Congressional Research Service
Informing the legislative debate since 1914

CIRCIA: Notice of Proposed Rule Making: In Brief

April 11, 2024

Congressional Research Service
https://crsreports.congress.gov
R48025

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48025

April 11, 2024

Chris Jaikaran
Specialist in Cybersecurity Policy

CIRCIA: Notice of Proposed Rule Making: In Brief

The federal government is planning to require certain businesses to report when they are victims of cyberattacks.

In March 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released their Notice of Proposed Rulemaking (NPRM) to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The NPRM is open for public comment until June 3, 2024. The final rule is expected in 2025 and would likely go into effect in 2026.

CISA's proposed rule would require a critical infrastructure company (a covered entity) to report to CISA within 72 hours after that entity experiences a substantial cyber incident (a covered event). Additionally, entities would need to report to CISA within 24 hours when they, or another party on their behalf, make a payment in response to a ransomware attack. The rule applies to critical infrastructure entities (i.e., companies belonging to a critical infrastructure sector). Small businesses (as described by the Small Business Administration) are generally exempt, with exceptions. Covered entities should expect that information they report to the government would be shared among relevant government agencies, and also carry protections against unauthorized disclosures and judicial proceedings.

As CISA furthers implementation of CIRCIA, policymakers may choose to pursue opportunities for oversight or to legislate. Congress may take interest in how the rule is applied to covered entities and covered events, how the federal government would share cyber incident report information among agencies, and the ability of CISA to produce useful intelligence from the reported information.

Since this is a new rulemaking, there are also issues related to the cost to both the government and private sector. CISA estimates the rule would cost around $2.6 billion over 11 years. Cybercrime is estimated to cost the United States over $450 billion in 2024.

Contents

Contacts

Introduction

On March 27, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released the Notice of Proposed Rulemaking (NPRM) for the Cyber Incident Reporting for Critical Infrastructure Act's (CIRCIA) reporting requirements.[1] This NPRM aims to fulfill CISA's requirement under CIRCIA (P.L. 117-103, Division Y) to issue a regulation defining how cyber incident reporting will work.[2] The final rule is expected in late 2025, with it going into effect in 2026.[3] The NPRM is open for public comment until June 3, 2024.

Given the large number of business entities to which the rule may apply, Members of Congress and their staff may hear from constituent and industry groups on its implementation. This CRS In Brief reviews the rule and considerations for policymakers.

Proposed Rule Summary

The proposed rule would require a critical infrastructure entity to report to CISA within 72 hours after that entity is the victim of a substantial cyber incident. Additionally, entities would need to report to CISA within 24 hours when they, or another party on their behalf, make a payment in response to a ransomware attack. Joint reports would be allowed within 72 hours if both an incident and ransom payment occurred.[4]

CISA's proposed rule would apply to entities that are either larger than the Small Business Administration's (SBA) Small Business Size Regulation or meet a sector-specific criterion set forth in the rule.[5] SBA uses a system based on North American Industry Classification System (NAICS) codes to determine small business eligibility by industry. Depending on the industry, a company may be exempt from the reporting requirement if it has fewer than between 100 and1,500 employees or has annual profits of less than between $2.5 million and $47 million.[6]

The regulation CISA proposed would add a new chapter II, consisting of part 226 to Title 6 of the *Code of Federal Regulations.* Chapter II, Part 226, titled *Covered Cyber Incident and Ransom Reporting*, would add 20 new sections to implement CIRCIA.

Reporting

CISA intends to create a website where incident and ransom payment reports may be submitted. Information required for the report would include:

[1] Department of Homeland Security, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting," notice of proposed rulemaking, April 4, 2024, at https://federalregister.gov/d/2024-06526. (The notice was released online prior to its publishing in the *Federal Register*.) Final publication of the NPRM is available at https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

[2] 6 U.S.C. §§681-681g.

[3] Per legislation, the final rule is to be published 18 months after the NPRM, putting release around October 2025. From then, CISA will hold implementation of the rule until sometime in 2026 to allow time for potential Congressional Review Act procedures.

[4] Information in this section summarizes the rule as published in the *Federal Register*, unless otherwise noted.

[5] For more information on small business size standards, see CRS Report R40860, *Small Business Size Standards: A Historical Analysis of Contemporary Issues*, by R. Corinne Blackford and Anthony A. Cilluffo.

[6] 13 C.F.R. §121.201; a table listing industries and their respective small business thresholds is available at https://www.ecfr.gov/current/title-13/section-121.201.

- contact information for the entity (including to which critical infrastructure sector the entity may belong);
- description of the incident (including networks and systems affected);
- technical details of the incident;
- whether or not the affected systems house information supporting the federal government's national security missions;
- a timeline of the incident;
- which (if known) vulnerabilities were exploited;[7]
- a description of security defenses the entity had in place at the time of the incident;
- a description of the techniques, tactics, and procedures (TTPs) used to carry out the attack;
- any known indicators of compromise (e.g., known or suspected malicious internet protocol addresses, emails, or files);
- description and samples of malware used in the attacks;
- any information the entity can provide which may lead to attribution of the adversary (e.g., contact information for a ransomware gang);
- a description of how the entity responded to the attack;
- which (in any) law enforcement agencies the entity has engaged; and
- which (if any) other entities (e.g., a cybersecurity firm) the entity has engaged.[8]

This information is necessary for initial incident and payment reports. Supplemental reports required under the rule are intended to provide substantially new, additional and amplifying information.

Reports of a ransomware attack are similar to reports of a cyber incident, with the addition of:

- the date and amount of a ransom payment;
- ransom payment instructions (e.g., preferred cryptocurrency); and
- whether the payment ended the attack or not.[9]

A third-party entity (e.g., a cybersecurity firm or insurance company) may submit the report on behalf of the affected entity. Third-party reports are allowed for both descriptions of the incident and ransom payments. In such cases, the affected entity is ultimately responsible for the information and compliance with the regulation, and express authority to make third-party reports must be disclosed.

Entities that are not subject to the mandatory reporting requirements may voluntarily report incidents through this system.

[7] Known vulnerabilities are catalogued in the CVE database, available online at https://www.cve.org/.

[8] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23720-23723, April 4, 2024.

[9] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23723-23724, April 4, 2024.

Reporting Thresholds

Entities must report events that are *substantial cyber incidents*. CISA proposes that a substantial cyber incident is one that:

- results in a substantial loss of the confidentiality, integrity, or availability of an entity's IT systems or networks;
- seriously impacts the safety or resiliency of an entity's operational technology (OT) systems or processes;
- disrupts the ability of the entity to conduct its business; or
- exposes the data of an entity held by a third-party (e.g., a cloud service provider) or through a supply-chain compromise.[10]

Actions by government agencies (including U.S. government and law enforcement entities) or approved security researchers (e.g., vulnerability disclosure programs or penetration testing) would not trigger reporting requirements.

Exceptions

An organization may be excused from submitting reports if:

- The entity is required to make a similar report to another federal agency (e.g., a regulator) and an agreement between the agencies is in place;
- The entity is a core internet service provider (i.e., the Internet Corporation for Assigned Names and Numbers [ICANN], the American Registry for Internet Numbers, one of their affiliates, or a root server operator for the domain naming system [DNS]); or
- The entity reported the incident to CISA under a Federal Information Security Modernization Act (FISMA) requirement.[11]

Information Retention

Entities submitting reports are required to preserve data and records related to the incident for no less than two years. Such data includes communications with the attackers, indicators of compromise, technical and forensic data, and logs. Information must be retained in its original form, if possible, and protected against unauthorized access, destruction, or manipulation.[12]

Enforcement

In instances where CISA learns that a critical infrastructure entity experienced a substantial cyber incident (e.g., from a press release or law enforcement agency), but CISA does not have a report from that entity, CIRCIA provides CISA with administrative authorities to compel reporting and tools to require compliance with the regulation.

[10] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23662-23664, April 4, 2024.

[11] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23708-23713, April 4, 2024.

[12] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23730-23733, April 4, 2024.

CISA may start with a request for information from the affected entity. Such a request is not a final government action, so is therefore unable to be appealed. If the entity does not respond or fails to respond adequately, then CISA could issue a subpoena to the entity to compel disclosure.

Information provided via a subpoena is eligible to be shared with the Department of Justice (DOJ) or regulatory agencies to pursue criminal prosecution or regulatory enforcement actions. Entities may appeal subpoenas, but must do so in writing within one week.

If an entity fails to comply with a subpoena, then CISA may refer the case to DOJ to bring a civil enforcement action against the entity. CISA may also refer the case to DOJ, or agencies who have federal contracts with the entity, for potential debarment from procurements.[13]

Protections

Any information shared through a CIRCIA report is not subject to federal or state and local disclosure laws (e.g., the Freedom of Information Act). Entities are required to disclose information in reports that is otherwise subject to certain protections (e.g., financial information or proprietary information).

If an entity submits information through a report, then that information may not be used for a regulatory action. However, a regulator may engage in a regulatory action with the information if it is obtained by alternative means (e.g., media reporting or whistleblower disclosure).

Information in reports shall not be subject to evidentiary or discovery procedures in a trial. Submitted information shall also receive liability protections from civil law suits, if the CIRCIA report is the basis of the suit.

Agencies may use reported information to respond to cybersecurity threats, mitigate a specific harm to a person or the economy, and investigate crimes.

CISA is to develop guidance on protecting the privacy and civil liberties of individuals whose information is included in the reports.[14]

History

As ransomware attacks and data breaches mounted in 2020 and 2021, Congress started to consider legislation to better understand the scope and scale of cybersecurity incidents. In an effort to get a common and more complete understanding of the types, frequency, and effect of cyberattacks against the nation, Congress considered mandated reporting.

During the 117th Congress, policymakers debated precursor legislation to the enacted bill with the Cyber Incident Reporting Act of 2021 (S. 2875) and the Cyber Incident Reporting for Critical Infrastructure Act of 2021 (H.R. 5440). The House Committee on Homeland Security held a hearing on stakeholder perspectives on H.R. 5440, soliciting feedback from the IT, financial services, communications, and energy sectors.[15] The Senate Homeland Security and

[13] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23737-23741, April 4, 2024.

[14] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23723-23724, April 4, 2024.

[15] 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*, 117th Cong., 1st sess., September 1, 2021, Serial No. 117-28 (Washington: GPO, 2021), at https://www.govinfo.gov/content/pkg/CHRG-117hhrg46175/pdf/CHRG-117hhrg46175.pdf.

Governmental Affairs Committee held a hearing to discuss S. 2875 and reported an amended version of the bill favorably to the full chamber.[16]

The 117th Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) as Division Y of the Consolidated Appropriations Act, 2022 (P.L. 117-103).

To develop the NPRM, CISA held 10 in-person, public sessions nationwide and additional sector-specific sessions to hear from industry stakeholders and solicit their input into the proposed rule. Substantive comments received through those sessions are discussed in the NPRM and include concerns about duplicative reporting, system ease of use, and integration of CIRCIA-required reporting with other reporting requirements.

Considerations for Policymakers

How CISA will execute the CIRCIA reporting requirement may be of interest to policymakers. Which entities will be subject to the rule, which federal agencies get and use cyber incident reporting information, how information will be protected, what types of actionable information can come from CIRCIA reports, and the costs associated with implementing the rule are all issues upon which policymakers may choose to conduct oversight or further legislate. Some of these issues are discussed below.

Applicability

Similar to other government regulations on cybersecurity and privacy, the CIRCIA proposed rule would apply a two-part formula for applicability. First, the rule applies only to *covered entities*. Second, covered entities only have to report on *covered events*. If both conditions are met, then the rule takes effect.

During their listening sessions, CISA received many comments on the second aspect of the applicability formula. In response to that feedback, CISA sought to simplify what would be considered a covered event to a single definition of a cyber incident affecting the operations or systems of the company. The threshold for a reportable event is relatively low, increasing the number of reportable incidents in an effort to help the government identify significant attacks and their patterns.

The definition of a covered entity received less stakeholder attention. CIRCIA requires the rule to apply to *critical infrastructure.* The Critical Infrastructures Protection Act of 2001 (P.L. 107-56, §1016, as amended) defines critical infrastructure as

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

That definition is broad, and requires federal agency scrutiny of individual entities to determine if the company or a facility would be considered critical infrastructure.[17]

[16] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Cyber Incident Reporting Act of 2021—Report to Accompany* S. 2875, 117th Cong., 2nd sess., December 13, 2022, S.Rept. 117-249 (Washington: GPO, 2023), at https://www.govinfo.gov/content/pkg/CRPT-117srpt249/pdf/CRPT-117srpt249.pdf.

[17] For more discussion of critical infrastructure policy, see CRS Report R45809, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys.

Under previous policies, being a critical infrastructure entity did not, by itself, create any requirement for the designated entity. The entity may have been subject to other responsibilities by being a regulated facility, but not because of the critical infrastructure designation. Conversely, federal agencies managing a critical infrastructure sector did see an increase in responsibility.

With CIRCIA, that policy shifts. Under the newly proposed rule, a company would now face reporting requirements because of their designation as critical infrastructure.

Of particular congressional concern during debate of cyber incident reporting requirements was to limit burdens on small businesses. CISA addresses this concern by adopting the SBA's criteria for small businesses and exempting them from the reporting requirement. Because different industries inherently require different staffing levels (e.g., nuclear power generation is more labor intensive than geothermal power generation) and bring in different receipts (e.g., dentists offices take in less, on average, than primary care providers), SBA's thresholds are set separately for different sector and subsector activities. Many of the industry firms listed in the SBA's classification system would not meet the base requirement for CIRCIA-required reporting as being part of a critical infrastructure sector.

Certain small businesses may still need to report cyber incidents if they meet sector-specific criteria set forth in the rule. For example, a company that manufactures components for airplanes and employs less than 1,250 people would still be required to report under CIRCIA as a member of the critical manufacturing sector.

The U.S. Census Bureau estimates that there are almost 6.3 million businesses in the United States, with 6.2 million having fewer than 100 employees.[18] CISA estimates that CIRCIA will apply to over 300,000 entities who will submit over 200,000 reports.[19] CISA's estimates imply that there are certain small businesses that will be made to report, but that reporting will not be necessary for the vast majority of U.S. companies. Additionally, state and local governmental entities (e.g., water utilities and schools) would be subject to CIRCIA, adding tens of thousands of additional entities to the estimate.

Federal Information Sharing

CIRCIA applies to federal information sharing in three ways. The first is the harmonization of cyber incident reporting requirements.[20] The second is the sharing of cyber incident reports by CISA among federal agencies. The third is the protection from disclosure for information held by the government.

Per CIRCIA, the Cyber Incident Reporting Council (CIRC) was established, produced a report surveying the existing cyber incident reporting requirements faced by critical infrastructure facilities, and recommended solutions to harmonize those requirements.[21] The CIRC identified over 50 federal cyber incident reporting requirements. These were in addition to various state and

[18] U.S. Census Bureau, "2021 SUSB Annual Data Tables by Establishment Industry," December 2023, at https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html.

[19] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23644-23776, April 4, 2014.

[20] For further discussion of cyber regulatory harmonization, see CRS Insight IN12211, *Harmonic Dissonance—Synching Up Cybersecurity Regulations*, by Chris Jaikaran.

[21] 6 U.S.C. §681f; Department of Homeland Security; *Harmonization of Cyber Incident Reporting to the Federal Government*, September 19, 2023, at https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

territorial data breach notification requirements companies may face.[22] To minimize duplication of efforts, CISA intends to work with federal regulators to enter into agreements regarding cyber incident reporting requirements and post those agreements publicly. If an agreement is in place, the entity may satisfy both its sector and CIRCIA requirements by either reporting to CISA under CIRCIA or to its regulator. It is unclear if CISA will engage state entities to harmonize CIRCIA reporting requirements with state data breach notification laws. CIRCIA does not preempt state data breach notification laws.

It seems unlikely that federal regulators will relinquish their specific reporting requirements in deference to CISA because existing regulations and the proposed CISA rule serve different purposes. For example, CIRCIA is built to help reduce national cyber risk, while the Security and Exchange Commission's (SEC) cyber reporting rule is built to inform investors.[23] In such cases, an agreement between the agencies could lead to a reduced burden on the covered entity if the entity could be made to only report via one channel and all federal entities interested in the event would receive notice of the event.

In cases where an agreement is not in place, agencies are still required to share information about the incident with CISA within 24 hours.[24] In turn, CISA intends to provide federal agencies—including the Federal Bureau of Investigation (FBI)—with information from the reports within 24 hours. CISA is to make information available to relevant agencies, not necessarily all federal agencies.

Entities may also have concerns about the effectiveness of the information protections established in the rule or under CIRCIA, as these procedures are new and have not been tested in judicial proceedings. For example, the Protected Critical Infrastructure Information (PCII) program has existed for two decades and provides similar protections from disclosure laws.[25] But it is unclear how many entities have used the PCII program, or how effective the PCII rule has been in delivering its intended purpose of protecting sensitive information while also facilitating information sharing.[26] Entities may have experience and reservations surrounding PCII and extend those reservations to CIRCIA.

Implementation Costs

Costs to implement CIRCIA-required reporting and report analysis are projected to be borne by both the public and private sectors. CISA projects the total cost to be around $2.6 billion over the 11-year period, 2023 – 2033.[27] CISA estimates that over 300,000 entities will be subject to the rule, submitting over 200,000 reports, and costing them $1.4 billion over that period.[28] These costs include the labor required to review incidents and submit a report, as well as the costs of

[22] National Conference of State Legislatures, "Security Breach Notification Laws," website, January 17, 2022, at https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

[23] Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," 88 *Federal Register* 51896-51945, August 4, 2023, at https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

[24] 6 U.S.C. §681g.

[25] Cybersecurity and Infrastructure Security Agency, "Protected Critical Infrastructure Information (PCII) Program," website, at https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program.

[26] For more information on PCII, see CRS Insight IN11683, *Critical Infrastructure Policy: Information Sharing and Disclosure Requirements After the Colonial Pipeline Attack*, by Brian E. Humphreys.

[27] 2023 is included because it covers the time that CISA worked on developing the rule.

[28] While CISA uses the baseline of an 11-year period in the discussion of costs in the NPRM, entities would bear the preponderance of those costs between 2026 and 2033, when the rule is in effect.

data retention. The federal government is to bear the remaining $1.2 billion over the same period.[29]

CISA expects the program to implement CIRCIA to cost the agency $116 million in FY2025 and require 70 positions.[30] This investment is to facilitate program management, rulemaking support, stakeholder outreach, report analysis, and ransomware mitigation.[31]

In contrast, cybercrime cost the United States an estimated $220 billion in 2022 and $320 billion in 2023. It is projected to cost $452 billion in 2024 before surpassing $1 trillion in 2027.[32]

In the agency's analysis, CISA recognizes a great deal of uncertainty in both their calculation for affected entities and their costs. Previous reporting requirements (e.g., the Health Insurance Portability and Accountability Act [HIPAA] Security Rule) focused on a specific sector (i.e., healthcare) and allowed regulators to tailor both their analysis and the rule. The broad applicability of CIRCIA across sectors and the varying maturity of entities between and among sectors to address cyber risks complicates the government's ability to accurately assess costs.

As comments are submitted on the rule, and before it goes into effect, additional information will likely become available to inform policymakers on the financial burden of the rule and its benefits.

Congress requires the Government Accountability Office (GAO) to evaluate the CIRCIA reporting requirement and issue a report one year after the final rule on the impact of submitted reports on businesses.

Information Analysis and Utility

A key component of CIRCIA is the requirement that CISA use the information it receives through mandated reports to issue intelligence products. The goal of the legislation is to increase awareness of risks and develop mitigation strategies, while also reducing national vulnerability to specific threats by distribution and adoption of CISA analysis.[33]

CISA anticipates that the rule will: (1) allow the agency to detect cyber campaigns sooner; (2) help entities remediate vulnerabilities; (3) increase awareness of threats to improve security by design; (4) help federal agencies counter malicious cyber campaigns; (5) help law enforcement attribute cyberattacks and pursue justice outcomes; and (6) create a common understanding of cyber risks to help public and private sector stakeholders allocate resources. All of these outcomes rely on timely and adequate information distribution.

[29] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23644-23776, April 4, 2014.

[30] Department of Homeland Security, "FY 2025 Budget in Brief," budget document, March 11, 2024, at https://www.dhs.gov/sites/default/files/2024-04/2024_0311_fy_2025_budget_in_brief.pdf.

[31] Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency: Budget Overview," Fiscal Year 2025 Congressional Justification, March 9, 2024, pp. O&S 33-34, at https://www.dhs.gov/sites/default/files/2024-03/2024_0309_cybersecurity_and_infrastructure_security_agency.pdf.

[32] Statista, "Market Insights: Cybersecurity," report, September 2023, at https://www.statista.com/outlook/tmo/cybersecurity/united-states#cybercrime.

[33] For further discussion on the collection of cyberattack reports and analysis of that information for policymakers, see CRS Report R47389, *Cybersecurity: Bureau of Cyber Statistics*, by Chris Jaikaran.

GAO has previous found that information sharing programs were not timely, not tailored to the recipient, and not clear in providing actionable mitigation steps. GAO also found that the government did not adequately track the disposition of information shared to ensure utility.[34]

The specific congressional mandate of this requirement—as opposed to the general information sharing authority CISA has—may help spur industry participation and focus federal resources in identifying, developing, and quickly delivering actionable cyber threat information and defensive measures.[35] Both sufficient resource allocation at CISA, and continuous improvement as the program matures, would likely be necessary to help ensure meeting Congress's intent of reducing nationwide cyber risk.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer

[34] U.S. Government Accountability Office, *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing*, GAO-22-104279, March 1, 2022, at https://www.gao.gov/products/gao-22-104279; U.S. Government Accountability Office, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*, GAO-22-105103, February 9, 2022, at https://www.gao.gov/products/gao-22-105103.

[35] 6 U.S.C. §681e (a)(2).