117TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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

A BILL

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

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Sanction and Stop Ransomware Act of 2021''.

SEC. 2. CYBERSECURITY STANDARDS FOR CRITICAL INFRASTRUCTURE.

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

"Subtitle C—Cybersecurity Standards for Critical Infrastructure

"SEC. 2231. DEFINITION OF CRITICAL INFRASTRUCTURE ENTITY.

''In this subtitle, the term 'critical infrastructure entity' means an owner or operator of critical infrastructure.

"SEC. 2232 CYBERSECURITY STANDARDS.

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

''(b) HARMONIZATION AND INCORPORATION.—In developing the cybersecurity standards required under subsection (a), the Secretary shall—

''(1) to the greatest extent practicable, ensure the cybersecurity standards are consistent with Federal regulations existing as of the date on enactment of the Sanction and Stop Ransomware Act of 2021; and

''(2) in coordination with the Director of the National Institute of Standards and Technology, ensure that the cybersecurity standards incorporate, to the greatest extent practicable, the standards developed with facilitation and support from the Director of the National Institute of Standards and Tech-

nology under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15)).

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

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) 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.''.

SEC. 3. REGULATION OF CRYPTOCURRENCY EXCHANGES.

(a) SECRETARY OF THE TREASURY.—Not later than 180 days after the date of enactment of this Act, the Secretary of the Treasury shall—

(1) develop and institute regulatory requirements for cryptocurrency exchanges operating within the United States to reduce the anonymity of users and accounts suspected of ransomware activity and make records available to the Federal Government in connection with ransomware incidents; and

(2) submit to Congress a report with any recommendations that may be necessary regarding cryptocurrency exchanges used in conjunction with ransomware.

(b) ATTORNEY GENERAL.—The Attorney General shall determine what information should be preserved by cryptocurrency exchanges to facilitate law enforcement investigations.

SEC. 4. DESIGNATION OF STATE SPONSORS OF RANSOMWARE AND REPORTING REQUIREMENTS.

(a) DESIGNATION OF STATE SPONSORS OF RANSOMWARE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Secretary of State, in consultation with the Director of National Intelligence, shall—

(A) designate as a state sponsor of ransomware any country the government of which the Secretary has determined has provided support for ransomware demand schemes (including by providing safe haven for individuals engaged in such schemes);

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

(C) in making designations under subparagraph (A), take into consideration the report submitted to Congress under section 5(c)(1).

(2) SANCTIONS AND PENALTIES.—The President shall impose with respect to each state sponsor of ransomware designated under paragraph (1)(A) the sanctions and penalties imposed with respect to a state sponsor of terrorism.

(3) STATE SPONSOR OF TERRORISM DEFINED.—In this subsection, the term ''state sponsor of terrorism'' means a country the government of which the Secretary of State has determined has repeatedly provided support for acts of international terrorism, for purposes of—

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

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

(C) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d)); or

(D) any other provision of law.

(b) REPORTING REQUIREMENTS.—

(1) SANCTIONS RELATING TO RANSOMWARE REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Treasury shall submit a report to Congress that describes, for each of the 5 fiscal years immediately preceding the date of such report, the number and geographic locations of individuals, groups, and entities subject to sanctions imposed by the Office of Foreign Assets Control who were subsequently determined to have been involved in a ransomware demand scheme.

(2) COUNTRY OF ORIGIN REPORT.—The Secretary of State, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, shall—

(A) submit a report, with a classified annex, to the Committee on Foreign Relations of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Foreign Affairs of the House of Representatives, and the Permanent Select Committee on Intelligence of the House of Representatives that identifies the country of origin of foreign-based ransomware attacks; and

(B) make the report described in subparagraph (A) (excluding the classified annex) available to the public.

(3) INVESTIGATIVE AUTHORITIES REPORT.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General of the United States shall issue a report that outlines the authorities available to the Federal Bureau of Investigation, the United States Secret Service, the Cybersecurity and Infrastructure Security Agency, the Homeland Security Investigations, and the Office of Foreign Assets Control to respond to foreign-based ransomware attacks.

SEC. 5. DEEMING RANSOMWARE THREATS TO CRITICAL INFRASTRUCTURE AS A NATIONAL INTELLIGENCE PRIORITY.

(a) CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term ''critical infrastructure'' has the meaning given such term in subsection (e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(b) RANSOMWARE THREATS TO CRITICAL INFRASTRUCTURE AS NATIONAL INTELLIGENCE PRIORITY.—The Director of National Intelligence, pursuant to the provisions of the National Security Act of 1947 (50 U.S.C. 3001 et seq.), the Intelligence Reform and Terrorism Pre-

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

(c) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the implications of the ransomware threat to United States national security.

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

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

threat, including attribution to individual ransomware attacks whenever possible.

(B) Locations from where individuals, groups, and entities conduct ransomware attacks.

(C) The infrastructure, tactics, and techniques ransomware actors commonly use.

(D) Any relationships between the individuals, groups, and entities that conduct ransomware attacks and their governments or countries of origin that could impede the ability to counter ransomware threats.

(E) Intelligence gaps that have, or currently are, impeding the ability to counter ransomware threats.

(3) FORM.—The report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

SEC. 6. RANSOMWARE OPERATION REPORTING CAPABILITIES.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.), as amended by section 2(a), is amended by adding at the end the following:

"Subtitle D—Ransomware Operation Reporting Capabilities

"SEC. 2241. DEFINITIONS.

''In this subtitle:

''(1) DEFINITIONS FROM SECTION 2201.—The definitions in section 2201 shall apply to this subtitle, except as otherwise provided.

''(2) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

''(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Select Committee on Intelligence of the Senate;

''(C) the Committee on the Judiciary of the Senate;

''(D) the Committee on Homeland Security of the House of Representatives;

''(E) the Permanent Select Committee on Intelligence of the House of Representatives; and

''(F) the Committee on the Judiciary of the House of Representatives.

''(4) COVERED ENTITY.—The term 'covered entity' means—

''(A) a Federal contractor;

''(B) an owner or operator of critical infrastructure;

''(C) a non-government entity that provides cybersecurity incident response services; and

''(D) any other entity determined appropriate by the Secretary, in coordination with the head of any other appropriate department or agency.

''(5) CRITICAL FUNCTION.—The term 'critical function' means any action or operation that is necessary to maintain critical infrastructure.

''(6) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.

''(7) FEDERAL AGENCY.—The term 'Federal agency' has the meaning given the term 'agency' in section 3502 of title 44, United States Code.

''(8) FEDERAL CONTRACTOR.—The term 'Federal contractor'—

"(A) means a contractor or subcontractor (at any tier) of the United States Government; and

"(B) does not include a contractor or subcontractor that is a party only to—

"(i) a service contract to provide housekeeping or custodial services; or

"(ii) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold (as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor thereto).

"(9) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40, United States Code.

"(10) RANSOMWARE.—The term 'ransomware' means any type of malicious software that—

"(A) prevents the legitimate owner or operator of an information system or network from accessing electronic data, files, systems, or networks; and

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

files, systems, or networks described in subparagraph (A).

''(11) RANSOMWARE NOTIFICATION.—The term 'ransomware notification' means a notification of a ransomware operation.

''(12) RANSOMWARE OPERATION.—The term 'ransomware operation' means a specific instance in which ransomware affects the information systems or networks owned or operated by—

''(A) a covered entity; or

''(B) a Federal agency.

''(13) SYSTEM.—The term 'System' means the ransomware operation reporting capabilities established under section 2242(b).

"SEC. 2242. ESTABLISHMENT OF RANSOMWARE OPERATION REPORTING SYSTEM.

''(a) DESIGNATION.—The Agency shall be the designated agency within the Federal Government to receive ransomware operation notifications from other Federal agencies and covered entities in accordance with this subtitle.

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

tial ransomware notifications by Federal agencies and covered entities to the Agency.

''(c) SECURITY ASSESSMENT.—The Director shall—

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

''(2) as soon as is practicable after conducting an assessment under paragraph (1), make any necessary corrective measures to the System.

''(d) REQUIREMENTS.—The System shall have the ability—

''(1) to accept classified submissions and notifications; and

''(2) to accept a ransomware notification from any entity, regardless of whether the entity is a covered entity.

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

''(1) shall be exempt from disclosure under—

''(A) section 552 of title 5, United States Code (commonly referred to as the ''Freedom of Information Act''), in accordance with subsection (b)(3)(B) of such section 552; and

''(B) any State, Tribal, or local law requiring the disclosure of information or records; and

''(2) may not be—

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

''(B) subject to a subpoena, unless the subpoena is issued by Congress for congressional oversight purposes.

''(f) PRIVACY AND PROTECTION.—

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

''(A) the personal information of a specific individual; or

''(B) information that identifies a specific individual that is not directly related to a ransomware operation.

''(2) MODEL FOR PROTECTIONS.—The Director shall base the privacy and protection procedures adopted under paragraph (1) on the privacy and protection procedures developed for information received and shared pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.).

"(g) ANNUAL REPORTS.—

"(1) DIRECTOR REPORTING REQUIREMENT.—Not later than 1 year after the date on which the System is established and once each year thereafter, the Director shall submit to the appropriate congressional committees a report on the System, which shall include, with respect to the 1-year period preceding the report—

"(A) the number of notifications received through the System; and

"(B) the actions taken in connection with the notifications described in subparagraph (A).

"(2) SECRETARY REPORTING REQUIREMENT.—Not later than 1 year after the date on which the System is established, and once each year thereafter, the Secretary shall submit to the appropriate congressional committees a report on the types of ransomware operation information and incidents in which ransom is requested that are required to be submitted as a ransomware notification, noting any changes from the previous submission.

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

"SEC. 2243. REQUIRED NOTIFICATIONS.

"(a) IN GENERAL.—

"(1) RANSOMWARE NOTIFICATION.—Not later than 24 hours after the discovery of a ransomware operation that compromises, is reasonably likely to compromise, or otherwise materially affects the performance of a critical function by a Federal agency or covered entity, the Federal agency or covered entity that discovered the ransomware operation shall submit a ransomware notification to the System.

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

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

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

Federal agency or covered entity shall submit to the System details of the ransom payment, including—

''(1) the method of payment;

''(2) the amount of the payment; and

''(3) the recipient of the payment.

''(d) REQUIRED RULEMAKING.—Notwithstanding any provision of this title that may limit or restrict the promulgation of rules, not later than 180 days after the date of enactment of this subtitle, the Secretary, acting through the Director, in coordination with the Director of National Intelligence and the Attorney General, without regard to the notice and comment rule making requirements under section 553 of title 5, United States Code, and accepting comments after the effective date, shall promulgate interim final rules that define—

''(1) the conditions under which a ransomware notification is required to be submitted under subsection (a)(1);

''(2) the ransomware operation information that shall be included in a ransomware notification required under this section; and

''(3) the information that shall be included in a ransom payment disclosure required under subsection (c).

''(e) REQUIRED COORDINATION WITH SECTOR RISK MANAGEMENT AGENCIES.—The Secretary, in coordination with the head of each Sector Risk Management Agency, shall—

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

''(2) take steps to harmonize the criteria described in paragraph (1) with the regulatory reporting requirements in effect on the date of enactment of this subtitle.

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

''(g) ENFORCEMENT.—

''(1) COVERED ENTITIES.—If a covered entity violates the requirements of this subtitle, the covered entity shall be subject to penalties determined by the Administrator of the General Services Administration, which may include removal from the Federal Contracting Schedules.

''(2) FEDERAL AGENCIES.—If a Federal agency violates the requirements of this subtitle, the violation shall be referred to the inspector general for the

agency, and shall be treated as a matter of urgent concern.''.

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

''Subtitle D—Ransomware Operation Reporting Capabilities

''Sec. 2241. Definitions.
''Sec. 2242. Establishment of ransomware operation reporting system.
''Sec. 2243. Required notifications.''.

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

(1) by redesignating the second and third paragraphs (12) as paragraphs (14) and (15), respectively; and

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

''(13) carry out the responsibilities described in subtitle D relating to the ransomware operation reporting system;''.

SEC. 7. DUTIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

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

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

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

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

(4) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217;

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

(6) by adding after section 2220, as so redesignated, the following:

"SEC. 2220A. INFORMATION SYSTEM AND NETWORK SECURITY FUND.

''(a) DEFINITIONS.—In this section:

''(1) COVERED ENTITY.—The term 'covered entity' has the meaning given the term in section 2241.

''(2) ELIGIBLE ENTITY.—The term 'eligible entity'—

''(A) means a covered entity; and

"(B) does not include an owner or operator of critical infrastructure that is not in compliance with the cybersecurity standards developed under section 2232(a).

"(3) FUND.—The term 'Fund' means the Information System and Network Security Fund established under subsection (b)(1).

"(b) INFORMATION SYSTEM AND NETWORK SECURITY FUND.—

"(1) ESTABLISHMENT.—There is established in the Treasury of the United States a trust fund to be known as the 'Information System and Network Security Fund'.

"(2) CONTENTS OF FUND.—

"(A) IN GENERAL.—The Fund shall consist of such amounts as may be appropriated for deposit in the Fund.

"(B) AVAILABILITY.—

"(i) IN GENERAL.—Amounts deposited in the Fund shall remain available through the end of the tenth fiscal year beginning after the date on which funds are first appropriated to the Fund.

"(ii) REMAINDER TO TREASURY.—Any unobligated balances in the Fund

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

''(3) USE OF FUND.—

''(A) IN GENERAL.—Amounts deposited in the Fund shall be available to the Director to distribute to eligible entities pursuant to this subsection, in such amounts as the Director determines appropriate, subject to subparagraph (B).

''(B) DISTRIBUTION.—The amounts distributed to eligible entities under this paragraph shall be made for a specific network security purpose, including to enable network recovery from an event affecting the network cybersecurity of the eligible entity.

''(4) ADMINISTRATION OF FUND.—The Director, in consultation with the Secretary and in coordination with the head of each Sector Risk Management Agency, shall—

''(A) establish criteria for distribution of amounts under paragraph (3); and

''(B) administer the Fund to support network security for eligible entities.

''(5) REPORT REQUIRED.—For each fiscal year for which amounts in the Fund are available under this subsection, the Director shall submit to Congress a report that—

''(A) describes how, and to which eligible entities, amounts from the Fund have been distributed;

''(B) details the criteria established under paragraph (4)(A); and

''(C) includes any additional information that the Director determines appropriate, including projected requested appropriations for the next fiscal year.

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

''SEC. 2220B. PUBLIC AWARENESS OF CYBERSECURITY OFFERINGS.

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

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

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

''SEC. 2220C. DARK WEB ANALYSIS.

''(a) DEFINITION OF DARK WEB.—In this section, the term 'dark web' means a part of the internet that—

''(1) cannot be accessed through standard web browsers; and

''(2) requires specific software, configurations, or authorizations for access.

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

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

''(d) NOTIFICATION.—If the Director finds credible evidence of a compromise to critical infrastructure under subsection (c), as soon as is practicable after the finding, the Director shall notify the owner or operator of the compromised critical infrastructure in a manner that protects

the sources and methods that led to the finding of the compromise.''.

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

(1) in the first paragraph (12), by striking ''section 2215'' and inserting ''section 2217''; and

(2) by redesignating the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

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

(d) ADDITIONAL TECHNICAL AMENDMENT.—

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

ceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

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