) REQUIRED RULEMAKING.—Notwithstanding
7 any provision of this title that may limit or restrict the
8 promulgation of rules, not later than 180 days after the
9 date of enactment of this subtitle, the Secretary, acting
10 through the Director, in coordination with the Director of
11 National Intelligence and the Attorney General, without
12 regard to the notice and comment rule making require-
13 ments under section 553 of title 5, United States Code,
14 and accepting comments after the effective date, shall pro-
15 mulgate interim final rules that define—

16 “(1) the conditions under which a ransomware
17 notification is required to be submitted under sub-
18 section (a)(1);

19 “(2) the ransomware operation information that
20 shall be included in a ransomware notification re-
21 quired under this section; and

22 “(3) the information that shall be included in a
23 ransom payment disclosure required under sub-
24 section (c).

1 “(e) REQUIRED COORDINATION WITH SECTOR RISK
2 MANAGEMENT AGENCIES.—The Secretary, in coordina-
3 tion with the head of each Sector Risk Management Agen-
4 cy, shall—

5 “(1) establish a set of reporting criteria for
6 Sector Risk Management Agencies to submit
7 ransomware notifications to the System; and

8 “(2) take steps to harmonize the criteria de-
9 scribed in paragraph (1) with the regulatory report-
10 ing requirements in effect on the date of enactment
11 of this subtitle.

12 “(f) PROTECTION FROM LIABILITY.—Section 106 of
13 the Cybersecurity Act of 2015 (6 U.S.C. 1505) shall apply
14 to a Federal agency or covered entity required to submit
15 a ransomware notification to the System.

16 “(g) ENFORCEMENT.—

17 “(1) COVERED ENTITIES.—If a covered entity
18 violates the requirements of this subtitle, the covered
19 entity shall be subject to penalties determined by the
20 Administrator of the General Services Administra-
21 tion, which may include removal from the Federal
22 Contracting Schedules.

23 “(2) FEDERAL AGENCIES.—If a Federal agency
24 violates the requirements of this subtitle, the viola-
25 tion shall be referred to the inspector general for the

1 agency, and shall be treated as a matter of urgent
2 concern.”.

3 (b) TABLE OF CONTENTS.—The table of contents in
4 section 1(b) of the Homeland Security Act of 2002 (Public
5 Law 107–296; 116 Stat. 2135), as amended by section
6 2(b), is further amended by adding at the end the fol-
7 lowing:

“Subtitle D—Ransomware Operation Reporting Capabilities

“Sec. 2241. Definitions.

“Sec. 2242. Establishment of ransomware operation reporting system.

“Sec. 2243. Required notifications.”.

8 (c) TECHNICAL AND CONFORMING AMENDMENTS.—
9 Section 2202(c) of the Homeland Security Act of 2002
10 (6 U.S.C. 652(c)) is amended—

11 (1) by redesignating the second and third para-
12 graphs (12) as paragraphs (14) and (15), respec-
13 tively; and

14 (2) by inserting before paragraph (14), as so
15 redesignated, the following:

16 “(13) carry out the responsibilities described in
17 subtitle D relating to the ransomware operation re-
18 porting system;”.

19 **SEC. 7. DUTIES OF THE CYBERSECURITY AND INFRASTRUC-**
20 **TURE SECURITY AGENCY.**

21 (a) IN GENERAL.—Subtitle A of title XXII of the
22 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)
23 is amended—

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

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

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

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

11 (5) 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 (6) by adding after section 2220, as so redesign-
15 nated, the following:

16 **“SEC. 2220A. INFORMATION SYSTEM AND NETWORK SECUR-**
17 **RITY FUND.**

18 “(a) DEFINITIONS.—In this section:

19 “(1) COVERED ENTITY.—The term ‘covered en-
20 tity’ has the meaning given the term in section
21 2241.

22 “(2) ELIGIBLE ENTITY.—The term ‘eligible en-
23 tity’—

24 “(A) means a covered entity; and

1 “(B) does not include an owner or operator
2 of critical infrastructure that is not in compli-
3 ance with the cybersecurity standards developed
4 under section 2232(a).

5 “(3) FUND.—The term ‘Fund’ means the In-
6 formation System and Network Security Fund es-
7 tablished under subsection (b)(1).

8 “(b) INFORMATION SYSTEM AND NETWORK SECU-
9 RITY FUND.—

10 “(1) ESTABLISHMENT.—There is established in
11 the Treasury of the United States a trust fund to
12 be known as the ‘Information System and Network
13 Security Fund’.

14 “(2) CONTENTS OF FUND.—

15 “(A) IN GENERAL.—The Fund shall con-
16 sist of such amounts as may be appropriated
17 for deposit in the Fund.

18 “(B) AVAILABILITY.—

19 “(i) IN GENERAL.—Amounts depos-
20 ited in the Fund shall remain available
21 through the end of the tenth fiscal year be-
22 ginning after the date on which funds are
23 first appropriated to the Fund.

24 “(ii) REMAINDER TO TREASURY.—
25 Any unobligated balances in the Fund

1 after the date described in clause (i) are
2 rescinded and shall be transferred to the
3 general fund of the Treasury.

4 “(3) USE OF FUND.—

5 “(A) IN GENERAL.—Amounts deposited in
6 the Fund shall be available to the Director to
7 distribute to eligible entities pursuant to this
8 subsection, in such amounts as the Director de-
9 termines appropriate, subject to subparagraph
10 (B).

11 “(B) DISTRIBUTION.—The amounts dis-
12 tributed to eligible entities under this para-
13 graph shall be made for a specific network secu-
14 rity purpose, including to enable network recov-
15 ery from an event affecting the network cyber-
16 security of the eligible entity.

17 “(4) ADMINISTRATION OF FUND.—The Direc-
18 tor, in consultation with the Secretary and in coordi-
19 nation with the head of each Sector Risk Manage-
20 ment Agency, shall—

21 “(A) establish criteria for distribution of
22 amounts under paragraph (3); and

23 “(B) administer the Fund to support net-
24 work security for eligible entities.

1 “(5) REPORT REQUIRED.—For each fiscal year
2 for which amounts in the Fund are available under
3 this subsection, the Director shall submit to Con-
4 gress a report that—

5 “(A) describes how, and to which eligible
6 entities, amounts from the Fund have been dis-
7 tributed;

8 “(B) details the criteria established under
9 paragraph (4)(A); and

10 “(C) includes any additional information
11 that the Director determines appropriate, in-
12 cluding projected requested appropriations for
13 the next fiscal year.

14 “(c) AUTHORIZATION OF APPROPRIATIONS.—There
15 are authorized to be appropriated for deposit in the Fund
16 \$1,500,000,000, which shall remain available until the last
17 day of the tenth fiscal year beginning after the fiscal year
18 during which funds are first appropriated for deposit in
19 the Fund.

20 **“SEC. 2220B. PUBLIC AWARENESS OF CYBERSECURITY OF-**
21 **FERINGS.**

22 “(a) IN GENERAL.—Not later than 180 days after
23 the date of enactment of the Sanction and Stop
24 Ransomware Act of 2021, the Director shall establish a

1 public awareness campaign relating to the cybersecurity
2 services of the Federal Government.

3 “(b) AUTHORIZATION OF APPROPRIATIONS.—There
4 are authorized to be appropriated to the Director
5 \$10,000,000 for each of fiscal years 2022 through 2031
6 to carry out subsection (a).

7 **“SEC. 2220C. DARK WEB ANALYSIS.**

8 “(a) DEFINITION OF DARK WEB.—In this section,
9 the term ‘dark web’ means a part of the internet that—

10 “(1) cannot be accessed through standard web
11 browsers; and

12 “(2) requires specific software, configurations,
13 or authorizations for access.

14 “(b) AUTHORITY TO ANALYZE.—The Director may
15 monitor the internet, including the dark web, for evidence
16 of a compromise to critical infrastructure.

17 “(c) MONITORING CAPABILITIES.—The Director
18 shall develop, institute, and oversee capabilities to carry
19 out the authority of the Director under subsection (b).

20 “(d) NOTIFICATION.—If the Director finds credible
21 evidence of a compromise to critical infrastructure under
22 subsection (c), as soon as is practicable after the finding,
23 the Director shall notify the owner or operator of the com-
24 promised critical infrastructure in a manner that protects

1 the sources and methods that led to the finding of the
2 compromise.”.

3 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

4 Section 2202(c) of the Homeland Security Act of 2002
5 (6 U.S.C. 652(c)) is amended—

6 (1) in the first paragraph (12), by striking
7 “section 2215” and inserting “section 2217”; and

8 (2) by redesignating the second and third para-
9 graphs (12) as paragraphs (13) and (14), respec-
10 tively.

11 (c) TABLE OF CONTENTS.—The table of contents in
12 section 1(b) of the Homeland Security Act of 2002 (Public
13 Law 107–296; 116 Stat. 2135) is amended by striking
14 the item relating to section 2214 and all that follows
15 through the item relating to section 2217 and inserting
16 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. Information System and Network Security Fund.

“Sec. 2220B. Public awareness of cybersecurity offerings.

“Sec. 2220C. Dark web analysis.”.

17 (d) ADDITIONAL TECHNICAL AMENDMENT.—

18 (1) AMENDMENT.—Section 904(b)(1) of the
19 DOTGOV Act of 2020 (title IX of division U of
20 Public Law 116–260) is amended, in the matter pre-

1 ceding subparagraph (A), by striking “Homeland
2 Security Act” and inserting “Homeland Security Act
3 of 2002”.

4 (2) EFFECTIVE DATE.—The amendment made
5 by paragraph (1) shall take effect as if enacted as
6 part of the DOTGOV Act of 2020 (title IX of divi-
7 sion U of Public Law 116–260).

○