AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 633

117TH CONGRESS *2d Session*	SENATE	REPORT 117–249

CYBER INCIDENT REPORTING ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2875

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO ESTABLISH THE CYBER INCIDENT REVIEW OFFICE IN THE CYBERSECURIY AND INFRASTRUCTURE SECURITY AGENCY OF THE DEPARTMENT OF HOMELAND SECURITY, AND FOR OTHER PURPOSES

DECEMBER 13, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 633

117TH CONGRESS *2d Session* | SENATE | REPORT 117–249

CYBER INCIDENT REPORTING ACT OF 2021

DECEMBER 13, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2875]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2875), to amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes, having considered the same, reports favorably thereon with an amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2875, *the Cyber Incident Reporting Act of 2021*, creates a system for critical infrastructure victims of cyber incidents and most ransomware victims who make ransom payments to share information about such attacks and payments with the federal government, in order to bolster the government's understanding and response to such attacks. In 2020 alone, malicious cyber actors targeted a wide range of critical infrastructure entities, including health care facilities, transportation and utility entities, schools, and local govern-

ments, with hundreds of debilitating ransomware attacks. The federal government, however, lacks the necessary situational awareness to respond to and mitigate this alarming trend. The *Cyber Incident Reporting Act of 2021* will help combat these attacks by providing enhanced coordination measures and promoting shared awareness of the cyber threat across the public and private sectors.

II. Background and Need for the Legislation

The federal government does not know how often critical infrastructure owners and operators experience substantial cyber incidents, which limits situational awareness of malicious cyber actors' impact on national security, reduces effectiveness in assisting victims response and recovery from cyber attacks, and hinders the government's ability to help prevent future attacks.[1] The increase in ransomware attacks on public and private entities has also caused a national security need for the government to know when these payments are made so that they may render assistance to victims and disrupt criminal enterprises executing these attacks.

Cyber attacks, including ransomware attacks, have increased in recent years. In 2020, the Federal Bureau of Investigation (FBI) received nearly 800,000 cyber complaints from victims, which was a 69 percent increase from 2019.[2] Private sector companies, such as Accenture Security, found that incidents increased globally by 125 percent, with the United States experiencing the bulk of those incidents.[3] The victims of these attacks span from major critical infrastructure entities to small businesses. The attacks and exploitations of SolarWinds' Orion software, the Microsoft Exchange Servers, the water supply system in the town of Oldsmar, Florida, and the Pulse Secure virtual private network (VPN) servers are just a few of the growing number of attacks on entities that are critical to national security.[4] Cybercriminals have also launched ransomware attacks against a range of public and private entities. Russia-based hackers used ransomware to disrupt one of the largest oil and natural gas pipelines in the United States, Colonial Pipeline.[5] Cybercriminals have also targeted the U.S. food-supply chain by attacking JBS USA and New Cooperative, an Iowa-based grain cooperative.[6] Additionally, the Financial Crimes Enforcement

---

[1] During a HSGAC hearing, National Cyber Director Chris Inglis and CISA Director Jen Easterly testified for the need for robust incident reporting. Homeland Security and Governmental Affairs Committee, *Hearing on The National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems*, 117th Cong. (Sep. 23, 2021) (S. Hrg. 117–XX). (https://www.hsgac.senate.gov/hearings/national-cybersecurity-strategy-protection-of-federal-and-critical-infrastructure-systems).

[2] Federal Bureau of Investigations, *Internet Crime Report 2020* (2020) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[3] *Triple digit increase in cyberattacks: What next?*, Accenture (Aug. 4, 2021) (https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks).

[4] *A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack,* NPR (Apr 16, 2021) (https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack); *Microsoft server hack has victims hustling to stop intruders*, Associated Press (Mar 8, 2021) (https://apnews.com/article/technology-politics-national-security-hacking-email-4813d462835dcf54cd1397adb94d468b); *'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town*, New York Times (Feb 8, 2021) https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html; *More US agencies potentially hacked, this time with Pulse Secure exploits*, Ars Technica (Apr 30, 2021) (https://arstechnica.com/gadgets/2021/04/more-us-agencies-potentially-hacked-this-time-with-pulse-secure-exploits/).

[5] *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, New York Times (May 14, 2021) (https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html).

[6] *JBS USA Cyberattack Media Statement-June* 9, JBS Foods (Jun 9, 2021) (https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9); *Iowa Grain Cooperative Hit by Cyberattack Linked to Ransomware Group*, Wall Street Journal (Sept. 20, 2021) (https://

Network found a 30 percent increase in financial institutions reporting suspicious ransomware related activities.[7] As a result, the total cost of ransoms paid to ransomware attackers reported to the Department of Treasury in the first six months of 2021 was $590 million, which was nearly $200 million more than the total amount of ransom payments reported in 2020.[8] These ransomware attacks are not limited to major institutions. One cybersecurity firm found that in the third quarter of 2020, more than 70 percent of ransomware incidents affected companies with fewer than 1,000 employees, and 60 percent of the victims had revenues of less than $50 million.[9] These statistics, however, are an incomplete picture of the threat environment. In 2016, the FBI admitted that the number of complaints only represent about 10 to 12 percent of all estimated cybercrime victims in the United States.[10]

While current state and federal laws collect certain information on data breaches and cyber incidents, the there is no fully comprehensive dataset on how often significant cyber incidents or ransomware attacks occur. All 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands have data breach notification laws, each of which have different requirements on when organizations should report when they experienced a defined breach.[11] Yet, these laws generally require organizations to report incidents when customers' personal information is breached, not when there is an impact to the organization's operations. The intent of these laws is to inform individuals of impacts to their privacy or to enable impacted individuals to take actions to protect their identities.[12]

At the federal level, a number of laws and regulations require certain critical infrastructure sectors to report specific types of breaches or incidents, but not comprehensively. The Securities and Exchange Commission (SEC), for instance, issued guidance in 2018 that interprets the Sarbanes-Oxley Act of 2002 by requiring publicly traded companies to inform investors about material cybersecurity risks and incidents in a timely fashion and to disclose to the SEC these incidents.[13] The Transportation Security Administration (TSA) issued security directives in 2021 to require owners and operators of pipelines and passenger railroads to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA).[14] The Federal Energy Regulatory Commission (FERC) has

---

www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945).

[7] U.S. Treasury Department, Financial Crimes Enforcement Network, *Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*, (2021) (https://www.fincen.gov/sites/default/files/2021–10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf).

[8] *Id.*

[9] *Why Small and Medium-Sized Professional Service Firms Are a Big Target for Ransomware Attacks*, Coveware (Jan. 3, 2021) (https://www.coveware.com/blog/2020/11/30/why-small-professional-service-firms-are-ransomware-targets).

[10] *An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported*, New York Times, (Feb. 5, 2018) (https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html).

[11] *Security Breach Notification Laws*, National Conference of State Legislatures (Apr. 15, 2021) (https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[12] *Id.*

[13] Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, (Release Nos. 33–10459; 34–82746) (Feb. 26, 2018) (https://www.sec.gov/rules/interp/2018/33–10459.pdf).

[14] U.S. Department of Homeland Security, *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators*, (Jul. 20, 2021) (https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators). And

Continued

implemented requirements on certain bulk power systems to provide information on "reportable cyber security incident[s]" to the government within one hour of determining the incident occurring.[15]

Both government and private officials concur that these current laws and regulations do not cover the full gambit of critical infrastructure entities and the type of incidents that are germane to national security. The U.S. Cyberspace Solarium Commission—a congressionally mandated commission comprised of lawmakers, federal officials, and private sector stakeholders—concluded that "there are insufficient federal and state laws and policies requiring companies to report incidents that impact or threaten to impact business operations. While mandated reporting for regulatory purposes and voluntary information-sharing protections exist, the federal government lacks a mandate to systematically collect cyber incident information reliably and at the scale necessary to inform situational awareness."[16] The Institute for Security and Technology's Ransomware Task Force, an international group that included multinational companies and the U.S. and foreign governments, also iterated the need for updating data breach laws to include ransomware reporting requirements. They recommended that a "ransom payment disclosure requirement would help increase the understanding of the scope and scale of the crime, allow for better estimates of the societal impact of these payments, and enable better targeting of disruption activities."[17]

S. 2875 improves the federal government's situational awareness of significant cyber incidents and ransomware attacks occurring in the United States, which will enhance the government's prevention and response efforts. S. 2875 requires certain critical infrastructure entities to report to the government within 72 hours if they experience a covered cybersecurity incident. It also creates reporting requirements for entities that pay a ransom to a ransomware actor to report to CISA within 24 hours of making the payment, except for a subset of small businesses and individuals. The bill provides authority to CISA to subpoena organizations that fail to report a covered cyber incident or ransomware payment and to then report potential wrongdoing to relevant federal regulators or the Attorney General.

The legislation also improves internal federal government information sharing when agencies receive information about cyber incidents. The bill requires every agency all federal agencies that receive reports of a cyber attacks to provide that information to the Director of CISA no later than 24 hours after receiving the notification. This ensures that cyber attack information coming into the government based on different regulations or laws is all shared with CISA, allowing for comprehensive analysis. The bill also re-

---

U.S. Department of Homeland Security, Transportation Security Administration, *Security Directive 1582–21–01*, (2021) (https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf).

[15] Federal Energy Regulatory Commission (164 FERC ¶ 61,033) (Jun. 20, 2019) (https://www.ferc.gov/sites/default/files/2020-04/E-2_8.pdf); North American Electric Reliability Corporation, *Cyber Security—Incident Reporting and Response Planning* (CIP–008–6) (Jan. 22, 2019) (https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf).

[16] United States Cyberspace Solarium Commission, *Final Report* (Mar. 2020) (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view).

[17] Institute for Security + Technology, *Ransomware Task Force: Combatting Ransomware* (2021) (https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf).

quires for each of significant cyber incident and ransomware payment report submitted to CISA, that CISA share the reported information within 24 hours with appropriate Sector Risk Management Agencies and other appropriate agencies as determined by the Director of Office Management and Budget, in consultation with the Director and the National Cyber Director (NCD). This ensures that the relevant agencies across the government also have access to this information.

S. 2875 also requires CISA to launch a vulnerability warning pilot program to identify and notify owners of systems that have security vulnerabilities that ransomware actors could exploit. The NCD must also establish a joint ransomware task force to coordinate federal efforts to prevent and disrupt ransomware attacks.

III. Legislative History

Chairman Peters (D–MI) and Ranking Member Portman (R–OH) introduced S. 2875 on September 28, 2021. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. The Committee considered S. 2875 at a business meeting on October 6, 2021. During the business meeting, Chairman Peters and Ranking Member Portman offered a substitute amendment, which was adopted by unanimous consent.

Ranking Member Portman offered two amendments. The first amendment, as modified, made clear that reports submitted under this legislation, as well as any other documents and records developed in drafting those reports, are not discoverable or otherwise useable in criminal proceedings, civil litigation, or regulatory enforcement proceedings. The amendment, as modified, was adopted by voice vote, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present. Ranking Member Portman's second amendment updated the definition of small business to utilize the statutory definition of small business under the Small Business Act. The second amendment was adopted by voice vote, with Senators Peters, Carper, Hassan, Rosen, Padilla, Ossoff, Portman, Lankford, Romney, Scott, and Hawley present. Senator Scott asked to be recorded for the record as voting "No". Senator Scott offered an amendment that would limit the types of entities who are required to report if they made a ransomware payment to just covered entities and state and local governments. The amendment was not adopted by a roll call vote of 7 Yeas to 7 Nays. Senators Portman, Johnson, Lankford, Romney, Scott, and Hawley voted Yea, with Senator Paul voting Yea by proxy. Senators Peters, Hassan, Sinema, Rosen, Padilla, and Ossoff voted Nay, with Senator Carper voting Nay by proxy.

The Committee ordered the bill, as amended, reported favorably by voice vote with Senators Peters, Carper, Hassan, Rosen, Padilla, Ossoff, Portman, Lankford, Romney, Scott, and Hawley present. Senator Scott asked to be recorded for the record as voting "No".

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section designates the name of the bill as the "Cyber Incident Reporting Act of 2021."

Section 2. Definitions

This section defines "covered cyber incident," "covered entity," "cyber incident," "cyber attack," "ransom payment," "ransomware attack," "Director," "information system," and "security vulnerability."

Section 3. Cyber incident reporting

Subsection (a) amends Section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651) by defining the terms "cloud service provider," "cyber attack," "managed service provider," "ransom payment," "ransomware attack," "supply chain compromise," "virtual currency," "virtual currency address," and "sector risk management agency."

Subsection (b) amends Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 *et seq.*) by adding "Subtitle C—Cyber Incident Reporting" and establishing the following new sections:

Section 2230(a) provides that, except as provided in subsection (b), the definitions under section 2201 shall apply to this new subtitle.

Section 2230(b) defines "council," "covered cyber incident," "covered entity," "cyber incident," "cyber threat," "cyber threat indicator," "cybersecurity purpose," "defensive measure," "federal entity," "information system," "security control," "security vulnerability," and "small organization."

Section 2231(a) creates the "cyber incident review office" at CISA to receive, aggregate, and analyze reports related to covered cyber incidents submitted by covered entities and reports related to ransom payments submitted by entities.

Section 2231(b)(1) requires the Office to receive, aggregate, analyze, and secure reports from covered entities related to a covered cyber incident to assess the effectiveness of security and controls and identify tactics, techniques, and procedures adversaries use to overcome those controls.

Section 2231(b)(2) requires the Office to receive, aggregate, analyze, and secure reports related to ransom payments identify tactics, techniques, and procedures, including identifying and tracking ransom payments utilizing virtual currencies, that adversaries use to perpetuate attacks and facilitate ransom payments.

Section 2231(b)(3) requires the Office to leverage information gathered about cybersecurity incidents to: (1) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate stakeholders; and (2) provide appropriate stakeholders with timely, actionable, and anonymized reports of cyber attack campaigns and trends.

Section 2231(b)(4) requires the Office to establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered incident reports, ransom payment reports, and other voluntarily provided information.

Section 2231(b)(5) requires the Office to facilitate timely sharing of information related to covered cyber incidents and ransom payments, on a voluntary basis, between relevant critical infrastructure owners and operators.

Section 2231(b)(6) requires the Office to conduct reviews of the details surrounding covered cyber incidents or groups of those inci-

dents and identify and disseminate ways to prevent or mitigate similar incidents in the future.

Section 2231(b)(7) requires the Office to immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders.

Section 2231(b)(8) requires the Office to publish quarterly, unclassified, public reports that may be based on the unclassified information contained in the reports required under this legislation.

Section 2231(b)(9) requires the office to leverage and utilize data on ransom attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies.

Section 2231(b)(10) requires the Office to proactively identify opportunities to leverage and utilize data on cyber incidents in a manner than enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations.

Section 2231(b)(11) requires the Office to analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Office.

Section 2231(b)(12) requires the Office to share the reported information with the appropriate Sector Risk Management Agency no later than 24 hours after receiving a covered cyber incident or ransomware payment.

Section 2231(c) requires the office to provide monthly reports to the NCD and Congress characterizing the current national cyber threat landscape facing federal agencies and covered entities, including applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks.

Section 2232(a) requires covered entities that are victims of covered cyber incidents to report the covered cyber incident to the Director of CISA within 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred. The section also requires an entity, including a covered entity and except for an individual or a small organization, that makes a ransom payment, as the result of a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made. This section states that an entity shall not have to submit a report if that entity is required to report substantially similar information pursuant to another regulatory requirement.

Section 2232(b) requires CISA to issue an interim final rule to implement this section no later than 270 days after the enactment of this section, after a 60-day consultative period followed by a 90-day comment period with appropriate stakeholders, and to issue a final rule no later than one year after the publication of the interim final rule.

Section 2232(c) requires the interim rule and final rule to include: (1) a clear description of the types of entities that constitute covered entities, based on certain characteristics; (2) a clear description of the types of substantial cyber incidents that constitute covered cyber incidents, including minimum thresholds; (3) a re-

quirement that, if a covered cyber incident or a ransom payment occurs, the threat shall comply with the requirements in this subtitle in report the covered cyber incident or ransom payment; (4) a clear description of the specific required contents of the covered cyber incident report covered entities would submit; (5) a clear description of the specific required contents of a ransomware payment report submitted by an entity that makes a ransomware payment; (6) a clear description of the types of data that must be preserved; (7) deadlines for submitting reports to the Director of CISA; (8) procedures for submitting reports, carrying out the enforcement provisions, implementing various exceptions, and anonymizing and safeguarding data received and disclosed through various reports; (9) and a clear description of what entities constitute other private sector entities.

Section 2232(d) states that a covered entity or entity that makes a ransom payment may use a third party to submit their required report and requires third parties to advise their client about the reporting requirements if they knowingly make a ransomware payment on behalf of their client.

Section 2232(e) requires entities to conduct a due diligence review prior to making a ransom payment.

Section 2232(f) requires the Director of CISA to conduct an outreach and education campaign to inform likely covered entities, entities that offer to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities about the requirements of this section.

Section 2232(g) requires the Director of CISA to review data collected by the Office and, in consultation with other appropriate entities, assess the effectiveness of the rule. The Director of CISA is also required to submit to Congress the results of the evaluation and may publish thereafter a final rule implementing this section in the Federal Register.

Section 2232(h) allows the Director of CISA to reorganize and reformat the means by which covered cyber incident reports, ransom payment reports, and any other voluntarily offered information is submitted to the Office, notwithstanding chapter 35 of title 44, United States Code (commonly known as the "Paperwork Reduction Act).

Section 2233 specifies that entities may voluntarily report incidents or ransom payments to CISA that are not required pursuant to this legislation and that those voluntary reports will receive the protections within this Act.

Section 2234 specifies that if an entity is required to submit a report pursuant to this legislation and fails to comply, the Director of CISA may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment. If the Director is unable to obtain information through such engagement, the Director may issue a subpoena to the entity to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted. Section 2234 further provides that if the Director of CISA determines that the information provided in response to the subpoena constitutes grounds for regulatory enforcement action or criminal prosecution, the Di-

rector may provide that information to the Attorney General or the appropriate regulator. If a covered entity has a Federal Government contract and fails to comply with a subpoena, the Administrator of the General Services Administration may assess additional available penalties, including removal from the Federal Contracting Schedule.

Section 2235 stipulates what authorized activities the Federal Government can perform with the reported information. The section applies privacy and civil liberties protections; requires CISA to protect the reports it collects; institutes a prohibition of the use of information in regulatory actions; includes a "no waiver of privilege or protection" clause; includes an exemption from disclosure; implements an ex parte communication clause; and specifies certain liability protections. This section also stipulates that CISA shall anonymize the victim who reports the information when sharing the information with critical infrastructure owners and operators and the general public. Finally, this section makes technical and conforming changes to the Homeland Security Act of 2002.

Section 4. Federal sharing of incident reports

Subsection (a) requires any federal agency that receives a report of a cyber attack from an entity to provide that information to the Director of CISA no later than 24 hours after receiving the notification.

Subsection (b) creates an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements (including those issued through regulations) for covered entities and entities that make a ransom payment.

Subsection (c) requires the NCD to lead efforts to harmonize reporting requirements by periodically reviewing existing regulatory requirements and ensuring that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements. The NCD will also identify opportunities to streamline reporting processes, and where feasible, enter into agreements with such authorities to permit the sharing of such reports with the Office.

Section 5. Ransomware vulnerability warning program

This section requires the Director of CISA to establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures, and to dedicate resources, to identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

Section 6. Ransomware threat mitigation activities

This section requires the NCD to create an interagency "Joint Ransomware Task Force" to coordinate an ongoing, nationwide campaign against ransomware attacks and identify and pursue opportunities for international cooperation. The Task Force shall prioritize intelligence-driven operations to disrupt ransomware actors; identify a list of the highest threat ransomware entities; disrupt ransomware criminal actors, associated infrastructure, and

their finances; facilitate coordination and collaboration between the public and private sector to improve federal actions against ransomware threats; and share information on ransomware trends.

This section also requires the NCD to submit a report to Congress that describes defensive measures that private-sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

Section 7. Congressional reporting

This section requires the Director of CISA to submit to Congress a report on their stakeholder engagement in developing the interim final rule; a report on identifying opportunities to strengthen security research; a report on the ransomware vulnerability warning program; and a report on the harmonization of reporting regulations. This section also requires the Government Accountability Office to submit a report to Congress on the implementation of this legislation.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, November 30, 2021.

Hon. Gary C. Peters,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2875, the Cyber Incident Reporting Act of 2021.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

Phillip L. Swagel,
Director.

Enclosure.

At a Glance

S. 2875, Cyber Incident Reporting Act of 2021

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on October 6, 2021

By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	*	*
Revenues	0	*	*
Increase or Decrease (-) in the Deficit	0	*	*
Spending Subject to Appropriation (Outlays)	3	55	not estimated

Statutory pay-as-you-go procedures apply?	Yes	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	Yes, Under Threshold
		Contains private-sector mandate?	Yes, Under Threshold

* = between -$500,000 and $500,000.

The bill would:

- Require operators of critical infrastructure to report cyber attacks and ransom payments
- Establish a program office to receive and analyze reports on cyber incidents
- Create a pilot program to warn federal agencies and nonfederal entities that are vulnerable to ransomware
- Impose intergovernmental and private-sector mandates by requiring the owners and operators of critical infrastructure to file reports about cyber incidents and ransom payments and to retain relevant data. The bill also would preempt state, local, and tribal public disclosure laws

Estimated budgetary effects would mainly stem from:

- Implementing new cyber incident reporting processes
- Identifying information systems that have security vulnerabilities
- Collecting civil and criminal fines from entities that do not comply with disclosure requirements

Areas of significant uncertainty include:

- Predicting the annual number of cyber incidents reported to the federal government
- Anticipating how often the federal government would impose fines and penalties

Bill summary: S. 2875 would require operators of critical infrastructure (such as utilities providers) to report to the federal government about cyber attacks on their systems and about ransom payments they make to hackers. The bill would establish an office under the Cybersecurity and Infrastructure Security Agency (CISA) to receive and analyze such reports and to inform those operators of the new reporting requirements. The bill also would authorize CISA to fine critical infrastructure operators that fail to report cyber incidents.

S. 2875 also would expand CISA's authority to share information about threats of ransomware attacks with federal agencies and nonfederal entities. Ransomware attacks are attacks on informa-

tion technology systems to extort a ransom payment from victims. In the rare instances when CISA would not be able to identify the owners of computers or devices that are vulnerable to ransomware threats, the bill would authorize the agency to compel Internet service providers (ISPs) to disclose the identity of owners of such technology.

Estimated Federal cost: The estimated budgetary effects of S. 2875 are shown in Table 1. The costs of the legislation fall within budget function 050 (national defense).

TABLE 1.—ESTIMATED BUDGETARY EFFECTS OF S. 2875

	By fiscal year, millions of dollars—					
	2022	2023	2024	2025	2026	2022–2026
Cyber Incident Review Office						
Estimated Authorization	2	6	11	11	12	42
Estimated Outlays	2	6	11	11	12	42
Ransomware Vulnerability Warning Program						
Estimated Authorization	1	2	2	2	2	9
Estimated Outlays	1	2	2	2	2	9
Outreach Campaign						
Estimated Authorization	0	2	2	0	0	4
Estimated Outlays	0	2	2	0	0	4
Total Changes						
Estimated Authorization	3	10	15	13	14	55
Estimated Outlays	3	10	15	13	14	55

In addition to the budgetary effects shown above, CBO estimates that enacting S. 2875 would have insignificant effects on direct spending and revenues and would decrease the deficit by an insignificant amount over the 2022–2031 period.

Basis of estimate: For this estimate, CBO assumes that S. 2875 will be enacted in early fiscal year 2022 and that regulations for cyber incident reporting would take effect in fiscal year 2023. Outlays are based on historical spending patterns for existing or similar programs.

Under current law, nonfederal entities can voluntarily report cyber incidents to CISA. Using available data from cybersecurity firms, CBO anticipates that CISA would receive several hundred additional reports of cyber incidents per year as a result of the mandatory reporting requirements of the bill. On the basis of information from CISA, CBO expects that the costs to implement the bill would be limited to the salaries and benefits of the new staff necessary to carry out the bill's cyber incident and ransomware reporting requirements. The agency indicates it would not need new information technology systems to do so.

Spending subject to appropriation: CBO estimates that implementing the bill would cost $55 million over the 2022–2026 period. Such spending would be subject to the availability of appropriated funds.

Cyber incident review office: S. 2875 would create a new office to receive and respond to the reports of cyber incidents. Using information about the current number of cyber incidents expected to occur in the United States each year, CBO anticipates that the new office would manage approximately 500 reports annually. On the basis of information from CISA about the workload requirements of similar expansions of the agency's responsibilities, CBO expects that each analyst in the Cyber Incident Review Office would manage about 10 incident reports per year. CBO estimates that enforcing the notification requirement and managing the reported infor-

mation would require 50 full-time equivalent employees, at an average annual rate of about $187,000 per employee for compensation and benefits. CBO expects that CISA would begin hiring those employees in 2022 and that all personnel would be hired by 2024. On that basis and accounting for the effects of anticipated inflation, CBO estimates that salaries and benefits expenses of those employees would total $42 million over the 2022–2026 period.

Ransomware vulnerability warning program: S. 2875 would establish a new program to identify information technology systems that are vulnerable to ransomware attacks and inform the owners of those systems about those vulnerabilities. Using information about similar efforts, CBO expects that implementing the program would require 10 full-time equivalent employees beginning in 2022, at an average annual rate of about $187,000 per employee. The salaries and benefits expenses of those employees would total $9 million over the 2022–2026 period, CBO estimates.

Outreach campaign: S. 2875 would require CISA to inform affected entities of new regulations for cyber incident reporting that are required under the bill. Based on the costs of similar public outreach campaigns at CISA, CBO estimates that advertising contracts and publication materials would cost about $2 million annually in the first two years after enactment and $4 million over the 2023–2024 period.

Direct spending: S. 2875 would authorize CISA to issue administrative subpoenas to critical infrastructure operators that do not provide cyber incident reports in a timely manner. The bill also would authorize CISA to issue administrative subpoenas to compel ISPs to disclose the identity of owners of critical infrastructure that are vulnerable to ransomware threats.

Entities that do not comply with subpoenas could be subject to civil and criminal penalties; therefore, the government might collect additional fines under the legislation. Civil fines are recorded in the budget as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent without further appropriation. CBO expects that few critical infrastructure operators would be fined for defying subpoenas. Thus, both revenues and direct spending would increase by insignificant amounts over the 2022–2031 period. On net, enacting the bill would reduce the deficit by an insignificant amount, CBO estimates.

Uncertainty: Areas of uncertainty in this estimate include accurately predicting CISA's additional workload. Nonfederal entities are not currently required to report cyber incidents, and the bill would provide CISA with broad rulemaking authority to define reportable incidents. The budgetary effects of the bill would be moderately larger or smaller than this estimate depending on how the actual number of incidents reported to CISA differs from CBO's estimate of 500 annual reports.

The budgetary effects of the bill also would depend on the number and amounts of fines imposed under the bill's provisions. If more fines were collected than CBO expects, both direct spending and revenues would be higher than estimated.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting S. 2875 would have insignificant effects on direct

spending and revenues and would, on net, reduce the deficit by insignificant amounts.

Increase in long-term deficits: None.

Mandates: S. 2875 would impose intergovernmental and private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA). CBO estimates that the aggregate cost of those mandates would not exceed the thresholds established in UMRA for intergovernmental and private-sector mandates ($85 million and $170 million in 2021, respectively, adjusted annually for inflation).

The bill would impose a mandate on owners and operators of critical infrastructure by requiring those entities to file reports with CISA about cyber incidents and ransom payments. The bill also would require entities filing reports to retain all information related to a reported incident or payment. Because public and private entities own critical infrastructure like utilities and public safety networks, the bill would impose an intergovernmental and private-sector mandate. Several hundred entities would be required to file reports under the bill, but the information for those reports would be readily available and would not be expensive to provide. Consequently, CBO estimates the cost to comply with the mandate would be small and well below the thresholds established in UMRA.

The bill would preempt state, local, and tribal laws by exempting information contained in the reports of cyber incidents and ransom payments from any public disclosure laws. It also would prohibit non-federal regulators from using information obtained solely through those reports to regulate the lawful activities of reporting entities. CBO estimates these provisions would not result in additional spending or a loss of revenue.

Estimate prepared by: Federal costs: Aldo Prosperi; Mandates: Brandon Lever.

Estimate reviewed by: David Newman, Chief, Defense, International Affairs, and Veterans' Affairs Cost Estimates Unit; Kathleen FitzGerald, Chief, Public and Private Mandates Unit; Leo Lex, Deputy Director of Budget Analysis; Theresa Gullo, Director of Budget Analysis.

VII. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 6—DOMESTIC SECURITY

* * * * * * *

CHAPTER 1—HOMELAND SECURITY ORGANIZATION

* * * * * * *

Subchapter XVIII—Cybersecurity and Infrastructure Security Agency

* * * * * * *

PART A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

* * * * * * *

SEC. 651. DEFINITIONS

In this part:

(1) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

([1]*2*) CRITICAL INFRASTRUCTURE INFORMATION

The term "critical infrastructure information" has the meaning given the term in section 671 of this title.

(3) CYBER ATTACK.—The term 'cyber attack' means the use of unauthorized or malicious code on an information system, or the use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system.

([2]*4*) CYBERSECURITY RISK

The term "cybersecurity risk" has the meaning given the term in section 659 of this title.

([3]*5*) CYBERSECURITY THREAT

The term "cybersecurity threat" has the meaning given the term in section 1501(5) of this title.

(6) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

([4]*7*) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES

The term "national cybersecurity asset response activities" means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(8) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

(9) RANSOMWARE ATTACK.—The term 'ransomware attack'—

(A) means a cyber attack that includes the threat of use of unauthorized or malicious code on an information system, or the threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

(B) does not include any such event where the demand for payment is made by a Federal Government entity, good-faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.

(❙5❙*10*) SECTOR RISK MANAGEMENT AGENCY

The term "Sector Risk Management Agency" means a federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

(❙6❙*11*) SHARING

The term "sharing" has the meaning given the term in section 659 of this title.

(13) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber attack that allows an adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (such as information technology products), or services at any point during the life cycle.

(14) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

(15) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

* * * * * * *

SEC. 652A. SECTOR RISK MANAGEMENT AGENCIES

(a) DEFINITIONS

In this section:

(1) * * *

* * * * * * *

❙(7) SECTOR RISK MANAGEMENT AGENCY

The term "sector risk management agency" has the meaning given the term "Sector-Specific Agency" in section 651(5) of this title❙

(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651).

* * * * * * *

SEC. 1500. NATIONAL CYBER DIRECTOR

(a) * * *

* * * * * * *

(c) DUTIES OF THE NATIONAL CYBER DIRECTOR

(1) IN GENERAL

(A) * * *

* * * * * * *

(G) annually report to Congress on cybersecurity threats and issues facing the United States, including any new or emerging technologies that may affect national security, economic prosperity, or enforcing the rule of law; **[**and**]**

(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate federal agencies, to coordinate, deconflict, and harmonize federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and

(**[**H**]***I*) be responsible for such other functions as the President may direct.

(2) * * *

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(H) shall be construed to provide any additional regulatory authority to any federal entity.

* * * * * * *

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SEC 1. SHORT TITLE; TABLE OF CONTENTS

(a) * * *

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

* * * * * * *

TITLE XXII

* * * * * * *

Subtitle C—Cyber Incident Reporting

SEC. 2230. DEFINITIONS.

(a) IN GENERAL.—Except as provided in subsection (b), the definitions under section 2201 shall apply to this subtitle.

(b) ADDITIONAL DEFINITIONS.—In this subtitle:

(1) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

(2) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the interim final rule and final rule issued pursuant to section 2232.

(3) COVERED ENTITY.—The term 'covered entity' means an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the interim final rule and final rule issued pursuant to section 2232.

(4) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2209(a).

(5) CYBER THREAT.—The term 'cyber threat'—

(A) has the meaning given the term 'cybersecurity threat' in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501); and

(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

(6) CYBER THREAT INDICATOR; CYBERSECURITY PURPOSE; DEFENSIVE MEASURE; FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL; SECURITY VULNERABILITY.—The terms 'cyber threat indicator', 'cybersecurity purpose', 'defensive measure', 'Federal entity', 'information system', 'security control', and 'security vulnerability' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(7) SMALL ORGANIZATION.—The term 'small organization'—

(A) means—

(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

(ii) any business, nonprofit organization, or other private sector entity with fewer than 50 employees (determined on a full-time equivalent basis); and

(B) does not include—

(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

(ii) a business, nonprofit organization, or other private sector entity that holds a government contract, unless that contractor 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 regulation.

SEC. 2231. CYBER INCIDENT REVIEW OFFICE.

(a) CYBER INCIDENT REVIEW OFFICE.—There is established in the Agency a Cyber Incident Review Office (in this section referred to as the 'Office') to receive, aggregate, and analyze reports related to covered cyber incidents submitted by covered entities and reports related to ransom payments submitted by entities in furtherance of the activities specified in subsection (b) of this section and sections 2202(e), 2203, and 2209(c) and any other authorized activity of the Director to enhance the situational awareness of cyber threats across critical infrastructure sectors.

(b) ACTIVITIES.—The Office shall, in furtherance of the activities specified in sections 2202(e), 2203, and 2209(c)—

(1) receive, aggregate, analyze, and secure, consistent with the requirements under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls and identify tactics, techniques, and procedures adversaries use to overcome those controls;

(2) receive, aggregate, analyze, and secure reports related to ransom payments to identify tactics, techniques, and procedures, including identifying and tracking ransom payments utilizing virtual currencies, adversaries use to perpetuate ransomware attacks and facilitate ransom payments;

(3) leverage information gathered about cybersecurity incidents to—

(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers; and

(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber attack campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures;

(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of infor-

mation relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a substantial cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

(7) with respect to covered cyber incident reports under subsection (c) involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

(8) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the reports required under subsection (c);

(9) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransom attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

(10) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;

(11) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Office; and

(12) in accordance with section 2235, not later than 24 hours after receiving a covered cyber incident report or ransom payment report, share the reported information with appropriate Sector Risk Management Agencies and other appropriate agencies as determined by the Director of Office Management and Budget, in consultation with the Director and the National Cyber Director.

(c) PERIODIC REPORTING.—Not later than 60 days after the effective date of the interim final rule required under section 2232(b)(1), and on the first day of each month thereafter, the Director, in consultation with the Attorney General and the Director of National Intelligence, shall submit to the National Cyber Director, the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report that characterizes the national cyber threat landscape, including the threat facing federal agencies and covered entities and applicable intelligence and law

enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the report, which shall—

(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

(B) intelligence gaps that have, or currently are, impeding the ability to counter covered cyber incidents and ransomware threats;

(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

(4) be unclassified, but may include a classified annex.

(d) ORGANIZATION.—The Director may organize the Office within the Agency as the Director deems appropriate, including harmonizing the functions of the Office with other authorized activities.

SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

(a) IN GENERAL.—

(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

(2) RANSOM PAYMENT REPORTS.—An entity, including a covered entity and except for an individual a small organization, or a religious institution, that makes a ransom payment as the result of a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

(4) PRESERVATION OF INFORMATION.—Any entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the interim final rule and final rule issued pursuant to subsection (b).

(5) EXCEPTIONS.—

(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the interim final rule and final rule issued pursuant to subsection (b).

(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another federal agency within a substantially similar timeframe.

(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed according to the interim final rule and final rule issued pursuant to subsection (b).

(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the interim final rule and the final rule issued pursuant to subsection (b), except that the requirements of paragraphs (1) through (4) shall not be effective for a period for more than 18 months after the effective date of the interim final rule if the Director has not issued a final rule pursuant to subsection (b)(2).

(b) RULEMAKING.—

(1) INTERIM FINAL RULE.—Not later than 270 days after the date of enactment of this section, and after a 60-day consultative period, followed by a 90-day comment period with appropriate stakeholders, the Director, in consultation with Sector Risk Management Agencies and the heads of other Federal agencies, shall publish in the Federal Register an interim final rule to implement subsection (a).

(2) FINAL RULE.—Not later than 1 year after publication of the interim final rule under paragraph (1), the Director shall publish a final rule to implement subsection (a).

(3) SUBSEQUENT RULEMAKINGS.—Any rule to implement subsection (a) issued after publication of the final rule under paragraph (2), including a rule to amend or revise the final rule issued under paragraph (2), shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

(c) ELEMENTS.—The interim final rule and final rule issued pursuant to subsection (b) shall be composed of the following elements:

(1) A clear description of the types of entities that constitute covered entities, based on—

(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

(A) at a minimum, require the occurrence of—

(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or

network, or a serious impact on the safety and resiliency of operational systems and processes;

(ii) a disruption of business or industrial operations due to a cyber incident; or

(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

(B) consider—

(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

(C) exclude—

(i) any event where the cyber incident is perpetuated by a United States Government entity, good-faith security research, or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as a through a vulnerability disclosure program or the use of authorized penetration testing services; and

(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

(A) A description of the covered cyber incident, including—

(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

(iii) the estimated date range of such incident; and

(iv) the impact to the operations of the covered entity.

(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

(D) Where applicable, identification of the category or categories of information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

(E) The name and, if applicable, taxpayer identification number or other unique identifier of the entity impacted by the covered cyber incident.

(F) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission, and at the direction, of the covered entity to assist with compliance with the requirements of this subtitle.

(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

(A) A description of the ransomware attack, including the estimated date range of the attack.

(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.

(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

(D) The name and, if applicable, taxpayer identification number or other unique identifier of the entity that made the ransom payment.

(E) Contact information, such as telephone number or electronic mail address, that the Office may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.

(F) The date of the ransom payment.

(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

(I) The amount of the ransom payment.

(J) A summary of the due diligence review required under subsection (e).

(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

(A) be established by the Director in consultation with the Council;

(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

(8) Procedures for—

(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), which shall include, at a minimum, a concise, user-friendly web-based form;

(B) the Office to carry out the enforcement provisions of section 2233, including with respect to the issuance of subpoenas and other aspects of noncompliance;

(C) implementing the exceptions provided in subparagraphs (A), (B), and (D) of subsection (a)(5); and

(D) anonymizing and safeguarding information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

(9) A clear description of the types of entities that constitute other private sector entities for purposes of section 2230(b)(7).

(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, to submit the required report under subsection (a).

(2) RANSOM PAYMENT.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding a due diligence review under subsection (e) and reporting ransom payments under this section.

(e) DUE DILIGENCE REVIEW.—Before the date on which a covered entity, or an entity that would be required to submit a ransom payment report under this section if that entity makes a ransom payment, makes a ransom payment relating to a ransomware attack,

the covered entity or entity shall conduct a due diligence review of alternatives to making the ransom payment, including an analysis of whether the covered entity or entity can recover from the ransomware attack through other means.

(f) OUTREACH TO COVERED ENTITIES.—

(1) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

(A) An overview of the interim final rule and final rule issued pursuant to subsection (b).

(B) An overview of mechanisms to submit to the Office covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

(F) An overview of the privacy and civil liberties requirements in this subtitle.

(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

(B) information sharing and analysis organizations;

(C) trade associations;

(D) information sharing and analysis centers;

(E) sector coordinating councils; and

(F) any other entity as determined appropriate by the Director.

(g) EVALUATION OF STANDARDS.—

(1) IN GENERAL.—Before issuing the final rule pursuant to subsection (b)(2), the Director shall review the data collected by the Office, and in consultation with other appropriate entities, assess the effectiveness of the rule with respect to—

(A) the number of reports received;

(B) the utility of the reports received;

(C) the number of supplemental reports required to be submitted; and

(D) any other factor determined appropriate by the Director.

(2) SUBMISSION TO CONGRESS.—The Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives the results of the evaluation described in paragraph (1) and may thereafter, in accordance with the requirements under subsection (b), publish in the Federal Register a final rule implementing this section.

(h) ORGANIZATION OF REPORTS.—Notwithstanding chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), the Director may reorganize and reformat the means by which covered cyber incident reports, ransom payment reports, and any other voluntarily offered information is submitted to the Office.

SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

(a) IN GENERAL.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

(c) APPLICATION OF PROTECTIONS.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

(a) PURPOSE.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

(b) INITIAL REQUEST FOR INFORMATION.—

(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2231(b), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Office within 72 hours in accordance to section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

(2) TREATMENT.—Information provided to the Office in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

(c) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

(2) CIVIL ACTION.—

(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as a contempt of court.

(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity with a Federal Government contract, grant, or cooperative agreement fails to comply with a subpoena issued under this subsection—

(A) the Director may refer the matter to the Administrator of General Services; and

(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

(d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Director determines, based on the information provided in response to the subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide that information to the Attorney General or the appropriate regulator, who may use that information for a regulatory enforcement action or criminal prosecution.

(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Office by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232

any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

(1) the size and complexity of the entity;

(2) the complexity in determining if a covered cyber incident has occurred;

(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments; and

(4) for non-covered entities required to submit a ransom payment report, the ability of the entity to perform a due diligence review pursuant to section 2232(e).

(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

(1) issued an initial request for information pursuant to subsection (b);

(2) issued a subpoena pursuant to subsection (c);

(3) brought a civil action pursuant to subsection (c)(2); or

(4) conducted additional actions pursuant to subsection (d).

SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

(a) DISCLOSURE, RETENTION, AND USE.—

(1) AUTHORIZED ACTIVITIES.—Information provided to the Office or Agency pursuant to section 2232 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(A) a cybersecurity purpose;

(B) the purpose of identifying—

(i) a cyber threat, including the source of the cyber threat; or

(ii) a security vulnerability;

(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a covered cyber incident or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

(2) AGENCY ACTIONS AFTER RECEIPT.—

(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Office shall immediately review the report to determine

whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Office pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

(A) personal information of a specific individual; or

(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

(4) DIGITAL SECURITY.—The Office shall ensure that reports submitted to the Office pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Office in accordance with this subtitle to regulate, including through an enforcement action, the lawful activities of any non-Federal entity.

(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report under section 2232 to the Office shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the 'Freedom of Information Act') and any State, Tribal, or local provision of law requiring disclosure of information or records.

(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision making official.

(e) LIABILITY PROTECTIONS.—

(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rules promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Office.

(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

(f) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.

* * * * * * *

○