

117TH CONGRESS
1ST SESSION

S. _____

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

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

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 Homeland Security
2 of the House of Representatives;

3 “(E) the Permanent Select Committee on
4 Intelligence of the House of Representatives;
5 and

6 “(F) the Committee on the Judiciary of
7 the House of Representatives.

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

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

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

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

23 “(8) DIRECTOR.—The term ‘Director’ means
24 the Director of the Cybersecurity and Infrastructure
25 Security Agency.

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

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

6 “(A) means a contractor or subcontractor
7 (at any tier) of the United States Government;
8 and

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

11 “(i) service contracts to provide
12 housekeeping or custodial services; or

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

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

23 “(12) RANSOMWARE.—The term ‘ransomware’
24 means any type of malicious software that prevents
25 the legitimate owner or operator of an information

1 system or network from accessing computer files,
2 systems, or networks and demands the payment of
3 a ransom for the return of such access.

4 **“SEC. 2232. ESTABLISHMENT OF CYBERSECURITY INTRU-**
5 **SION REPORTING CAPABILITIES.**

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

10 “(b) ESTABLISHMENT.—Not later than 180 days
11 after the date of enactment of this subtitle, the Director
12 shall establish Cyber Intrusion Reporting Capabilities to
13 facilitate the submission of timely, secure, and confidential
14 cybersecurity notifications from Federal agencies and cov-
15 ered entities to the Agency.

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

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

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

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

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

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

15 “(2) may not be—

16 “(A) admitted as evidence in any civil or
17 criminal action; or

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

21 “(f) PRIVACY.—The Agency shall adopt privacy and
22 protection procedures, based on the comparable privacy
23 and protection procedures developed for information re-
24 ceived and shared pursuant to the Cybersecurity Informa-
25 tion Sharing Act of 2015 (6 U.S.C. 1501 et seq.), for in-

1 formation submitted to the Agency through the Cyber In-
2 trusion Reporting Capabilities established under sub-
3 section (b) that is known at the time of sharing to contain
4 personal information of a specific individual or informa-
5 tion that identifies a specific individual that is not directly
6 related to a cybersecurity threat.

7 “(g) ANNUAL REPORTS.—

8 “(1) DIRECTOR REPORTING REQUIREMENT.—

9 Not later than 1 year after the date on which the
10 Cyber Intrusion Reporting Capabilities are estab-
11 lished and once each year thereafter, the Director
12 shall submit to the appropriate congressional com-
13 mittees a report, in classified form if necessary, on
14 the number of notifications received through the
15 Cyber Intrusion Reporting Capabilities, and a de-
16 scription of the associated mitigations taken, during
17 the 1-year period preceding the report.

18 “(2) SECRETARY REPORTING REQUIREMENT.—

19 Not later than 1 year after the date on which the
20 Cyber Intrusion Reporting Capabilities are estab-
21 lished, and once each year thereafter, the Secretary
22 shall submit to the appropriate congressional com-
23 mittees a report on—

24 “(A) the categories of covered entities, not-
25 ing additions or removals of categories, that are

1 required to submit cybersecurity notifications;
2 and

3 “(B) the types of cybersecurity intrusions
4 and other information required to be submitted
5 as a cybersecurity notification, noting any
6 changes from the previous submission.

7 **“SEC. 2233. REQUIRED NOTIFICATIONS.**

8 “(a) NOTIFICATIONS.—

9 “(1) IN GENERAL.—Except as provided in para-
10 graph (2), not later than 24 hours after the con-
11 firmation of a cybersecurity intrusion or potential
12 cybersecurity intrusion, the Federal agency or cov-
13 ered entity that discovered the cybersecurity intru-
14 sion or potential cybersecurity intrusion shall submit
15 a cybersecurity notification to the Agency through
16 the Cyber Intrusion Reporting Capabilities.

17 “(2) EXCEPTION.—If a Federal agency or cov-
18 ered entity required to submit a cybersecurity notifi-
19 cation under paragraph (1) is subject to another
20 Federal law, regulation, policy, or government con-
21 tract requiring notification of a cybersecurity intru-
22 sion or potential cybersecurity intrusion to a Federal
23 agency within less than 24 hours, the notification
24 deadline required in the applicable law, regulation,

1 or policy shall also apply to the notification required
2 under this section.

3 “(b) REQUIRED UPDATES.—A Federal agency or
4 covered entity that submits a cybersecurity notification
5 under subsection (a) shall, until the date on which the cy-
6 bersecurity incident is mitigated or any follow-up inves-
7 tigation is completed, submit updated cybersecurity threat
8 information to the Agency through the Cyber Intrusion
9 Reporting Capabilities not later than 72 hours after the
10 discovery of new information.

11 “(c) REQUIRED CONTENTS.—The notification and
12 required updates submitted under subsections (a) and (b)
13 shall include, at minimum, any information required to be
14 included pursuant to the rules promulgated under sub-
15 section (d).

16 “(d) REQUIRED RULEMAKING.—

17 “(1) IN GENERAL.—Notwithstanding any provi-
18 sions set out in this title that may limit or restrict
19 the promulgation of rules, and not later than 60
20 days after the date of enactment of this subtitle, the
21 Secretary, acting through the Director, in coordina-
22 tion with the Director of National Intelligence, the
23 Director of the Office of Management and Budget,
24 the Secretary of Defense, and the Federal Chief In-
25 formation Officer, shall promulgate interim final

1 rules, waiving prior public notice and accepting com-
2 ments after the effective date—

3 “(A) that define ‘covered entity’ for the
4 purpose of identifying entities subject to the cy-
5 bersecurity notification requirements of this
6 section and which shall include, at a minimum,
7 Federal contractors, owners or operators of
8 critical infrastructure, and nongovernmental en-
9 tities that provide cybersecurity incident re-
10 sponse services;

11 “(B) that define ‘cybersecurity intrusion’
12 and ‘potential cybersecurity intrusion’ for the
13 purpose of determining when a cybersecurity
14 notification shall be submitted under this sec-
15 tion;

16 “(C) that define ‘cybersecurity threat in-
17 formation’ for the purpose of describing the
18 threat information to be included in a cyberse-
19 curity notification under this section;

20 “(D) that define ‘confirmation of a cyber-
21 security incident or potential cybersecurity inci-
22 dent’ for the purpose of determining when a no-
23 tification obligation is triggered; and

24 “(E) that address whether a Federal agen-
25 cy or covered entity shall be required to provide

1 a cybersecurity notification for a cybersecurity
2 intrusion of which the Federal agency or cov-
3 ered entity is aware, but does not directly im-
4 pact the networks or information systems
5 owned or operated by the Federal agency or
6 covered entity.

7 “(2) REQUIREMENTS FOR DEFINITIONS.—At a
8 minimum, the definitions required to be promulgated
9 under paragraph (1)(B) shall include a cybersecurity
10 intrusion that—

11 “(A) involves or is assessed to involve a
12 nation-state;

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

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

19 “(D) results, or has the potential to result,
20 in demonstrable harm to the national security
21 interests, foreign relations, or economy of the
22 United States or to the public confidence, civil
23 liberties, or public health and safety of people
24 in the United States;

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

3 “(F) is identified by covered entities but
4 affects, or has the potential to affect, agency
5 systems; or

6 “(G) involves ransomware.

7 “(3) REQUIRED INFORMATION FOR CYBERSE-
8 CURITY THREAT INFORMATION.—For purposes of
9 the rules required to be promulgated under para-
10 graph (1)(B), the cybersecurity threat information
11 required to be included in a cybersecurity notifica-
12 tion shall include, at a minimum—

13 “(A) a description of the cybersecurity in-
14 trusion, including identification of the affected
15 systems and networks that were, or are reason-
16 ably believed to have been, accessed by a cyber
17 actor, and the estimated dates of when such an
18 intrusion is believed to have occurred;

19 “(B) a description of the vulnerabilities le-
20 veraged, and tactics, techniques, and procedures
21 used by the cyber actors to conduct the intru-
22 sion;

23 “(C) any information that could reasonably
24 help identify the cyber actor, such as internet

1 protocol addresses, domain name service infor-
2 mation, or samples of malicious software; and

3 “(D) contact information, such as a tele-
4 phone number or electronic mail address, that
5 a Federal agency may use to contact the cov-
6 ered entity, either directly or through an au-
7 thorized agent of the covered entity; and

8 “(E) actions taken to mitigate the intru-
9 sion.

10 “(e) REQUIRED COORDINATION WITH SECTOR RISK
11 MANAGEMENT AGENCIES.—The Secretary of Homeland
12 Security, acting through the Director, in coordination with
13 the head of each Sector Risk Management Agency and
14 other Federal agencies, as determined appropriate by the
15 Director, shall—

16 “(1) establish a set of reporting criteria for
17 Sector Risk Management Agencies and other Fed-
18 eral agencies as identified by the Director to submit
19 cybersecurity notifications regarding cybersecurity
20 incidents affecting covered entities in their respective
21 sectors or covered entities regulated by such Federal
22 agencies to the Agency through the Cyber Intrusion
23 Reporting Capabilities; and

24 “(2) take steps to harmonize the criteria de-
25 scribed in paragraph (1) with the regulatory report-

1 ing requirements in effect on the date of enactment
2 of this subtitle.

3 “(f) PROTECTION FROM LIABILITY.—No cause of ac-
4 tion shall lie or be maintained in any court by any person
5 or entity, other than the Federal Government pursuant
6 to subsection (g) or any applicable law, against any cov-
7 ered entity due to the submission of a cybersecurity notifi-
8 cation to the Agency through the Cyber Intrusion Report-
9 ing System, in conformance with this subtitle and the
10 rules promulgated under subsection (d), and any such ac-
11 tion shall be promptly dismissed.

12 “(g) ENFORCEMENT.—

13 “(1) COVERED ENTITIES WITH FEDERAL GOV-
14 ERNMENT CONTRACTS.—If a covered entity violates
15 the requirements of this subtitle, including the rules
16 promulgated under this subtitle, the covered entity
17 shall be subject to penalties determined by the Ad-
18 ministrator of the General Services Administration,
19 which may include removal from the Federal Con-
20 tracting Schedules.

21 “(2) COVERED ENTITIES WITHOUT FEDERAL
22 GOVERNMENT CONTRACTS.—If a covered entity vio-
23 lates the requirements of this subtitle, including the
24 rules promulgated under this subtitle, the covered
25 entity shall be subject to financial penalties equal to

1 0.5 percent per day of the entity’s gross revenue
2 from the prior year.

3 “(3) FEDERAL AGENCIES.—If a Federal agency
4 violates the requirements of this subtitle, the viola-
5 tion shall be referred to the Inspector General for
6 the agency, and shall be treated as a matter of ur-
7 gent concern.

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

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

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

18 “(a) IN GENERAL.—Not later than 60 days after the
19 date of enactment of this subtitle, the Secretary, acting
20 through the Director, in coordination with the Director of
21 the Office of Management and Budget, shall promulgate
22 rules for data preservation standards and requirements for
23 Federal agencies and covered entities to assist with cyber-
24 security intrusion response and associated investigatory
25 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
8 Reporting Capabilities;”.