Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity: Comparison of Selected Cyber Incident Reporting Bills—In Brief

October 22, 2021

Congressional Research Service
https://crsreports.congress.gov
R46944

CRS REPORT
Prepared for Members and
Committees of Congress

Contents

Tables

Contacts

Introduction

The 117th Congress has debated requirements for nonfederal entities to report to the federal government incidents of cyberattacks. As part of this debate, Members of Congress have introduced legislation seeking to address reporting requirements in different ways. This report compares selected bills addressing cyber incident reporting from the first session of the 117th Congress, specifically:

- H.R. 5440, the Cyber Incident Reporting for Critical Infrastructure Act of 2021 (as introduced);[1]
- S. 2407, the Cyber Incident Notification Act of 2021 (as introduced);
- S. 2875, the Cyber Incident Reporting Act of 2021 (as introduced); and
- S. 2943, the Ransom Disclosure Act (as introduced).
- H.R. 5440 was introduced on September 30, 2021, following a House Committee on Homeland Security (CHS) legislative hearing on a discussion draft of the bill.[2] S. 2407 was introduced on July 21, 2021, and was referred to the Senate Committee on Homeland Security and Governmental Affairs (HSGAC); it has not been debated.[3] S. 2875 was introduced on September 28, 2021, marked up during a HSGAC business meeting, and was ordered to be reported favorably with an amendment in the nature of a substitute on October 6, 2021.[4] All three bills would require the Cybersecurity and Infrastructure Security Agency (CISA) to impose cyber incident reporting requirements upon nonfederal entities via rulemaking. However, the entities affected and what the federal government does with the information received differ slightly among the three bills.
- S. 2943 was introduced on October 6, 2021, and referred to HSGAC. S. 2943 differs more significantly from the other three bills in that its rulemaking authority is limited to enforcement and that it does not apply to cyber incidents broadly—it only addresses the payment of ransoms from ransomware attacks. The National Institute of Standards and Technology (NIST) describes *ransomware* as follows:[5]

  > Ransomware is a type of malware that encrypts an organization's data and demands payment as a condition of restoring access to that data. In some instances, ransomware may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware

[1] This act was engrossed by the House of Representatives on September 23, 2021, as part of its inclusion in the House version of the National Defense Authorization Act for Fiscal Year 2022 (H.R. 4350, Section 1535).

[2] U.S. Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021*, legislative hearing, 117th Cong., 1st sess., September 1, 2021.

[3] As of the publishing of this report.

[4] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Business Meeting*, 117th Cong., 1st sess., October 6, 2021. For analysis, the introduced version of the bill is used in this memorandum as that is the version publicly available on https://www.congress.gov. The Amendment in the Nature of the Substitute addressed definitions of small businesses. The two versions are substantively similar for the purposes of analysis and comparison in the table.

[5] William C. Barker, Karen Scarfone, William Fisher, et al., "Cybersecurity Framework Profile for Ransomware Risk Management," *Draft NISTIR 8374*, September 2021, at https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8374-draft.pdf.

> attacks target the organization's data or critical infrastructure, disrupting or halting operations and posing a dilemma for management: pay the ransom and hope that the attackers keep their word about restoring access and not disclosing data, or do not pay the ransom and restore operations themselves. The methods ransomware uses to gain access to an organization's information and systems are common to cyberattacks more broadly, but they are aimed at forcing a ransom to be paid.

Table 1 provides a side-by-side comparison of these bills, across common traits related to cyber incident reporting.[6]

[6] For further analysis of cyber incident reporting considerations, see CRS Report R46926, *Federal Cybersecurity: Background and Issues for Congress*, by Chris Jaikaran.

Table 1. Comparison of Select Cyber Incident Reporting Bills

Bill Element	Cyber Incident Reporting for Critical Infrastructure Act of 2021 (H.R. 5440)	Cyber Incident Notification Act of 2021 (S. 2407)	Cyber Incident Reporting Act of 2021 (S. 2875)	Ransom Disclosure Act (S. 2943)
Purpose	"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."	"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."	"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."	"To require certain entities to disclose to the Secretary of Homeland Security ransom payments, and for other purposes."
Capability	Program to receive, aggregate, analyze and report on cybersecurity incidents.	Program to receive timely, secure, and confidential notifications on cyber incidents.	Program to receive, aggregate, analyze and report on cybersecurity incidents.	System for DHS to collect and report on ransomware payments.
Due Date to Implement the Act	270 days after enactment.	240 days after enactment.	270 days after enactment.	90 days after enactment.
Reporting Entities	Defined by a rule. At a minimum includes cloud service providers, managed service providers, and critical infrastructure operators. Other entities may report and receive the same liability and disclosure protections described below.	Defined by a rule. At a minimum includes federal agencies, federal contractors, critical infrastructure operators, and cybersecurity companies.	Defined by a rule. Will include critical infrastructure owners and operators. Other entities may be included based on the consequences of the attack and the entity's likelihood of being targeted by malicious actors.	Any entity (public or private) engaged in interstate commerce or that receives federal funds. This includes local governments, but excludes individuals for the purposes of mandatory reporting. Individuals may voluntarily report.
Receiving Entity	CISA	CISA	CISA	DHS
Reporting Threshold	Defined by a rule. Definition of qualifying incidents shall consider the sophistication of the attack, impact to individuals, impacts to industrial control systems or systems related to safety and	Defined by a rule.	Defined by a rule. Definition of qualifying incidents shall consider the sophistication of the attack, the number of individuals affected, and impacts to industrial control systems. At a	The payment of a ransom by a covered entity who experienced a ransomware attack.

Bill Element	Cyber Incident Reporting for Critical Infrastructure Act of 2021 (H.R. 5440)	Cyber Incident Notification Act of 2021 (S. 2407)	Cyber Incident Reporting Act of 2021 (S. 2875)	Ransom Disclosure Act (S. 2943)
	resilience, and operational disruptions.		minimum, will include unauthorized access to systems that leads to a loss of information security, disruptions, and compromises to cloud or managed service providers. Shall not include U.S. government operations, good-faith research, vulnerability disclosure program activities.	
Reporting Timeliness	Defined by a rule. Reporting shall not be earlier than 72 hours after discovery.	Initial report within 24 hours after the confirmation of the incident. Update within 72 hours of new information.	Covered entities must report cyber incidents within 72 hours of discovery. Ransomware payments must be reported within 24 hours of payment.	No later than 48 hours after payment of the ransom.
Report Content	Defined by a rule. At a minimum includes: description of the incident; systems affected, vulnerabilities and TTPs observed; point-of-contact information from the reporter; mitigating actions the reporter has taken.	Expanded in the rule. At a minimum includes: description of the incident; vulnerabilities and TTPs observed; internet traffic information and/or malware samples; point-of-contact information from the reporter; mitigating actions the reporter has taken. Additional content requirements will be described in the rule.	Defined by a rule. Shall include description of the incident; systems affected, vulnerabilities and TTPs observed; identifiers for the entity attacked (e.g., taxpayer identifier); and point-of-contact information from the reporter. For ransom payments, include the amount, payment instructions, and date of payment.	The date and amount of the ransom demanded. The date and amount of the ransom paid. The form of currency used (e.g., cryptocurrency) to make payment. Whether the covered entity received federal funds. Any information on the identity of the attacker.
Report Format	Defined by a rule. Reports may be submitted by a third party (e.g., an information sharing and analysis organization or cybersecurity firm) on behalf of the victim.	Defined by a rule.	Defined by a rule.	Not defined in the bill.
Information Classification	Unclassified.	Classified & unclassified	Unclassified, but may include classified annexes.	Unclassified.

Bill Element	Cyber Incident Reporting for Critical Infrastructure Act of 2021 (H.R. 5440)	Cyber Incident Notification Act of 2021 (S. 2407)	Cyber Incident Reporting Act of 2021 (S. 2875)	Ransom Disclosure Act (S. 2943)
Information Protection	Exemption from federal, state, local, tribal, and territorial disclosure laws. Information shall only be used for: a cybersecurity purpose (as defined in 6 U.S.C. §1501); identifying a threat or vulnerability; responding to or preventing personal harm, injury, or death; investigating threat to minors; and other crimes.	Exemption from federal, state, local, tribal, and territorial disclosure laws. Exemption from civil or criminal action (except for actions brought to enforce the reporting requirement).	Follow protections of personal information in the Cybersecurity Act of 2015 (6 U.S.C. §1504). Further defined by CISA Director.	DHS shall exclude information that identifies covered entities that report.
Information Use	Quarterly, CISA shall provide public reports providing aggregated and anonymized findings and recommendations from the submitted incidents.	Monthly, CISA shall develop a cyber threat intelligence report based on submissions. Annually, CISA shall develop a report on the number of incident notifications received and actions taken.	Quarterly, CISA shall provide public reports providing aggregated and anonymized findings and recommendations from the submitted incidents.	DHS shall annually publish information received from disclosures, including the total dollar amount of ransoms paid.
Information Sharing	CISA shall develop standards to facilitate the timely sharing of information. Information to be shared with federal and nonfederal entities.	CISA shall share with Sector Risk Management Agencies the respective critical infrastructure sector reports.	Agencies that receive notification of a cyberattack shall share that with CISA within 24 hours. CISA shall lead a Cybersecurity Incident Reporting Council with other agencies to deconflict and harmonize reporting requirements. CISA shall share data with Sector Risk Management Agencies. CISA shall determine if further information sharing is necessary upon receipt of reports.	Not defined in the bill.
Liability Protection	Protections are extended from the Cybersecurity Act of 2015 (found in 6 U.S.C. §1505).	Information reported shall not be used for purposes other than stated in the law.	Protections are extended from the Cybersecurity Act of 2015 (found in 6 U.S.C. §1505).	Not defined in the bill.

Bill Element	Cyber Incident Reporting for Critical Infrastructure Act of 2021 (H.R. 5440)	Cyber Incident Notification Act of 2021 (S. 2407)	Cyber Incident Reporting Act of 2021 (S. 2875)	Ransom Disclosure Act (S. 2943)
Rulemaking	DHS shall promulgate rules to implement this act. DHS shall engage in outreach to stakeholders, in addition to rulemaking requirements, to educate potentially covered entities as well as to solicit feedback.	DHS shall promulgate rules to implement this act.	CISA shall promulgate rules to implement this act. DHS shall engage in outreach to stakeholders, in addition to rulemaking requirements, to educate potentially covered entities as well as to solicit feedback.	DHS shall promulgate a rule regarding penalties for covered entities that fail to report.
Enforcement	CISA may issue subpoenas to compel disclosure. If an entity does not comply with the subpoena, CISA may bring a civil action against the entity. Entities lose liability and disclosure protections in this event.	CISA may fine a company for noncompliance up to 0.5% of the company's gross revenue from the prior year for each day of noncompliance. Federal contractors may face further fines.	CISA may issue subpoenas to compel disclosure. If an entity does not comply with the subpoena, CISA may bring a civil action against the entity. Entities lose liability and disclosure protections in this event. CISA may refer federal contractors to GSA for failure to comply with subpoenas for penalties, suspension or debarment. CISA may refer reports to DOJ and regulators for criminal prosecution or regulatory actions.	DHS shall define this in a rule.
Other	CISA shall work with other agencies to harmonize reporting requirements.	Paperwork Reduction Act exemption.	CISA shall develop a ransomware pilot to identify common vulnerabilities and warn potential victims if they are exposed to those vulnerabilities. DHS shall establish a Joint Ransomware Task Force to disrupt criminals and improve defenses.	15 months after enactment DHS shall send to Congress findings related to commonalities of ransomware attacks, the extent to which cryptocurrencies facilitated the attacks, and recommendations to improve cybersecurity.

Source: CRS analysis.

Notes: Cybersecurity and Infrastructure Security Agency (CISA). U.S. Code (U.S.C.). U.S. Department of Homeland Security (DHS). Techniques, Tactics, and Procedures (TTPs). U.S. General Services Administration (GSA). U.S. Department of Justice (DOJ).

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer