

117TH CONGRESS
1ST SESSION

S. 2407

To ensure timely Federal Government awareness of cyber intrusions that pose a threat to national security, enable the development of a common operating picture of national-level cyber threats, and to make appropriate, actionable cyber threat information available to the relevant government and private sector entities, as well as the public, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 21, 2021

Mr. WARNER (for himself, Mr. RUBIO, Ms. COLLINS, Mr. HEINRICH, Mr. TESTER, Mr. KING, Mr. BURR, Mr. BLUNT, Mr. BENNET, Mr. CASEY, Mr. SASSE, Mrs. GILLIBRAND, Mrs. FEINSTEIN, Mr. RISCH, and Mr. MANCHIN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To ensure timely Federal Government awareness of cyber intrusions that pose a threat to national security, enable the development of a common operating picture of national-level cyber threats, and to make appropriate, actionable cyber threat information available to the relevant government and private sector entities, as well as the public, 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.**

2 This Act may be cited as the “Cyber Incident Notifi-
3 cation Act of 2021”.

4 **SEC. 2. CYBERSECURITY INTRUSION REPORTING CAPABILI-**
5 **TIES.**

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

9 **“Subtitle C—Cybersecurity**
10 **Intrusion Reporting Capabilities**

11 **“SEC. 2231. DEFINITIONS.**

12 “In this subtitle:

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

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

18 “(3) APPROPRIATE CONGRESSIONAL COMMIT-
19 TEES.—In this section, the term ‘appropriate con-
20 gressional committees’ means—

21 “(A) the Committee on Homeland Security
22 and Governmental Affairs of the Senate;

23 “(B) the Select Committee on Intelligence
24 of the Senate;

25 “(C) the Committee on the Judiciary of
26 the Senate;

1 “(D) the Committee on Armed Services of
2 the Senate;

3 “(E) the Committee on Homeland Security
4 of the House of Representatives;

5 “(F) the Permanent Select Committee on
6 Intelligence of the House of Representatives;

7 “(G) the Committee on the Judiciary of
8 the House of Representatives; and

9 “(H) the Committee on Armed Services of
10 the House of Representatives.

11 “(4) COVERED ENTITY.—The term ‘covered en-
12 tity’ has the meaning given the term under the rules
13 required to be promulgated under section 2233(d).

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

18 “(6) CYBER INTRUSION REPORTING CAPABILI-
19 TIES.—The term ‘Cyber Intrusion Reporting Capa-
20 bilities’ means the cybersecurity intrusion reporting
21 capabilities established under section 2232.

22 “(7) CYBERSECURITY NOTIFICATION.—The
23 term ‘cybersecurity notification’ means a notification
24 of a cybersecurity intrusion, as defined in accord-
25 ance with section 2233.

1 “(8) DIRECTOR.—The term ‘Director’ means
2 the Director of the Cybersecurity and Infrastructure
3 Security Agency.

4 “(9) FEDERAL AGENCY.—The term ‘Federal
5 agency’ has the meaning given the term ‘agency’ in
6 section 3502 of title 44, United States Code.

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

9 “(A) means a contractor or subcontractor
10 (at any tier) of the United States Government;
11 and

12 “(B) does not include a contractor or sub-
13 contractor that holds only—

14 “(i) service contracts to provide
15 housekeeping or custodial services; or

16 “(ii) contracts to provide products or
17 services unrelated to information tech-
18 nology below the micro-purchase threshold
19 (as defined in section 2.101 of title 48,
20 Code of Federal Regulations, or any suc-
21 cessor thereto).

22 “(11) INFORMATION TECHNOLOGY.—The term
23 ‘information technology’ has the meaning given the
24 term in section 11101 of title 40, United States
25 Code.

1 “(12) RANSOMWARE.—The term ‘ransomware’
2 means any type of malicious software that prevents
3 the legitimate owner or operator of an information
4 system or network from accessing computer files,
5 systems, or networks and demands the payment of
6 a ransom for the return of such access.

7 **“SEC. 2232. ESTABLISHMENT OF CYBERSECURITY INTRU-**
8 **SION REPORTING CAPABILITIES.**

9 “(a) DESIGNATION.—The Agency shall be the des-
10 ignated agency within the Federal Government to receive
11 cybersecurity notifications from other Federal agencies
12 and covered entities in accordance with this subtitle.

13 “(b) ESTABLISHMENT.—Not later than 240 days
14 after the date of enactment of this subtitle, the Director
15 shall establish Cyber Intrusion Reporting Capabilities to
16 facilitate the submission of timely, secure, and confidential
17 cybersecurity notifications from Federal agencies and cov-
18 ered entities to the Agency.

19 “(c) RE-EVALUATION OF SECURITY.—The Director
20 shall re-evaluate the security of the Cyber Intrusion Re-
21 porting Capabilities not less frequently than once every 2
22 years.

23 “(d) REQUIREMENTS.—The Cyber Intrusion Report-
24 ing Capabilities shall allow the Agency—

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

3 “(2) to accept a cybersecurity notification from
4 any entity, regardless of whether the entity is a cov-
5 ered entity.

6 “(e) LIMITATIONS ON USE OF INFORMATION.—Any
7 cybersecurity notification submitted to the Agency
8 through the Cyber Intrusion Reporting Capabilities estab-
9 lished under this section—

10 “(1) shall be exempt from disclosure under sec-
11 tion 552 of title 5, United States Code (commonly
12 referred to as the “Freedom of Information Act”),
13 in accordance with subsection (b)(3)(B) of such sec-
14 tion 552, and any State, Tribal, or local provision of
15 law requiring disclosure of information or records;
16 and

17 “(2) may not be—

18 “(A) admitted as evidence in any civil or
19 criminal action brought against the victim of
20 the cybersecurity incident, except for actions
21 brought by the Federal Government under sec-
22 tion 2233(h); or

23 “(B) subject to a subpoena, unless the sub-
24 poena is issued by Congress and necessary for
25 congressional oversight purposes.

1 “(f) PRIVACY.—The Agency shall adopt privacy and
2 data protection procedures, based on the comparable pri-
3 vacy and data protection procedures developed for infor-
4 mation received and shared pursuant to the Cybersecurity
5 Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.),
6 for information submitted to the Agency through the
7 Cyber Intrusion Reporting Capabilities established under
8 subsection (b) that is known at the time of sharing to con-
9 tain personal information of a specific individual or infor-
10 mation that identifies a specific individual that is not di-
11 rectly related to a cybersecurity threat.

12 “(g) ANNUAL REPORTS.—

13 “(1) DIRECTOR REPORTING REQUIREMENT.—
14 Not later than 1 year after the date on which the
15 Cyber Intrusion Reporting Capabilities are estab-
16 lished and once each year thereafter, the Director
17 shall submit to the appropriate congressional com-
18 mittees a report, in classified form if necessary, on
19 the number of notifications received through the
20 Cyber Intrusion Reporting Capabilities, and a de-
21 scription of the associated mitigations taken, during
22 the 1-year period preceding the report.

23 “(2) SECRETARY REPORTING REQUIREMENT.—

24 Not later than 1 year after the date on which the
25 Cyber Intrusion Reporting Capabilities are estab-

1 lished, and once each year thereafter, the Secretary
2 shall submit to the appropriate congressional com-
3 mittees a report on—

4 “(A) the categories of covered entities, not-
5 ing additions or removals of categories, that are
6 required to submit cybersecurity notifications;
7 and

8 “(B) the types of cybersecurity intrusions
9 and other information required to be submitted
10 as a cybersecurity notification, noting any
11 changes from the previous submission.

12 “(3) FORM.—The annual reports required
13 under this subsection may be submitted as a single
14 report for each year, at the discretion of the Sec-
15 retary.

16 **“SEC. 2233. REQUIRED NOTIFICATIONS.**

17 “(a) NOTIFICATIONS.—

18 “(1) IN GENERAL.—Except as provided in para-
19 graph (2), not later than 24 hours after the con-
20 firmation of a cybersecurity intrusion or potential
21 cybersecurity intrusion, the Federal agency or cov-
22 ered entity that discovered the cybersecurity intru-
23 sion or potential cybersecurity intrusion shall submit
24 a cybersecurity notification to the Agency through
25 the Cyber Intrusion Reporting Capabilities.

1 “(2) EXCEPTION.—If a Federal agency or cov-
2 ered entity required to submit a cybersecurity notifi-
3 cation under paragraph (1) is subject to another
4 Federal law, regulation, policy, or government con-
5 tract requiring notification of a cybersecurity intru-
6 sion or potential cybersecurity intrusion to a Federal
7 agency within less than 24 hours, the notification
8 deadline required in the applicable law, regulation,
9 or policy shall also apply to the notification required
10 under this section.

11 “(b) REQUIRED UPDATES.—A Federal agency or
12 covered entity that submits a cybersecurity notification
13 under subsection (a) shall, until the date on which the cy-
14 bersecurity incident is mitigated or any follow-up inves-
15 tigation is completed, submit updated cybersecurity threat
16 information to the Agency through the Cyber Intrusion
17 Reporting Capabilities not later than 72 hours after the
18 discovery of new information.

19 “(c) REQUIRED CONTENTS.—The notification and
20 required updates submitted under subsections (a) and (b)
21 shall include, at minimum, any information required to be
22 included pursuant to the rules promulgated under sub-
23 section (d).

24 “(d) REQUIRED RULEMAKING.—

1 “(1) IN GENERAL.—Notwithstanding any provi-
2 sions set out in this title that may limit or restrict
3 the promulgation of rules, and not later than 270
4 days after the date of enactment of this subtitle, the
5 Secretary, acting through the Director, in coordina-
6 tion with the Director of National Intelligence, the
7 Director of the Office of Management and Budget,
8 the Secretary of Defense, and the National Cyber
9 Director, shall promulgate interim final rules,
10 waiving prior public notice, and accepting comments
11 after the effective date in order to inform the final
12 rules—

13 “(A) that define ‘covered entity’ for the
14 purpose of identifying entities subject to the cy-
15 bersecurity notification requirements of this
16 section and which shall include, at a minimum,
17 Federal contractors, owners or operators of
18 critical infrastructure, as determined appro-
19 priate by the Director based on assessment of
20 risks posed by compromise of critical infrastruc-
21 ture operation, and nongovernmental entities
22 that provide cybersecurity incident response
23 services;

24 “(B) that define ‘cybersecurity intrusion’
25 and ‘potential cybersecurity intrusion’ for the

1 purpose of determining when a cybersecurity
2 notification shall be submitted under this sec-
3 tion;

4 “(C) that define ‘cybersecurity threat in-
5 formation’ for the purpose of describing the
6 threat information to be included in a cyberse-
7 curity notification under this section;

8 “(D) that define ‘confirmation of a cyber-
9 security incident or potential cybersecurity inci-
10 dent’ for the purpose of determining when a no-
11 tification obligation is triggered;

12 “(E) that address whether a Federal agen-
13 cy or covered entity shall be required to provide
14 a cybersecurity notification for a cybersecurity
15 intrusion of which the Federal agency or cov-
16 ered entity is aware, but does not directly im-
17 pact the networks or information systems
18 owned or operated by the Federal agency or
19 covered entity; and

20 “(F) that contain other provisions nec-
21 essary to implement the requirements of this
22 subtitle.

23 “(2) REQUIREMENTS FOR DEFINITIONS.—At a
24 minimum, the definitions of ‘cybersecurity intrusion’
25 and ‘potential cybersecurity intrusion’ required to be

1 promulgated under paragraph (1)(B) shall include a
2 cybersecurity intrusion, including an intrusion in-
3 volving ransomware, that—

4 “(A) involves or is assessed to involve a
5 nation-state;

6 “(B) involves or is assessed to involve an
7 advanced persistent threat cyber actor;

8 “(C) involves or is assessed to involve a
9 transnational organized crime group (as defined
10 in section 36 of the State Department Basic
11 Authorities Act of 1956 (22 U.S.C. 2708));

12 “(D) results, or has the potential to result,
13 in demonstrable harm to the national security
14 interests, foreign relations, or economy of the
15 United States or to the public confidence, civil
16 liberties, or public health and safety of people
17 in the United States;

18 “(E) is or is likely to be of significant na-
19 tional consequence; or

20 “(F) is identified by covered entities but
21 affects, or has the potential to affect, agency
22 systems.

23 “(3) REQUIRED INFORMATION FOR CYBERSE-
24 CURITY THREAT INFORMATION.—For purposes of
25 the rules required to be promulgated under para-

1 graph (1)(B), the cybersecurity threat information
2 required to be included in a cybersecurity notifica-
3 tion shall include, at a minimum—

4 “(A) a description of the cybersecurity in-
5 trusion, including identification of the affected
6 systems and networks that were, or are reason-
7 ably believed to have been, accessed by a cyber
8 actor, and the estimated dates of when such an
9 intrusion is believed to have occurred;

10 “(B) a description of the vulnerabilities le-
11 veraged, and tactics, techniques, and procedures
12 used by the cyber actors to conduct the intru-
13 sion;

14 “(C) any information that could reasonably
15 help identify the cyber actor, such as internet
16 protocol addresses, domain name service infor-
17 mation, or samples of malicious software; and

18 “(D) contact information, such as a tele-
19 phone number or electronic mail address, that
20 a Federal agency may use to contact the cov-
21 ered entity, either directly or through an au-
22 thorized agent of the covered entity; and

23 “(E) actions taken to mitigate the intru-
24 sion.

1 “(4) REQUIRED CONSULTATION.—For purposes
2 of the rules required to be promulgated under para-
3 graph (1), the Secretary, acting through the Direc-
4 tor, shall consult with appropriate private sector
5 stakeholders, as determined by the Secretary, in co-
6 ordination with the Director of National Intelligence,
7 the Director of the Office of Management and Budg-
8 et, the Secretary of Defense, and the National Cyber
9 Director.

10 “(e) REQUIRED RESPONSE.—The Director shall de-
11 velop and implement a process to respond to a Federal
12 agency or covered entity that submits a cybersecurity noti-
13 fication under subsection (a) not later than 2 business
14 days after the date on which the notification is submitted,
15 which shall notify the entity as to whether the Director
16 requires further information about the cybersecurity intru-
17 sion.

18 “(f) REQUIRED COORDINATION WITH SECTOR RISK
19 MANAGEMENT OR OTHER REGULATORY AGENCIES.—The
20 Secretary of Homeland Security, acting through the Di-
21 rector, in coordination with the head of each Sector Risk
22 Management Agency and other Federal agencies, as deter-
23 mined appropriate by the Director, shall—

24 “(1) establish a set of reporting criteria for
25 Sector Risk Management Agencies and other Fed-

1 eral agencies as identified by the Director to submit
2 cybersecurity notifications regarding cybersecurity
3 incidents affecting covered entities in their respective
4 sectors or covered entities regulated by such Federal
5 agencies to the Agency through the Cyber Intrusion
6 Reporting Capabilities; and

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

11 “(g) PROTECTION FROM LIABILITY.—No cause of
12 action shall lie or be maintained in any court by any per-
13 son or entity, other than the Federal Government pursu-
14 ant to subsection (h) or any applicable law, against any
15 covered entity due to the submission by that person or
16 entity of a cybersecurity notification to the Agency
17 through the Cyber Intrusion Reporting System, in con-
18 formance with this subtitle and the rules promulgated
19 under subsection (d), and any such action shall be prompt-
20 ly dismissed.

21 “(h) ENFORCEMENT.—

22 “(1) IN GENERAL.—If, on the basis of any in-
23 formation, the Director determines that a covered
24 entity has violated, or is in violation of, the require-
25 ments of this subtitle, including rules promulgated

1 under this subtitle, the Director may assess a civil
2 penalty not to exceed 0.5 percent of the entity's
3 gross revenue from the prior year for each day the
4 violation continued or continues.

5 “(2) DETERMINATION OF AMOUNT.—The Di-
6 rector shall have the authority to reduce or other-
7 wise modify the civil penalties assessed under para-
8 graph (1) and may take into account mitigating or
9 aggravating factors, including the nature, cir-
10 cumstances, extent, and gravity of the violations
11 and, with respect to the covered entity, the covered
12 entity's ability to pay, degree of culpability, and his-
13 tory of prior violations.

14 “(3) PROCEDURES.—The Director shall estab-
15 lish procedures for contesting civil penalties imposed
16 under this section.

17 “(4) COVERED ENTITIES WITH FEDERAL GOV-
18 ERNMENT CONTRACTS.—In addition to the penalties
19 authorized under this subsection, if a covered entity
20 with a Federal Government contract violates the re-
21 quirements of this subtitle, including rules promul-
22 gated under this subtitle, the Administrator of the
23 General Services Administration may assess addi-
24 tional available penalties, including removal from the
25 Federal Contracting Schedule.

1 “(5) FEDERAL AGENCIES.—If a Federal agency
2 violates the requirements of this subtitle, the viola-
3 tion shall be referred to the Inspector General for
4 the agency, and shall be treated by the Inspector
5 General for the agency as a matter of urgent con-
6 cern.

7 “(i) EXEMPTION.—All information collection activi-
8 ties under sections 2232 and 2233 of this subtitle shall
9 be exempt from the requirements of sections 3506(e),
10 3507, 3508, and 3509 of title 44, United States Code
11 (commonly known as the ‘Paperwork Reduction Act’).

12 “(j) RULE OF CONSTRUCTION.—Nothing in this sub-
13 title shall be construed to supersede any reporting require-
14 ments under subchapter I of chapter 35 of title 44, United
15 States Code.

16 **“SEC. 2234. PRESERVATION OF INFORMATION.**

17 “(a) IN GENERAL.—Not later than 60 days after the
18 date of enactment of this subtitle, the Secretary, acting
19 through the Director, in coordination with the Director of
20 the Office of Management and Budget, shall promulgate
21 rules for data preservation standards and requirements for
22 Federal agencies and covered entities to assist with cyber-
23 security intrusion response and associated investigatory
24 activities.

1 “(b) **MINIMUM REQUIREMENTS.**—The rules for data
2 preservation promulgated under subsection (a) shall re-
3 quire, at a minimum, that a Federal agency or covered
4 entity that submits a cybersecurity notification under this
5 subtitle shall preserve all of the data designated for preser-
6 vation under such rules.

7 **“SEC. 2235. ANALYSIS OF CYBERSECURITY NOTIFICATIONS.**

8 “(a) **ANALYSIS.**—

9 “(1) **IN GENERAL.**—The Secretary, acting
10 through the Director, the Attorney General, and the
11 Director of National Intelligence, shall jointly de-
12 velop procedures for ensuring any cybersecurity noti-
13 fication submitted to the System is promptly and ap-
14 propriately analyzed to—

15 “(A) determine the impact of the breach or
16 intrusion on the national economy and national
17 security;

18 “(B) identify the potential source or
19 sources of the breach or intrusion;

20 “(C) recommend actions to mitigate the
21 impact of the breach or intrusion; and

22 “(D) provide information on methods of
23 securing the system or systems against future
24 breaches or intrusions.

1 “(2) REQUIREMENT.—The procedures required
2 to be developed under paragraph (1) shall include
3 criteria for when rapid analysis, notification, or pub-
4 lic dissemination is required.

5 “(3) AUTHORITY.—The Secretary, acting
6 through the Director, the Attorney General, and the
7 Director of National Intelligence may each designate
8 employees within each respective agency who may
9 search intelligence and law enforcement information
10 for cyber threat intelligence information with a na-
11 tional security or public safety purpose, based on cy-
12 bersecurity notifications received by the Agency
13 through the Cyber Intrusion Reporting Capabilities,
14 and consistent with the procedures developed under
15 paragraph (1).

16 “(b) ANALYTIC PRODUCTION.—

17 “(1) IN GENERAL.—Not less frequently than
18 once every 30 days, the Secretary, acting through
19 the Director, the Attorney General, and the Director
20 of National Intelligence shall produce a joint cyber
21 threat intelligence report that characterizes the cur-
22 rent cyber threat picture facing Federal agencies
23 and covered entities.

24 “(2) REQUIREMENTS.—Each report required to
25 be produced under paragraph (1)—

1 “(A) shall be in a form which may be
2 made publicly available;

3 “(B) may include a classified annex, as
4 necessary; and

5 “(C) shall, to the maximum extent prac-
6 tical, anonymize attribution information from
7 cybersecurity notifications received through the
8 Cyber Intrusion Reporting Capabilities.

9 “(3) AUTHORITY TO DECLASSIFY.—The Direc-
10 tor of National Intelligence may declassify any ana-
11 lytic products, or portions thereof, produced under
12 this section if such declassification is required to
13 mitigate cyber threats facing the United States.”.

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

 “Subtitle C—Cybersecurity Intrusion Reporting Capabilities

 “Sec. 2231. Definitions.

 “Sec. 2232. Establishment of cybersecurity intrusion reporting capabilities.

 “Sec. 2233. Required notifications.

 “Sec. 2234. Preservation of information.

 “Sec. 2235. Analysis of cybersecurity notifications.”.

18 (c) TECHNICAL AND CONFORMING AMENDMENTS.—
19 Section 2202(c) of the Homeland Security Act of 2002
20 (6 U.S.C. 652(c)) is amended—

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

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

6 “(13) carry out the responsibilities described in
7 subtitle C relating to the cybersecurity intrusion re-
8 porting capabilities;”.

○