

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Efforts Underway to Implement Federal Incident Reporting Requirements



Report to Congressional Addressees

July 2024
GAO-24-106917
United States Government Accountability Office

Accessible Version

GAO Highlights

View [GAO-24-106917](#). For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcaim@gao.gov.

Highlights of [GAO-24-106917](#), a report to congressional addressees

July 2024

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Efforts Underway to Implement Federal Incident Reporting Requirements

Why GAO Did This Study

Cybersecurity incidents involving critical infrastructure sectors—the sectors whose assets, systems, and networks provide essential services—cost the United States billions of dollars annually and cause significant disruptions. To provide increased visibility into the growing cyber threats to critical infrastructure, Congress and the President enacted a law on cyber incident reporting. This law calls for DHS to address 13 requirements by March 2024, including publishing a proposed rule for certain entities to submit reports on cyber incidents and ransom payments to DHS.








The law also includes a provision for GAO to report on the implementation of the act. This report (1) examines the extent to which DHS has implemented the act's requirements and (2) describes efforts DHS has made to identify and mitigate challenges with meeting the act's requirements.

To do so, GAO identified 59 requirements in the act that DHS was responsible for implementing. Of those, 13 requirements were due by March 2024. GAO organized the requirements into four categories: proposed rule for reporting requirements, cyber incident reporting council, ransomware pilot program, and joint ransomware task force. GAO then analyzed the department's implementation of the 13 requirements. GAO also summarized documentation and testimonial evidence regarding challenges DHS faced in implementing the act's requirements and its mitigation plans.

What GAO Found

The Department of Homeland Security (DHS) has implemented the 13 requirements from the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the act) that were due by March 2024. Specifically, DHS's Cybersecurity and Infrastructure Security Agency (CISA) submitted a proposed rule related to cyber incident reporting requirements to the Federal Register in March 2024, and it was published in April 2024. DHS plans to issue the final rule by October 2025. In addition, the department implemented the remaining 12 requirements (see figure). As a result of these efforts, DHS should be better positioned to coordinate the federal government cybersecurity and mitigation efforts more effectively, as intended by the act. Additionally, DHS should be better positioned to assist entities with defending against cyber incidents on the critical infrastructure.

Extent to Which the Department of Homeland Security (DHS) Implemented 13 Applicable Cyber Incident Reporting for Critical Infrastructure Act of 2022 Requirements

Proposed Rule for Reporting Requirements	Ransomware Vulnerability Warning Pilot Program	Joint Ransomware Task Force
 <ul style="list-style-type: none"> Issue proposed rule for certain entities to submit cyber incident and ransom payment reports. 	 <ul style="list-style-type: none"> Establish ransomware vulnerability warning pilot program. Submit congressional report on program effectiveness. Ensure most common ransomware vulnerabilities and mitigation techniques are identified. Identify information systems that contain identified security vulnerabilities. Notify entities at risk. Ensure notifications include identified security vulnerability and mitigation techniques. Ensure no pilot program procedures or notifications require entity action because of a security vulnerability. 	 <ul style="list-style-type: none"> Establish and chair a joint ransomware task force. Ensure task force consists of participants from federal agencies, as determined appropriate. Ensure existing authorities of task force members are used to coordinate ransomware activities.
<h3>Cyber Incident Reporting Council</h3>  <ul style="list-style-type: none"> Lead intergovernmental cyber incident reporting council. Submit congressional report on council actions. 		
<p>  Fully implemented  Not implemented  Partially implemented </p>		

Sources: GAO (shield icons), lovemask/stock.adobe.com (all other icons); starlineart/stock.adobe.com (background). | GAO-24-106917

DHS identified a variety of challenges in implementing the act and is taking steps to address them. These challenges are related to harmonizing cyber incident reporting requirements, addressing cyber incident review responsibilities, and facilitating a more efficient method for federal agencies to begin sharing cyber incident reports. DHS noted that it has taken several mitigation steps to address these challenges, such as (1) identifying four recommendations for federal agencies and three proposals to Congress to address duplicative reporting requirements; (2) updating its technologies; and (3) hiring additional staff to facilitate the review, analysis, and sharing of reports. If implemented effectively, the four recommendations and three proposals can further mitigate challenges and help standardize incident reporting.

Contents

GAO Highlights	ii
Why GAO Did This Study	ii
What GAO Found	ii

Letter	1
Background	3
DHS Has Implemented CIRCIA Requirements Due by March 2024	8
DHS Identified Challenges in Implementing CIRCIA and Is Taking Steps to Mitigate Them	16
Concluding Observations	18
Agency Comments	19

Appendix I	Objectives, Scope, and Methodology	20
Appendix II	GAO Contact and Staff Acknowledgments	22

Tables	
Table 1: Overview of Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Key Sections	4
Table 2: Selected GAO Reports Addressing Aspects of Cyber Incidents and Threats on Critical Infrastructure	7
Table 3: Examples of Joint Ransomware Task Force Ransomware Mitigation Activities	14

Figure	
Extent to Which the Department of Homeland Security (DHS) Implemented 13 Applicable Cyber Incident Reporting for Critical Infrastructure Act of 2022 Requirements	iii
Figure 1: Extent to Which the Department of Homeland Security (DHS) Implemented 13 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Requirements	9

Abbreviations

CIRCA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency
DOD	Department of Defense
DHS	Department of Homeland Security
K-12	kindergarten through grade 12
PPD-21	Presidential Policy Directive 21
TSA	Transportation Security Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



July 30, 2024

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark E. Green, M.D.
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Critical infrastructure in the United States includes the assets, systems, and networks in 16 sectors that provide essential services (e.g., banking, communication, health care, and transportation).¹ However, persistent and increasingly pervasive cyber threats to these sectors could have potentially debilitating national security, economic, and public health or safety consequences.

Cybersecurity incidents involving critical infrastructure sectors cost the United States billions of dollars annually and cause significant disruptions.² For example, a February 2024 ransomware³ attack on Change Healthcare resulted in payment delays to pharmacies and hospitals and disruptions to health care nationwide.⁴ In 2023, the Internet Crime Complaint Center received 1,193 complaints from organizations belonging to a critical infrastructure sector that were affected by a ransomware attack. Of the 16 critical infrastructure sectors, the center’s reporting indicated 14 sectors had at least one member that fell to a ransomware attack.⁵ Incidents like these highlight how important it is for affected entities to provide timely reporting so that the impacts can be mitigated.

¹Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

²The White House, Office of the National Cyber Director, *National Cybersecurity Strategy* (March 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

³Ransomware is a form of malicious software designed to encrypt files on a device, rendering any data and systems that rely on them unusable unless ransom payments are made.

⁴HHS, *HHS Statement Regarding the Cyberattack on Change Healthcare*, (Washington, D.C.: March 2024), accessed June 24, 2024, [HHS Statement Regarding the Cyberattack on Change Healthcare | HHS.gov](https://www.hhs.gov/press/20240301-statement-regarding-the-cyberattack-on-change-healthcare).

⁵Federal Bureau of Investigation, Internet Crime Complaint Center, *Internet Crime Report 2023*, (Washington, D.C.: March 2024).

To provide increased visibility into the growing cyber threats to critical infrastructure, Congress and the President enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). This act required the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to take actions, such as developing and implementing reporting requirements for certain cyber incidents and ransomware payments.⁶ According to CISA, access to these reports will allow the agency to rapidly deploy resources, analyze trends, and share information that could prevent or mitigate future cyber incidents.⁷

CIRCIA, enacted in March 2022, includes a provision for GAO to report on the implementation of this act. This review (1) examines the extent to which DHS has implemented CIRCIA requirements and (2) describes efforts DHS has made to identify and mitigate challenges with meeting CIRCIA requirements.

To address our first objective, we reviewed CIRCIA and identified 59 requirements aimed at DHS. Among the 59 DHS requirements, 13 were due by March 2024, including publishing a proposed rule for certain entities to submit reports on cyber incidents and ransom payments to DHS, as applicable.⁸ We focused on these 13 requirements. The time frame for implementing the remaining 46 requirements does not begin until 2025.⁹

Next, we organized the 13 requirements into four categories: proposed rule for reporting requirements, cyber incident reporting council, ransomware pilot program, and joint ransomware task force. To assess the extent to which DHS addressed the requirement to implement the proposed rule, we reviewed the proposed rule and elements that were required to be included in it. For the remaining 12 requirements, we analyzed documentation from the department, including organizational charters, policy memorandums, processes, concept of operations, meeting minutes, and congressional reports. We then determined whether DHS had fully implemented, partially implemented, or not implemented each of the requirements. We supplemented our analysis with interviews with relevant DHS officials to gain additional information regarding steps taken to implement requirements, including any gaps identified in our initial analysis.

To address our second objective, we interviewed and obtained written responses from relevant officials to identify any challenges DHS faces in implementing CIRCIA requirements and any actions the department has planned or taken to mitigate them. Further, we corroborated these responses with documentation, when available. For more details on our objectives, scope, and methodology see appendix I.

We conducted this performance audit from June 2023 to July 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our

⁶The Cyber Incident Reporting for Critical Infrastructure Act of 2022, enacted as division Y of the Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 49, 1038 (Mar. 15, 2022). CIRCIA added Subtitle D, Cyber Incident Reporting, to title XXII of the Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 2240-2246) (codified at 6 U.S.C. §§ 681-681f).

⁷Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet," accessed April 8, 2024, https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf.

⁸As required by CIRCIA, CISA is responsible for determining the types of entities and incidents covered by these reporting requirements as part of its final rule.

⁹One of the 46 requirements was due by March 2023; while CISA met this requirement, CISA stated it could not take specific actions related to that requirement until after its final rule goes into effect and therefore was not included in our analysis.

audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Criminal groups are increasingly targeting U.S. critical infrastructure, which includes systems and assets supporting emergency services, government operations, elections infrastructure, telecommunications networks, and energy production and transmission facilities.¹⁰ Increasing cyber incidents, such as ransomware attacks, highlight the significant cyber threats facing the nation and the range of consequences that these incidents pose. The increased dependence on IT makes the U.S. potentially more vulnerable to cyber incidents.

Cybersecurity Incidents Affecting Critical Infrastructure Are Increasing

Recent cybersecurity incidents highlight the significant cyber threats facing the nation's critical infrastructure and the range of consequences that these incidents pose. For example:

- In February 2024, a ransomware attack against Change Healthcare potentially affected more than 110 million Americans.¹¹ Malicious actors gained access to significant amounts of sensitive personal data within Change Healthcare's information systems, 9 days before the ransomware was deployed. As a result of the attack, a ransom of \$22 million was paid to the malicious actors and there was disruption to Change Healthcare's daily operations, financial strain on providers, and impacted patients. According to a recent update from Change Healthcare, patients whose data was potentially stolen are expected to begin to be notified in late July 2024.
- In May 2021, a ransomware attack was deployed against the Colonial Pipeline Company's business systems. This incident led to the temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast U.S. More than 2.7 million miles of pipelines transport and distribute oil, natural gas, and other hazardous products throughout the United States.
- In December 2020, DHS alerted agencies to a cybersecurity incident which resulted in one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector.¹² Beginning in as early as January 2019, a malicious actor breached the computing networks at SolarWinds—a Texas-based network management software company. SolarWinds estimated that nearly 18,000 of its customers received a compromised software update.

In addition, much of the national's critical infrastructure relies on operational technology—systems that interact with the physical environment—to provide essential services. However, malicious actors and national adversaries pose a significant threat to these systems. For example, according to the 2023 Annual Threat

¹⁰GAO, *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*, [GAO-23-105468](#) (Washington, D.C.: Sept. 26, 2023) and *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure*, [GAO-23-106441](#) (Washington, D.C.: Feb. 7, 2023).

¹¹Ransomware is a form of malicious software designed to encrypt files on a device, rendering any data and systems that rely on them unusable unless ransom payments are made.

¹²GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, [GAO-22-104746](#) (Washington, D.C.: Jan. 13, 2022).

Assessment of the U.S. Intelligence Community, China, Iran, North Korea, and Russia possess the ability to launch cyberattacks that could have disruptive effects on critical infrastructure.¹³ Further, the assessment stated that transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause disruptions of critical services worldwide.

Furthermore, as described above, ransomware is having increasingly devastating impacts on the nation's critical infrastructure. The Department of the Treasury reported that the total value of U.S. ransomware-related incidents reached \$886 million in 2021, a 68 percent increase compared to 2020.¹⁴ In addition, the FBI reported that 870 critical infrastructure organizations were victims of ransomware in 2022, affecting 14 of the 16 critical infrastructure sectors.¹⁵ Among those incidents, almost half were from four sectors—critical manufacturing, energy, healthcare and public health, and transportation systems. However, the full impact of ransomware is likely not known because reporting is generally voluntary.

CIRCSIA Introduced Requirements for Protecting the Nation's Critical Infrastructure

Recognizing the increased threat of cyber incidents, including ransomware, to national security, public safety, and economic prosperity, Congress and the President enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCSIA). Prior to the enactment, there was no single federal statute or regulation addressing cyber incident reporting requirements across the 16 critical infrastructure sectors. The act was intended, in part, to help prioritize efforts to combat cyber threats, including ransomware, by requiring entities to submit cyber incident and ransom payment reports to CISA.¹⁶

The act includes five key sections that contain requirements for addressing cyber incident reporting, federal sharing of incident reports, ransomware activities, and congressional reporting.¹⁷ Table 1 provides an overview of the five key sections.

Table 1: Overview of Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCSIA) Key Sections

Sections	Description
Cyber Incident Reporting	Amends the Homeland Security Act of 2002 to include key definitions, cyber incident reporting and sharing requirements, and requirements for an intergovernmental Cyber Incident Reporting Council, among other things.
Federal Sharing of Incident Reports	Includes requirements for agencies to share incident reports to the Cybersecurity and Infrastructure Security Agency as well as requirements related to harmonizing cyber incident reporting.

¹³Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (February 2023).

¹⁴Treasury, Financial Crimes Enforcement Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021*, Retrieved from <https://www.fincen.gov/resources/financial-trend-analysis>.

¹⁵FBI Internet Crime Compliant Center, *Internet Crime Report 2022*, http://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

¹⁶As previously mentioned, CISA's final rule will determine the types of entities covered by these reporting requirements.

¹⁷There are two other sections that provide supporting information (i.e., the short title and definitions used in the act).

Sections	Description
Ransomware Vulnerability Warning Pilot Program	Includes requirements for the establishment of a ransomware vulnerability warning pilot program.
Ransomware Threat Mitigation Activities	Includes requirements for the establishment of a joint ransomware task force.
Congressional Reporting	Requires various entities to submit congressional reports regarding CIRCIA.

Source: GAO analysis of CIRCIA requirements and amendments. | GAO-24-106917

The five sections of the act include various requirements for DHS (including CISA), other federal agencies, and regulated entities, including owners and operators of critical infrastructure. For example:

- The **cyber incident reporting** section of CIRCIA includes several requirements directed to DHS (including CISA and its national cybersecurity and communications integration center) and critical infrastructure sector entities. For example, CIRCIA directs CISA to issue a rule to implement requirements for how “covered entities” are to submit “covered cyber incident” and ransom payment reports, and the law states that CISA is to establish the definitions and criteria for these key terms in its rule.¹⁸ The final rule must include elements such as clear descriptions for the types of entities that constitute covered entities, the types of substantial cyber incidents that constitute covered cyber incidents, and the content of reports. In addition, CISA must include related procedures for entities, including the manner and form with which entities must submit reports, among others.

The section states that once the rulemaking is finalized, covered entities are required to submit cyber incident reports to CISA no later than 72 hours after the entity reasonably believes an incident has occurred. It also specifies a timeline of 24 hours for covered entities to report a ransom payment.

Further, the section requires CISA to perform several cyber incident review activities intended to combat cyber threats, including ransomware. For example, its national cybersecurity and communications integration center is responsible for receiving, aggregating, analyzing, and securing cyber incident reports from covered entities. This would allow the center to assess the effectiveness of security controls and identify tactics, techniques, and procedures adversaries used to overcome those controls. The center is also tasked with taking actions such as leveraging information gathered about cyber incidents to assist CISA with providing appropriate entities with timely, actionable, and anonymized reports of cyber incident campaigns—including related contextual information, actionable cyber threat indicators, and defensive measures.

In addition, DHS is responsible for leading an intergovernmental Cyber Incident Reporting Council to harmonize (i.e., minimize conflicting or duplicative) federal incident reporting requirements. The department is required to consult with key officials within the Office of Management and Budget, Department of Justice,

¹⁸CIRCIA defines a “covered entity” to mean any entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21 (PPD-21), that satisfies the definition to be established by CISA in the rulemaking. CIRCIA defines a “covered cyber incident” to mean a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by CISA in the rulemaking. See 6 U.S.C. 681(3), (4). Although the National Security Memorandum on Critical Infrastructure Security and Resilience 22 of April 30, 2024, rescinds and replaces PPD-21 of February 12, 2013, there were no updates to the identified critical infrastructure sectors.

the Office of the National Cyber Director, sector risk management agencies, and other appropriate federal agencies to lead the council.¹⁹

- The ***federal sharing of incident reports*** section of CIRCIA includes a requirement for any federal agency that receives a report of a cyber incident to provide the report to CISA within 24 hours of receipt. In addition, CISA and any federal agency that receives an incident report from covered entities are required to, as appropriate, enter into a documented agreement. The agreement is to establish policies, processes, procedures, and mechanisms to ensure these reports are shared with CISA.

CISA is also required to periodically review existing regulatory requirements to report incidents, including the information required in such reports, to ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements. Furthermore, CISA is responsible for coordinating with appropriate federal partners and regulatory authorities that receive reports to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements with such authorities to permit the sharing of incident reports without impacting the ability to gain timely situational awareness of a covered cyber incident or ransom payment.

- The ***ransomware vulnerability warning pilot program*** section of CIRCIA requires CISA to establish a pilot program no later than 1 year after its enactment. This pilot program is required to take actions such as identifying information systems that contain security vulnerabilities associated with common ransomware attacks and notifying at-risk system owners of these vulnerabilities.²⁰
- The ***ransomware threat mitigation activities*** section of CIRCIA requires CISA to establish a task force to coordinate ransomware mitigation activities, such as analyzing ransomware trends to inform federal actions and disrupting ransomware critical actors. The task force is intended to include participants from federal agencies as determined by the National Cyber Director in consultation with DHS.
- The ***congressional reporting*** section of CIRCIA requires DHS, CISA, and GAO to submit reports related to requirements in CIRCIA. For example, DHS is responsible for issuing a report no later than 180 days after the Cyber Incident Reporting Council is convened that includes elements such as identifying a list of duplicative reporting requirements on covered entities and proposing legislative changes necessary to address duplicative reporting. Additionally, CISA is responsible for issuing reports on the effectiveness of the Ransomware Vulnerability Warning Pilot Program and opportunities to strengthen security research within the academic and private sector no later than March 2023.²¹ Lastly, we are responsible for reporting on items such as the implementation of the act no later than 2 years after the enactment of the act.²²

¹⁹The cyber incident reporting section also includes requirements related to (1) third-party report submission, (2) CISA's outreach campaign responsibilities, (3) voluntary reporting of other cyber incidents or additional information, (4) actions CISA may take if the agency has reasons to believe that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment, and (5) information shared with or provided to the federal government.

²⁰According to CIRCIA, throughout the duration of the pilot program, CISA shall ensure, to the extent practicable, that the program prioritizes covered entities for identification and notification activities. The pilot program is to be terminated in March 2026.

²¹The congressional reporting section also requires CISA to report on (1) how the agency engaged stakeholders in the development of the final rule, no later than 30 days after the final rule is issued, and (2) the effectiveness of enforcement mechanisms used in instances of noncompliance with reporting requirements no later than 1 year after the date the final rule is issued.

²²We satisfied this requirement by submitting a congressional briefing on March 15, 2024, and this report as a follow-up on that briefing. Lastly, this section further requires us to report on exemptions to reporting requirements no later than 1 year after the issuance of the final rule.

GAO Has Reported on Cyber Threats to Critical Infrastructure

We have issued a number of reports on various aspects of cyber incidents and threats to critical infrastructure, as well as the need to strengthen the federal role in protecting such infrastructure. In those reports, we have made numerous recommendations aimed at improving agencies' roles in securing the critical infrastructure; however, as of July 2024, all recommendations except for one remain open. Table 2 summarizes key findings from selected reports.

Table 2: Selected GAO Reports Addressing Aspects of Cyber Incidents and Threats on Critical Infrastructure

GAO report	Key finding
<p><i>Cybersecurity: Improvements Needed in Addressing Risks to Operational Technology</i>, GAO-24-106576 (Washington, D.C.: Mar. 7, 2024).</p>	<p>A review of Cybersecurity and Infrastructure Security Agency's (CISA) challenges in delivering operational technology cybersecurity products and services and efforts to collaborate with seven selected agencies to mitigate cyber operational technology risks. The seven agencies were: (1) Department of Defense's (DOD) Defense Cyber Crime Center; (2) DOD's National Security Agency; (3) Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response; (4) Department of Homeland Security's (DHS) Transportation Security Administration (TSA); (5) DHS's U.S. Coast Guard; (6) Department of Transportation's Federal Railroad Administration; and (7) Transportation's Pipeline and Hazardous Materials Safety Administration. We reported that selected nonfederal entities identified challenges related to customer service and workforce planning. Furthermore, four of the selected agencies identified challenges collaborating with CISA. We made four recommendations to CISA to implement processes and guidance to improve its operational technology products and services and collaboration.</p>
<p><i>Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support</i>, GAO-24-106221 (Washington, D.C.: Jan. 30, 2024).</p>	<p>A review of agencies' efforts to enhance the oversight of ransomware practices, assess ransomware risks, and the related federal support. We reported that most of the six selected lead federal agencies (CISA, Energy, Department of Health and Human Services, Transportation, TSA, and U.S. Coast Guard) have assessed or plan to assess risks of cybersecurity threats including ransomware for their respective sectors, as required by law. Further, half of the agencies had evaluated their support of sector efforts to address ransomware. For example, agencies had received and assessed feedback on their ransomware guidance and briefings. However, none had fully assessed the effectiveness of their support to sectors, as recommended by the National Infrastructure Protection Plan. We made a total of 11 recommendations to Energy, Department of Health and Human Services, DHS, and Transportation to determine selected sectors' adoption of cybersecurity practices.</p>
<p><i>Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods</i>, GAO-23-105468 (Washington, D.C.: Sept. 26, 2023).</p>	<p>A review of federal and nonfederal entities' responsibilities for sharing cyber threat information. The 14 federal agencies in the review reported relying on a range of methods to facilitate the sharing of cyber threat information with critical infrastructure owners and operators. Federal agencies relied on 11 methods that fall into two broad categories: cybersecurity and law enforcement services and collaborative sharing environments. Seven federal agencies—CISA, FBI, DOD, Energy, Department of Health and Human Services, TSA, and U.S. Coast Guard—reported using incident reporting services to gather information on cybersecurity incidents that have impacted critical infrastructure owners and operators. CISA and the FBI used separate web-based incident reporting services that allow victims of cyberattacks across all 16 sectors to voluntarily report information on cyber incidents, such as a description of the incident and type of organization impacted. We made two recommendations, one to the Office of the National Cyber Director and one to CISA. Specifically, we recommended that CISA, in coordination with the 14 agencies, should conduct a comprehensive assessment of whether the current mix of centralized and federated sharing methods used by the agencies is the optimal approach to addressing the cyber threat sharing challenges—including whether existing sharing methods should be retired in favor of centralized or federated approaches.</p>

GAO report	Key finding
<i>Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity</i> , GAO-23-105480 (Washington, D.C.: Oct. 24, 2022).	A review of identified areas where the federal government could improve the coordination and assistance it provides to others for addressing ransomware attacks. We reported that federal guidance calls for the development of government coordinating councils to, among other things, enable interagency and intergovernmental coordination to address a specific need for federal assistance, such as cybersecurity at kindergarten through grade 12 (K-12) schools. However, we found that while the Department of Education and CISA offered cybersecurity resources to K-12 schools, they otherwise had little to no interaction with the K-12 community regarding their cybersecurity. We made three recommendations to Education and one to DHS to improve coordination of K-12 schools' cybersecurity and to measure the effectiveness of products and services. The recommendation made to DHS has been implemented.
<i>Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration</i> , GAO-22-104767 (Washington, D.C.: Oct. 4, 2022).	A review of federal efforts to provide ransomware prevention and response assistance to state, local, tribal, and territorial government organizations. We reported that CISA, the FBI, and Secret Service provide assistance in preventing and responding to ransomware attacks on state, local, tribal, and territorial government organizations. We made three recommendations to DHS (for CISA and Secret Service) and the Department of Justice (for FBI) to address identified challenges and incorporate key collaboration practices in delivering services to state, local, tribal, and territorial governments.

Source: GAO. | GAO-24-106917

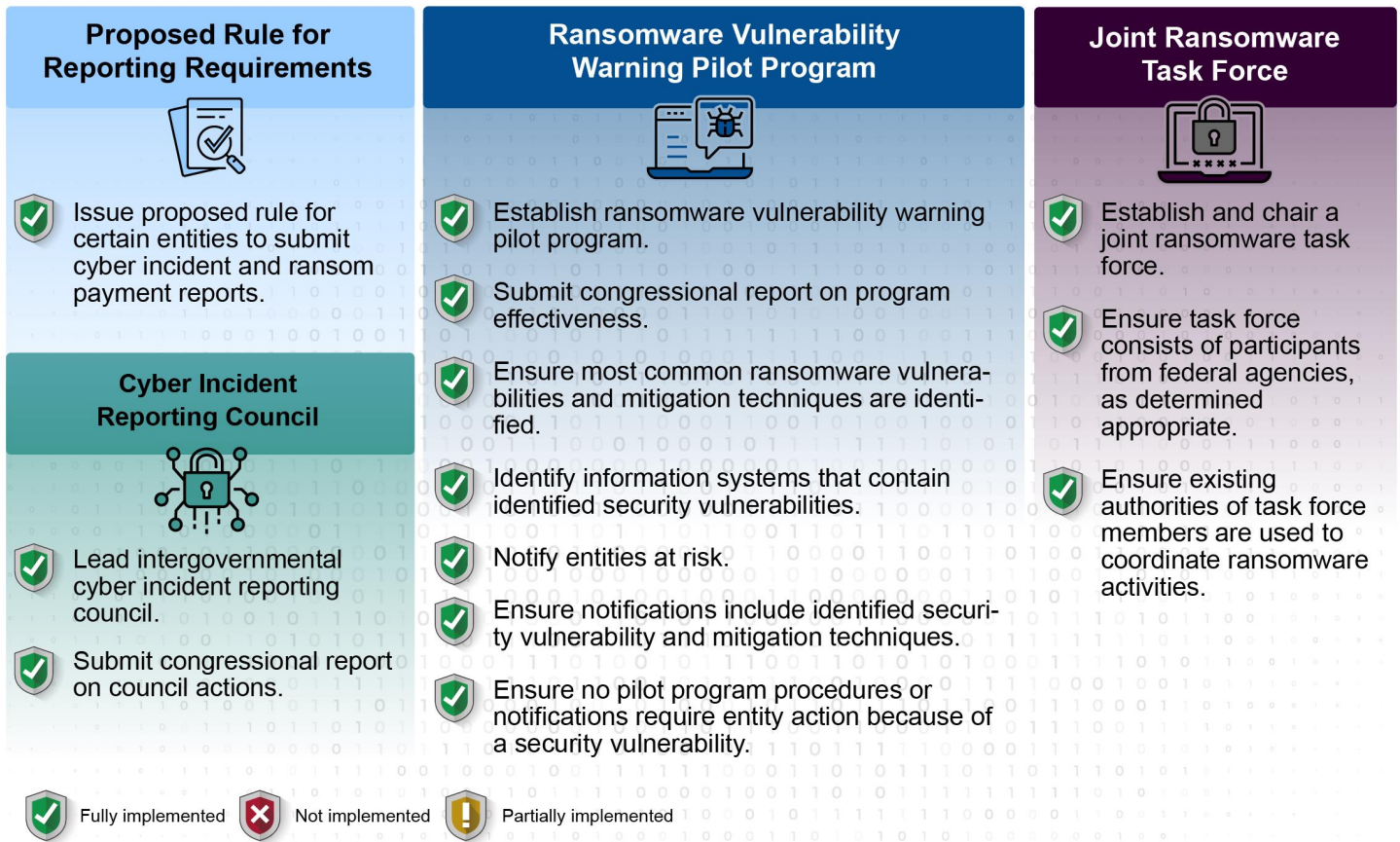
DHS Has Implemented CIRCIA Requirements Due by March 2024

DHS has implemented the 13 requirements due by March 2024. As previously discussed, a significant requirement was for CISA to develop and publish a proposed rule. CIRCIA requires the rule to contain a number of elements, including the following key elements: (1) what entities are required to report, (2) what types of incidents are required to be reported, (3) what information to include, and (4) the process for submitting reports.²³ Additionally, the final rule is required to be published no later than 18 months after publication of the proposed rule.

Further, CIRCIA also contained 12 requirements for DHS that were due by March 2024 pertaining to establishing a council, pilot program, and task force. Specifically, two involve the Cyber Incident Reporting Council, seven involve the Ransomware Vulnerability Warning Pilot Program, and three involve the Joint Ransomware Task Force. Figure 1 describes the requirements and the extent to which DHS has implemented them.

²³CIRCIA is structured so that the exact scope of the reporting is explicitly up to CISA to define through these elements.

Figure 1: Extent to Which the Department of Homeland Security (DHS) Implemented 13 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Requirements



Sources: GAO (shield icons); lovemask/stock.adobe.com (all other icons); starlineart/stock.adobe.com (background). | GAO-24-106917

Proposed Rule for Reporting Requirements

CISA submitted the proposed rule regarding CIRCIA reporting requirements to the Federal Register for publication in March 2024, and it was published in April 2024.²⁴ The proposed rule included the four key required elements that were mandated to be included in the final rule. Specifically, CISA proposed:

- Entities required to report.** A “covered entity” is to include entities within a critical infrastructure sector that either exceed the applicable small business size standards specified by the U.S. Small Business Administration or meets at least one sector-based standard that CISA has proposed.²⁵

²⁴Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644 (proposed Apr. 4, 2024).

²⁵As previously mentioned, the 16 critical infrastructure sectors are defined in federal policy as: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater.

- **Types of incidents to be reported.** “Covered cyber incidents” are generally defined as “substantial cyber incidents” experienced by a covered entity. “Substantial cyber incidents” are defined as cyber incidents that lead to (1) a substantial loss of confidentiality, integrity, or availability of a covered entity’s information system or network; (2) a serious impact on the safety and resiliency of a covered entity’s operational systems and processes; (3) a disruption of a covered entity’s ability to engage in business or industrial operations, or deliver goods or services; or (4) unauthorized access to a covered entity’s information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.
- **Information to be included in reports.** Covered entities are to include information such as a description of the covered cyber incident or ransomware attack, any vulnerabilities exploited, and any mitigation and response activities taken in response to the covered cyber incident or ransomware attack.
- **Process for submitting reports.** Covered entities to submit reports through a web-based form that will be available on the reporting page of CISA’s website.²⁶

The proposed rule was open for public comment until July 3, 2024. According to agency officials, CISA will review all properly submitted comments and respond to them in the preface to the final rule. As required by CIRCIA, CISA plans to issue the rule by October 2025.

Cyber Incident Reporting Council

DHS fully implemented the two requirements related to the council:

- **Lead intergovernmental Cyber Incident Reporting Council.** DHS was required to lead the council to coordinate, deconflict, and harmonize federal cyber incident reporting requirements. This was to be done in consultation with key officials within the Office of Management and Budget, Department of Justice, the Office of the National Cyber Director, sector risk management agencies, and other appropriate federal agencies.

According to the council’s charter, signed in August 2022, the Secretary of DHS designated the Under Secretary for Strategy, Policy, and Plans to lead the council. The council includes membership from over 30 federal departments and agencies, including representation from key officials and sector risk management agencies. Since July 2022, the council has met and taken action to coordinate and deconflict on reporting requirements. For example, the council has reviewed existing and proposed cyber incident reporting requirements and developed recommendations to facilitate harmonization of federal incident reporting requirements. Specifically, the council recommended the federal government take actions such as adopting a model definition of a reportable cyber incident and adopting a model reporting form for cyber incident reports, as appropriate.

- **Submit congressional report on council actions.** DHS was required to submit a congressional report on the harmonization of federal cyber incident reporting requirements no later than 180 days after the council convened. The report was required to include: (1) identification of duplicative federal reporting, (2) challenges in harmonizing duplicative requirements, (3) actions CISA intends to take to harmonize requirements, and (4) proposed legislative changes necessary to address duplicative reporting.

²⁶Covered entities will be required to use the “CIRCIA Incident Reporting Form” on CISA’s website.

The council first convened in July 2022. In addition, although delayed by 8 months in meeting the 180-day requirement, DHS delivered its *Harmonization of Cyber Incident Reporting to the Federal Government* report to Congress on September 19, 2023.²⁷ Agency officials stated the report was submitted late due to unexpected lengthy interagency review and clearance processes. The report included all required elements related to the (1) identification of duplicative federal reporting requirements, (2) challenges in harmonizing identified challenges, (3) actions CISA plans to take to harmonize requirements, and (4) necessary proposed legislative changes to address duplicative reporting. For example, the report identified duplication in federal sector-specific regulatory reporting requirements; cross-sector reporting requirements; voluntary reporting to CISA; and sector risk management agencies, law enforcement, state, foreign, and other nonfederal regulatory requirements. CISA plans to continue participating in the council to help it achieve its harmonization mission. In addition, where feasible, CISA plans to explore opportunities with federal entities to minimize the burden on entities that report substantially similar information as part of an existing reporting requirement.

Ransomware Vulnerability Warning Pilot Program

DHS, through CISA, fully implemented the seven requirements related to the pilot program:

- **Establish ransomware vulnerability warning pilot program.** CIRCIA required CISA to establish a pilot program no later than 1 year after its enactment. This pilot program is required to develop processes and procedures to facilitate the identification and the notification of systems at risk of common ransomware vulnerabilities.

We previously reported that CISA launched its pilot program in January 2023, within the required time frame.²⁸ CISA developed operating procedures that outlined the pilot program's processes and responsibilities. These procedures stated that CISA is to leverage existing activities, including its administrative subpoena, for its vulnerability notification authority. The authority allows CISA to identify and notify owners of devices that contain vulnerabilities associated with ransomware within critical infrastructure sectors.

- **Submit congressional report on program effectiveness.** No later than March 2023 and annually thereafter for the duration of the pilot program, CISA was required to submit a congressional report on the effectiveness of the program which includes elements identifying (1) common ransomware vulnerabilities, (2) the number of notifications issued during the preceding year, and (3) the number of mitigated systems.

We previously stated that CISA delivered its *Ransomware Vulnerability Warning Pilot Program Annual Report* for calendar year 2022.²⁹ It was submitted a month late in April 2023. Similar to the council's report, CISA officials stated it was submitted late due to what officials described as lengthy review and clearance processes. The report included information on the most common vulnerabilities used in ransomware. According to the report, since the program was established in 2023, it does not yet contain specific elements related to the number of notifications issued, the number of vulnerable systems mitigated, or the effectiveness of notifications issued by the program in the previous year. In April 2024, CISA issued its

²⁷Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government* (Sept. 19, 2023).

²⁸GAO, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support*, [GAO-24-106221](#) (Washington, D.C.: Jan. 30, 2024).

²⁹[GAO-24-106221](#) and Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Ransomware Vulnerability Warning Pilot Program Annual Report – Calendar Year 2022 Report to Congress* (Apr. 3, 2023).

second annual report, which included the elements that had not been previously included.³⁰ Specifically, CISA reported it issued 1,754 notifications to 1,248 unique entities in calendar year 2023. According to the report, scanning tools were used to identify vulnerable systems and determine if the entity mitigated the vulnerability after assistance from CISA. For calendar year 2023, CISA reported that 852 vulnerabilities in devices appear to have been mitigated.³¹

- **Ensure most common ransomware vulnerabilities and mitigation techniques are identified.** CISA was required to ensure the pilot program identifies the most common security vulnerabilities exploited in ransomware attacks and mitigation techniques. According to CISA's policy and procedures, various resources are leveraged to identify vulnerabilities known to be exploited by ransomware actors. For example, CISA uses resources such as a public inventory of vulnerabilities known to be exploited by threat actors, a national vulnerability database, and threat information from the agency's own detection capabilities.³² Using its resources, CISA developed and included in its first annual ransomware report a preliminary list of ransomware vulnerabilities that threat actors have previously exploited.³³ Additionally, according to its second annual report, CISA published a list of exploited vulnerabilities known to be used in ransomware campaigns and a list of weaknesses and misconfigurations in vulnerable services on its website.³⁴

Regarding mitigation techniques, the pilot program has developed mitigation guidance related to steps entities can take to mitigate common vulnerabilities and exposures. Additionally, CISA published a guide on its Stop Ransomware website intended to help entities prevent and mitigate ransomware and data extortion incidents. This guide included prevention best practices intended to assist with preparing for, preventing, and mitigating ransomware and data extortion incidents. It also included a checklist for how to respond to these incidents.

- **Identify information systems that contain identified security vulnerabilities.** CISA must ensure the pilot program identifies information systems that contain identified security vulnerabilities.

According to CISA's policy, the agency uses its available resources and capabilities to identify vulnerabilities. These vulnerabilities can be identified through its cyber hygiene vulnerability scanning services, exploited vulnerabilities catalog, open source asset search engines, and commercial tools. After identifying vulnerabilities, CISA actively searches for the presence of these vulnerabilities within critical infrastructure entities. In addition, the agency's ransomware operating procedures described the steps that assigned personnel should follow to identify systems at risk. These steps included using open source tools to gain data used to identify entities and the resource to use when owner entities are unclear prior to using subpoena authorities. Further, CISA's ransomware report stated the agency also assesses identified systems on an ongoing basis to determine the entities' mitigation status.

³⁰Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Ransomware Vulnerability Warning Pilot Program Annual Report – Calendar Year 2023 Report to Congress* (Apr. 25, 2024).

³¹While a device may not reflect a visible vulnerability during scanning, CISA considers the vulnerability to be “apparently mitigated” when the vulnerable devices or specific vulnerability is no longer visible via its scanning tools.

³²According to CISA, beginning in October 2023, in order to directly track common ransomware vulnerabilities, the pilot program added the “known to be used in ransomware campaigns” identifier on the agency's Known Exploited Vulnerabilities catalog. Officials stated there are currently over 200 of these known vulnerabilities used in ransomware campaigns.

³³CISA's Ransomware Report (April 2023).

³⁴CISA's Ransomware Report (April 2024).

- **Notify entities at risk.** CISA is responsible for ensuring entities at risk are notified. Specifically, if CISA can identify the entity at risk that owns or operates a vulnerable information system, it may notify the owner. However, if CISA is not able to identify the owner of the information system, it may use its subpoena authority to identify and notify the entity at risk.

CISA documented a notification process for entities within its ransomware pilot program policy and described the process in its annual ransomware report.³⁵ For example, when CISA can identify the owner of a vulnerable system, it conducts direct notification to the entity pursuant to prioritization guidance provided by the Director of CISA using its regional cybersecurity personnel. The agency uses its existing authority to issue subpoenas to appropriate providers to identify the owner or operator of systems CISA is unable to identify. Once identified, the agency conducts a direct notification to the entity. Officials stated that CISA uses multiple channels, such as email, phone calls, and in-person contacts, to communicate with entities to perform notifications.

According to an agency report that included prevention and detection highlights from October 2022 through September 2023, the pilot program conducted over 1,000 notifications to known entities.³⁶ In February 2024, CISA officials stated they made notifications to entities in 14 of 16 critical infrastructure sectors and in calendar year 2023 the pilot program submitted 1,754 notifications for 1,248 unique entities. For calendar year 2024, from January through April, CISA officials stated the pilot program submitted 589 notifications to 286 unique entities.

CISA plans to further develop its notification activities by taking actions such as building a vulnerability research and prioritization team to effectively prioritize vulnerabilities and allocate actions related to internet-exposed vulnerabilities at risk of exploitation from ransomware. CISA plans to hire staff in fiscal year 2025 to fully establish and implement its vulnerability research and prioritization initiatives.

- **Ensure notifications include identified security vulnerability and mitigation techniques.** If CISA can identify the entity at risk, it must ensure notifications include information on the identified security vulnerability and mitigation techniques.

As previously stated, CISA documented a process for notifying entities at risk. This process required that a notification needs to include information on the identified security vulnerability and mitigation techniques. CISA officials provided an example notification template for notifications issued through its subpoena authority. The template included information such as the potentially vulnerable device, the active internet protocol address, and the suspected vulnerabilities. CISA also provided an example of a standardized mitigation document that included additional details on the identified vulnerability and recommendations, such as applying current vendor-issued relevant updates and available patches as appropriate. Officials stated mitigation documents are provided to all entities at risk, regardless of the method of notification.

- **Ensure no pilot program procedures or notifications require entity action because of a security vulnerability.** CISA must ensure that no procedures or notifications issued by the pilot program shall require an owner or operator of an at-risk system to take action as a result of a notice of a security vulnerability. CISA's ransomware pilot program policy, operating procedures, and entity notifications do not require an owner or operator of a vulnerable information system to take any action as a result of a notice of

³⁵CISA's Ransomware Report (April 2023).

³⁶In addition to the notifications issued through the pilot program, CISA uses threat intelligence through a pre-ransomware notification initiative to send rapid notifications to entities. This is intended to help remove malicious actors from networks before a ransomware attack occurs. According to CISA officials, the initiative will help with the sharing and joint analysis of threat intelligence related to the potential early stages of ransomware activity through collaboration with sector agencies and other partners. CISA officials stated they issued 1,213 pre-ransomware notifications in calendar year 2023.

a security vulnerability. Instead, CISA will encourage notified entities to take appropriate actions to minimize exposure of vulnerable internet-accessible devices.

Joint Ransomware Task Force

DHS, through CISA, fully implemented the three requirements related to the task force:

- **Establish and chair a joint ransomware task force.** No later than 180 days after the enactment of CIRCIA, CISA was required to establish and chair the Joint Ransomware Task Force, in consultation with the Office of the National Cyber Director, the Department of Justice, and the FBI. The task force is required to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation. The task force charter was signed within 180 days of enactment on September 9, 2022. CISA co-chairs the task force with the FBI and consults with the Office of the National Cyber Director and the Department of Justice.

Further, CISA provided documentation of its ongoing nationwide campaign and collaboration efforts against ransomware attacks, which included how it had identified and pursued opportunities with the international community. For example, the documents summarized collaboration efforts between task force members to share information intended to help disrupt ransomware actors. The documents also included efforts to coordinate with international partners within the International Watch and Warning Network.³⁷

- **Ensure task force consists of appropriate participants from federal agencies.** The task force was required to consist of participants from federal agencies, as determined appropriate by the National Cyber Director in consultation with DHS. The task force charter identified membership from over 10 federal agencies whose membership was deemed appropriate by task force authorities. Additionally, CISA identified existing authorities and established two oversight groups within the task force—the Executive Steering Group and Strategic Coordination Group—to facilitate the implementation of its responsibilities.
- **Ensure existing authorities of task force members are used to coordinate ransomware activities.** CIRCIA also required the existing authorities of each task force member be used to coordinate eight ransomware mitigation activities across the federal government. See table 3 for examples of the activities the task force has taken for each assigned responsibility.

Table 3: Examples of Joint Ransomware Task Force Ransomware Mitigation Activities

Mitigation activity	Examples of action taken
1. Analyzing ransomware trends to inform federal actions	The task force leverages its metrics and measurements group to lead efforts to gather data to improve the cybersecurity community's collective understanding of ransomware affecting U.S. organizations and trends, among others. Cybersecurity and Infrastructure Security Agency (CISA) documentation describes lines of efforts conducted by the group, including efforts to update CISA's ransomware dashboard to expand its data sources. The dashboard is shared monthly and includes information on ransomware incidents and trends, the most active ransomware variants, and the most targeted critical infrastructure sectors.

³⁷The International Watch and Warning Network was established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities and to enhance global cyber situational awareness and incident response capabilities.

Mitigation activity	Examples of action taken
2. Identifying highest ransomware threat entities and metrics for success	The task force's metrics and measurements working group identifies the highest ransomware threats by using existing processes led by the FBI, according to CISA officials. For example, the FBI produces publications every 6 months that identify ransomware entities in a prioritized list to enable interagency operations to combat ransomware. Agency officials stated these updates are provided to task force members and the White House. To address the metrics for the success, the group also developed a data metrics proposal that could be used when collaborating with task force stakeholder teams to share ransomware and cyber incident data. The proposal established how the task force plans to coordinate, and it is intended to be a starting point for a universal standard within the task force and its stakeholders.
3. Facilitating collaboration to combat ransomware threats	The task force's external partners group is leveraged to facilitate coordination and collaboration between federal and relevant entities, including the private sector, to improve federal actions against ransomware threats. For example, the group held a meeting in August 2023 that focused on a specific ransomware case, where meeting participants shared technical information about the case with each other and collaborated on various solutions. As of May 2024, officials stated the group has hosted four analytical exchanges of information with private and public partners to allow for open discussion about ransomware threat actors and networks. ^a According to CISA, the group intends to continue to have similar analytical exchanges with other ransomware cases moving forward.
4. Identifying needs and establishing feedback mechanisms	The task force's external partners group is also responsible for advancing efforts to identify stakeholder needs and establish mechanisms for task force input. The group engaged in efforts to identify needs, including briefing and engaging with the International Watch and Warning Network member countries in 2023. CISA officials stated this briefing included member countries from Canada, Denmark, Finland, France, Germany, Japan, the Netherlands, Singapore, Sweden, and the United Kingdom. The briefing was intended to foster collaboration tactics that will aid in the creation of strategies to combat ransomware. Additionally, CISA coordinates with private sector, state, local, tribal, and territorial governments, as well as with international and other stakeholders through its oversight and working groups.
5. Prioritizing intelligence-driven operations	The task force's intelligence integration group is responsible for leading efforts to prioritize intelligence-driven operations to facilitate the disruption of ransomware actors. The group uses the existing intelligence collection capabilities of the task force community—such as FBI authorities—in addition to international partners' capabilities to identify and disrupt specific ransomware actors. The group provides task force members with information regarding top targets, among others, and discusses considerations related to creating various versions of a comprehensive tool to mitigate ransomware and disseminating it to international partners.
6. Disrupting ransomware criminal actors	The task force's investigations and operations group is responsible for using existing authorities to disrupt ransomware criminal actors, associated infrastructure, and their finances through coordinated investigations and operations across the U.S. government. The task force concept of operations describes actions, such as conducting domestic online operations that take down, seize, or otherwise disrupt criminal online infrastructure and resources. According to CISA documentation, between October 2022 and September 2023, existing authorities were used to disrupt ransomware attacks in 21 instances. These disruptions resulted in the arrest of criminal actors, the seizure of associated infrastructure, and the seizure or recovery of millions in dollars and cryptocurrency.
7. Implementing other ransomware threat mitigation activities	The task force's working groups are responsible for coordinating and implementing other ransomware threat mitigation activities. For example, victim services and campaigns groups are responsible for activities such as providing: (1) timely notification to entities targeted by ransomware campaigns, and (2) effective professional guidance to affected entities in ongoing ransomware attacks. Specifically, CISA developed a plan to better position kindergarten through grade 12 schools and hospitals to defend against ransomware attacks and increase the resilience of their information systems. Various actions were documented to meet this goal between July and September 2023, such as prevention and preparedness exercises, notifications, education and awareness classes, trainings, and the issuance of advisories.
8. Identifying successes and failures to improve federal actions	The task force's strategic coordination group is responsible for identifying successes and failures related to ransomware. Specifically, the group reports and reviews progress, shares lessons learned, and provides updates on specific ransomware activities, including the creation of after-action reports on federal actions to mitigate ransomware attacks. For example, agency documentation outlined discussions held related to the creation of an after-action report for a ransomware event affecting the healthcare sector.

Source: GAO analysis of DHS documentation related to CIRCIA requirements. | GAO-24-106917

³In these exchanges, officials stated the FBI highlights several priorities for the targeted ransomware threat and provides an overview of ongoing efforts. In turn, private sector partners share useful information such as the identification of adversary infrastructure, targeting information, tactics, techniques, and procedures pertinent to each targeted ransomware threat.

As a result of taking these steps, DHS and CISA are better positioned to effectively coordinate the federal government's cybersecurity and mitigation efforts.

DHS Identified Challenges in Implementing CIRCIA and Is Taking Steps to Mitigate Them

DHS identified a variety of challenges in implementing CIRCIA and is taking steps to address those challenges. Specifically, DHS, through its Office of Strategy, Policy, and Plans and in collaboration with the Cyber Incident Reporting Council, reported significant challenges associated with harmonizing cyber incident reporting requirements. In addition, DHS, through CISA, also cited challenges related to its cyber incident review responsibilities and the way federal agencies will begin sharing cyber incident reports with the agency.³⁸ DHS has taken action to address these challenges, including making recommendations to the federal government and proposals to Congress, investing in technology, and hiring additional staff.

DHS Identified Challenges in Harmonizing Cyber Reporting Requirements and Issued Recommendations to Address Them

As previously mentioned, DHS, through the Office of Strategy, Policy, and Plans, released a congressional report on the council's efforts to harmonize cyber incident reporting requirements in September 2023.³⁹ The report included an identification of some of the most significant challenges with harmonizing cyber incident reporting requirements. These challenges include, but are not limited to, differences in: (1) definitions of reportable cyber incidents, (2) timelines and triggers for when reports must be made, (3) the contents of cyber incident reports, and (4) how the reports are submitted to federal agencies. Specifically, according to the report:

- **definitions of reportable cyber incidents** are meant to describe the impact of the incident and the qualifying threshold of when the reportable cyber incident must be reported. Cyber incident reporting authorities may use a wide range of terminologies (i.e., "substantial loss," "disruption," and "serious impact") to describe the thresholds for which incidents must be reported. Others may use incidents that are still under internal investigation as a reportable cyber incident.
- **timelines and triggers** define when entities are required to "start the clock" and report on the reportable cyber incident. While some timelines require reporting as early as "immediately," others may not require reporting until the end of a calendar year. Additionally, different reporting timelines are dependent on the purpose of the underlying regulations. The various timelines and triggers could cause unnecessary confusion for a reporting entity in the immediate hours after an incident.

³⁸As previously mentioned, CISA's national cybersecurity and communications integration center is responsible for taking actions such as receiving, aggregating, and analyzing reports from covered entities.

³⁹Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government* (Sept. 19, 2023).

- **contents of cyber incident reports** define what information must be included in the reports. Various reporting authorities include different requirements related to the types of information that must be submitted as part of an incident report. Specifically, required content generally falls into five categories: (1) content related to identifying the reporting entity, (2) content related to the incident impacts, (3) content related to the threat actor, (4) information on how individuals can protect themselves, and (5) response actions taken by or on behalf of the reporting entity.
- multiple agencies currently employ their own reporting methods to **submit reports**, including web portals, file transmission systems, and email reports. As a result, there are wide disparities in terms of reporting mechanisms used by agencies. The diversity in reporting mechanisms could help agencies have several options for reporting in case their system is down. However, this can increase the challenges associated with normalizing and analyzing the data that is reported. Additionally, it may affect harmonizing the reporting process across the federal government.

DHS's review of current federal cyber incident reporting requirements highlighted several opportunities to address these challenges. For example, DHS made four recommendations to the federal government and three proposals to Congress in an effort to mitigate the challenges described above related to some of the most significant challenges with harmonizing cyber incident reporting requirements.⁴⁰ Specifically, DHS recommended that the federal government, wherever practicable:

- adopt a model definition of a reportable cyber incident,
- adopt model cyber incident reporting timelines and triggers,
- adopt a model reporting form for cyber incident reports, and
- assess how best to streamline the receipt and sharing of cyber incident reports and information.

Subsequently, DHS provided suggestions related to these recommendations such as model (1) definitions, (2) reporting timelines and triggers, and (3) reporting form for cyber incident reports that could be used by federal agencies to assist in harmonizing cyber incident reporting.

Furthermore, DHS identified three proposals for Congress to consider for addressing duplicative reporting requirements and further facilitating harmonization of federal cyber incident reporting requirements. Specifically, DHS proposed for Congress to consider:

- removing any legal or statutory barriers to harmonizing identified by the council, including authorizing adoptions of the model definitions of a reportable cyber incident, timeline and trigger provisions, and cyber incident reporting form and/or common data elements for current and future federal cyber incident reporting requirements;
- providing authority and funding, as requested by the Administration, to federal agencies to enable them to collect and share common cyber incident data elements that may not otherwise be authorized; and
- exempting from disclosure under the Freedom of Information Act, or other similar legal mechanisms, cyber incident information reported to the federal government and protect any relevant privileges.

These recommendations and proposals are intended to address various goals such as harmonizing federal cyber incident reporting, reducing the burden on reporting entities, and protecting information submitted to the government. As previously mentioned, CISA issued its proposed rule to implement CIRCIA's cyber incident

⁴⁰In its report, DHS also made recommendations to address challenges not highlighted in this report.

reporting requirements in March 2024. According to the notice of proposed rulemaking, CISA attempted to leverage the model definition and reporting form recommended in the DHS harmonization report, as appropriate. CISA intends to continue to engage federal partners during the development and implementation of the final rule to harmonize reporting requirements and reduce the burden on potential covered entities, where practicable.

DHS Identified Challenges with Other CIRCIA Requirements and Has Taken Steps to Mitigate Them

DHS, through CISA, identified a variety of challenges related to implementing other aspects of the CIRCIA requirements. For example, CISA officials identified challenges in areas related to (1) handling the influx of mandatory and voluntary incident reports it will be receiving and reviewing and (2) facilitating a more efficient method for federal agencies to begin sharing cyber incident reports with CISA. Specifically, CISA anticipates receiving an increased number of mandatory and voluntary reports that the agency will be required to review and act on within a short time frame. CISA officials stated that the agency lacked sufficient technology and staff to effectively handle these cyber incident review requirements.

Additionally, CISA and interagency partners currently share incident reports through manual processes. Based on feedback received from these interagency partners, CISA officials stated that having an automated mechanism for entities to share incident reports with CISA could help reduce burdens for reporting entities. In addition, officials stated automation could enable the agency to receive more reports. As a result, CISA would like to develop a more efficient process and technology which enables agencies to share mandatory and voluntary cyber incident reports, but stated this would be considered a new technology project not accounted for within the agency's budget allocations.

To address these challenges, CISA plans to update and implement new technology solutions and hire additional staff. Specifically, officials stated they are actively working to develop critical technology projects, such as an incident reporting portal to accept cyber incident reports, a unified ticketing system, and other integrated tools. Further, CISA officials stated they prioritized their budget request to successfully obtain funds to begin implementing these initiatives in fiscal year 2023. CISA is using existing funds to prioritize critical technology projects, which might take multiple years to finalize, over hiring all needed staff. CISA officials also stated that the hiring of new staff who would be responsible for the handling of cyber incident reports is planned to occur closer to the date when they might expect to receive those reports (between June and October 2024).

The agency stated it will continue to prioritize project planning related to its technology projects and recruitment activities so that all the necessary technology is fully operational and needed resources are in place by the time the final rule goes into effect. If CISA is able to implement the new technology solutions and hire the additional staff it needs to process the CIRCIA cyber incident reports, it may be able to address the identified challenges.

Concluding Observations

As a result of publishing the proposed rule and implementing all CIRCIA requirements due by March 2024, DHS has better positioned itself to coordinate the federal government's cybersecurity and mitigation efforts

more effectively. Additionally, this may improve its ability to assist entities with defending against cyber incidents affecting the critical infrastructure, as intended by CIRCIA.

If the federal government effectively implements some or all of the recommendations from DHS's report, and Congress considers DHS's proposals, the identified challenges related to duplicative reporting requirements and further facilitating harmonization of federal cyber incident reporting requirements could be minimized. Furthermore, if DHS follows through on its plans to implement new technology solutions and hire additional staff, the likelihood of further mitigating the challenges will increase.

Agency Comments

We provided a draft of this report to the Department of Homeland Security for review and comment. The department provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and to the Secretary of the Department of Homeland Security. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.



Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The objectives of this review were to (1) examine the extent to which the Department of Homeland Security (DHS) has implemented Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCI) requirements and (2) describe efforts DHS has made to identify and mitigate challenges with meeting CIRCI requirements.

To address our first objective, we identified 109 total provisions established by CIRCI. In addition, we reviewed relevant federal law, and government policy, such as the Homeland Security Act of 2002, as amended, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, and the National Security Memorandum on Critical Infrastructure Security and Resilience 22, to identify information related to key terms used within the 109 provisions. We removed 35 provisions that required no action (e.g., definitions used in the act). The remaining 74 provisions required an action from entities. Of these, we counted 59 requirements for which DHS is responsible, but determined that 46 were dependent on a regulation that is not required to be issued until 2025.¹ As a result, our review focused on 13 requirements: one was a requirement to publish a proposed rule for certain entities to submit reports on cyber incidents and ransom payments to DHS, as applicable.²

To identify the extent to which DHS implemented the 13 CIRCI requirements, we first assessed whether DHS published the proposed rule. To do so, we reviewed the rule and elements that were required to be included in it. For the remaining 12 requirements, we collected and analyzed documentation from the department, including organizational charters, policy memoranda, concept of operations, meeting minutes, and congressional reports. We then determined whether DHS had fully implemented, partially implemented, or not implemented each of the requirements.³ We supplemented our analysis with interviews and written responses from relevant DHS officials to gain additional information regarding steps taken to implement requirements, including any gaps identified in our initial analysis.

To address our second objective, we interviewed relevant officials to identify and describe any challenges DHS faced in implementing CIRCI requirements and any actions the department has planned or taken to mitigate them. After compiling a list of potentially common challenges, we gathered written input from DHS officials through a data collection instrument about those challenges and any action plans to mitigate them. We summarized DHS's responses and testimonial evidence, as well as the factors that contributed to the challenges. Further, we corroborated these responses with documentation, when available.

We conducted this performance audit from June 2023 to July 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our

¹Other entities, such as federal agencies and owners and operators of critical infrastructure, are responsible for implementing the remaining 14.

²As previously mentioned, CISA's final rule will determine the types of entities covered by these reporting requirements.

³*Fully implemented* = documentation demonstrated all aspects of the requirement; *partially implemented* = documentation demonstrated some but not all aspects of the requirement; and *not implemented* = did not provide any documentation or if documentation was provided, it did not demonstrate any aspect of the requirement.

audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, (202) 512-5017 or CruzCainM@gao.gov

Staff Acknowledgments

In addition to the contact named above, Rosanna Guerrero (Assistant Director), Shaunyce Thurman (Analyst-in-Charge), Amanda Andrade, Prisca Anyiam, Ben Atwater, Chris Businsky, Lauri Barnes, Kiana Beshir, Ashley Campbell, Corey Evans, Rebecca Eyler, Destin Hinkel, Andrew Stavisky, and Adam Vodraska made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Acting Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548