U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Accessible Version

March 5, 2026

The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Andrew R. Garbarino
Chairman
Committee on Homeland Security
House of Representatives

Cybersecurity Regulations: Additional Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization

Our nation increasingly depends on computer-based information systems and electronic data to execute fundamental operations and to process, maintain, and report crucial information. Further, nearly all federal and nonfederal operations, including the nation's critical infrastructure, are supported by these systems and data. Consequently, the safety of these systems and data is critical to public confidence and the nation's security, economy, and welfare.

GAO has identified cybersecurity as a government-wide high-risk area for more than 25 years. Recognizing a growing threat, we first designated information security as a government-wide high-risk area in 1997. Subsequently, in 2003, we expanded the information security high-risk area to include the cybersecurity of critical infrastructure. We further expanded this high-risk area in 2015 to include protecting the privacy of personally identifiable information. In our most recent update on this high-risk area in February 2025, we reiterated that fully establishing and implementing a national cybersecurity strategy was needed to protect the nation's information systems and infrastructure.[1]

You asked us to convene a series of discussions with industry representatives to gather their perspectives on federal progress in harmonizing cybersecurity regulations, and to provide periodic updates on these discussions. Our first report in this series was issued in July 2025.[2] This is the second such report and summarizes the views shared by selected industry participants in a September 2025 panel. Participants commented on the impact of federal cybersecurity regulations and federal agencies' progress, challenges, and opportunities in harmonizing these regulations.

To gather these perspectives, GAO convened a panel discussion on September 17, 2025. The panel included seven representatives, each from different critical infrastructure sectors:

[1]GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness,* GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

[2]GAO, *Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization,* GAO-25-108436 (Washington, D.C.: July 30, 2025).

communications, energy, financial services, healthcare and public health, information technology, transportation systems, and water and wastewater systems. The representatives included directors of information technology and cybersecurity, chief information officers, general counsel and regulatory affairs specialists. We committed to treat industry participants' comments made during the panel with confidentiality to encourage them to speak candidly, unless they otherwise agreed to attribution in specific cases. The information in this report summarizes the industry participants' perspectives and the points that were raised.[3] The summary of panelists' viewpoints does not necessarily reflect a unanimous opinion of the panel or a collective view of the panelists' respective sectors. See enclosure I for additional information on our objectives, scope, and methodology. For a list of panel participants, see enclosure II.

We conducted our work from August 2025 to March 2026 in accordance with all applicable sections of GAO's Quality Assurance Framework. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

Background

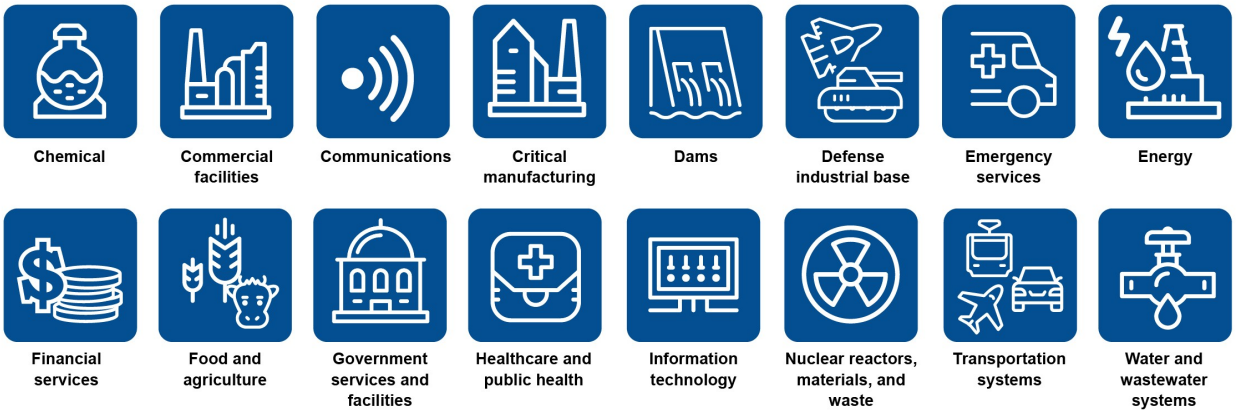
Cyber-based intrusions and attacks on both federal and nonfederal systems by malicious actors are becoming more common and disruptive. These attacks threaten the continuity, confidence, integrity, and accountability of essential systems. Moreover, the risks to these systems—including insider threats from witting or unwitting employees, mounting threats from around the globe, and the rise of new and more destructive attacks—collectively threaten to compromise sensitive data and destabilize critical operations.

Because the private sector owns most of the nation's critical infrastructure (see fig. 1), it is vital that the public and private sectors work together to protect these assets and systems.[4]

[3]For the purposes of quantifying the number of industry participants who made certain statements during the panels, "few" means one to two participants, "several" means three to four, and "most" means five or more participants.

[4]The term "critical infrastructure" refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

Figure 1: The 16 Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-26-108685

Accessible Text for Figure 1: The 16 Critical Infrastructure Sectors

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government services and facilities
- Healthcare and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems

Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). I GAO-26-108685

Toward this end, various federal agencies are responsible for assisting the private sector in protecting critical infrastructure, including enhancing cybersecurity. In doing so, federal agencies have issued a variety of regulations to help protect the nation's critical infrastructure. However, according to the Office of the National Cyber Director, when critical infrastructure sectors are subject to multiple cybersecurity regulations, the result can be conflicting guidance, inconsistencies, and redundancies.

Harmonization refers to the development and adoption of consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations so that these requirements will not overlap, duplicate, or contradict

each other. In June 2024, we testified that consistent cybersecurity regulations could help protect against the increasing risks that threaten our nation's critical infrastructure sectors.[5] At that time, we also discussed the importance of harmonized regulations in avoiding adverse impacts, such as conflicting incident reporting requirements.

We have previously identified concerns around varying federal cybersecurity requirements and the implementation of those requirements. For example, in May 2020, we identified adverse impacts that varying cybersecurity requirements issued by selected federal agencies and related compliance assessments had on state government agencies.[6] We made recommendations to the five agencies to improve coordination with respect to their cybersecurity requirements and assessments of state government agencies. Of the 12 recommendations we made in this area, the agencies have implemented 11 and partially addressed the one remaining.

Further, in July 2024, we reported on the Department of Homeland Security's efforts to implement federal cyber incident reporting requirements and the challenges with harmonizing these requirements.[7] Though we did not have recommendations, we identified challenges including differences in the (1) definitions of reportable cyber incidents, (2) timelines and triggers for when reports must be made, (3) contents of cyber incident reports, and (4) how the reports are submitted to federal agencies.

Several actions have been taken in recent years to improve federal coordination on cyber regulations.

- Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[8] CIRCIA established a Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements.[9]
- The White House established a national cybersecurity strategy in March 2023 and national critical infrastructure policy in April 2024.[10]
- In support of the national cybersecurity strategy, the Office of the National Cyber Director issued a request for information that invited public comments on opportunities for, and obstacles to, harmonizing cybersecurity regulations.[11]

---

[5]GAO, *Efforts Initiated to Harmonize Regulations, but Significant Work Remains,* GAO-24-107602 (Washington, D.C.: June 5, 2024).

[6]GAO, *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*, GAO-20-123 (Washington, D.C.: May 27, 2020).

[7]GAO, *Critical Infrastructure Protection: DHS Has Efforts Underway to Implement Federal Incident Reporting Requirements,* GAO-24-106917 (Washington, D.C.: July 30, 2024).

[8]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).

[9]Pub. L. No. 117-103, div. Y, sec. 103(a), 136 Stat. 49, 1054 (Mar. 15, 2022).

[10]The White House, *National Cybersecurity Strategy*, (Washington, D.C.: March 2023) and *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum-22 (Washington, D.C.: Apr. 30, 2024).

[11]Request for Information on Cyber Regulatory Harmonization, Request for Information: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023).

- In July 2024 and May 2025, proposed legislation known as the Streamlining Federal Cybersecurity Regulations Act was introduced in the Senate, which included requirements aimed at reducing duplicative or contradictory cybersecurity regulations.[12]

Industry Identified Impacts, Progress, Challenges, and Opportunities in Harmonizing Cybersecurity Regulations

Industry panelists identified positive and negative impacts resulting from federal cybersecurity regulations and viewed federal progress in harmonizing them as limited. Panelists also identified several challenges and opportunities related to such harmonization efforts. The views of participants in our September 2025 panel were generally similar to the views of industry participants from our May 2025 panels. Industry participants in our September 2025 panel also offered several additional perspectives and examples regarding impacts, progress, challenges, and opportunities.

Positive and Negative Impacts on Industry

Impacts identified in the panel were mostly negative. However, industry participants identified a few positive impacts of cybersecurity regulations, including helpful federal cybersecurity guidance:

- **Cybersecurity assessments.** One participant stated that the National Credit Union Administration had adopted the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tools, which worked to provide threat assessments and provide a single location to cross-reference multiple cybersecurity frameworks. The participant noted that the tools had since been replaced by the National Credit Union Administration's Automated Cybersecurity Evaluation Toolbox, which helps to provide cybersecurity evaluations.[13]
- **Federal guidance.** According to a few participants, the Cybersecurity and Infrastructure Security Agency's efforts to engage with industry to provide free guidance, cybersecurity tools, and risk assessments have been helpful. For example, one participant stated that the agency promoted simplifying harmonization for different regulations, increasing cybersecurity hygiene, and offering public infrastructure scans to identify vulnerabilities with weekly reporting.[14]

However, as noted above, industry participants identified mostly negative impacts experienced by their industries because of multiple and overlapping cybersecurity regulations and how this has resulted in redundant work and conflicts:

- **Regulation overlap.** According to several participants, sectors are often subject to multiple regulatory frameworks which can result in potentially duplicative and overly burdensome cybersecurity requirements. For example, one participant noted the cybersecurity disclosure rules promulgated by the Securities and Exchange Commission overlap with sector-specific

[12]Streamlining Federal Cybersecurity Regulations Act, S.4630, 118th Cong. (2024) and Streamlining Federal Cybersecurity Regulations Act, S.1875, 119th Cong. (2025).

[13]The Federal Financial Institutions Examination Council developed the Cybersecurity Assessment Tools in June 2015 to provide a voluntary assessment tool to help financial institutions identify cybersecurity risks. The tools were sunset on August 31, 2025. The National Credit Union Administration developed a similar toolkit in October 2021, the Automated Cybersecurity Evaluation Toolbox.

[14]Cyber hygiene is a set of practices for managing the most common and pervasive cybersecurity risks.

standards, such as those from banking regulators.[15] Another participant stated that federal regulations that go beyond their industry's baseline standard are duplicative and do not result in a better outcome.

- **Definitions and requirements within regulations.** Several participants noted that cybersecurity definitions and requirements can be vague or may not account for sector differences. For example, one participant stated that regulations often use similar definitions, but without standardization of terminology, it can be difficult to fully address and understand the requirements of competing standards. A specific example of this was also illustrated in our May 2025 panel when a few participants noted that there is greater use of the term "operational technology." However, when the term is vaguely defined, it is unclear how to account for the different safety and cybersecurity needs of operational technology compared to traditional IT systems.[16] In addition, several participants stated that different frameworks have similar controls and reporting requirements but have small differences that can create unnecessary overlap and confusion. One participant suggested this was because, in their view, regulatory agencies were seemingly developing definitions and requirements without coordinating with other regulators in the same sector.
- **Incident reporting requirements.** Participants felt that incident reporting is often duplicative, and that there are inconsistent incident reporting requirements. A few participants said that there can be differences in the amount of detail, time frames, and thresholds required by agencies for reporting cyber incidents. For example, one participant stated that incident reporting and data collection requirements under CIRCIA would likely be burdensome on top of other existing cyber incident reporting requirements.[17] Specifically, one participant stated that their sector already requires incident reporting within one hour to their regulatory agency and CIRCIA would require additional reporting requirements within 72 hours. Additionally, one participant stated that it can be both difficult and technically burdensome to collect information for multiple entities within a short amount of time to meet reporting requirements.

One Participant's View on the Impact of Overlap, Duplication, or Conflicts in Federal Cybersecurity Regulations

"We want to spend time responding to an incident instead of checking boxes complying with redundant reporting requirements."

Source: Participant in the industry panel on cybersecurity regulation harmonization. | GAO-26-108685

While difficult to estimate the impact of cyber regulations due to sector differences, several participants generally agreed that industry expends significant resources handling overlapping, duplicative, or conflicting federal cybersecurity regulations. Doing so diverts resources away from the critical mission of securing systems and can impact:

[15]The Securities and Exchange Commission has enhanced and standardized disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.

[16]Information technology (IT) refers to the technologies combined for networking, information processing, enterprise data centers, and cloud systems. Operational technology (OT) is the hardware and software that monitors and controls devices, processes, and infrastructure in industrial settings.

[17]CIRCIA requires the Cybersecurity and Infrastructure Security Agency to promulgate regulations to implement the act's reporting provisions. In April 2024, the Cybersecurity and Infrastructure Security Agency published its proposed rule under CIRCIA for public comment. The rule is intended to help prioritize efforts to combat cyber threats and ransomware activities and to enhance capabilities related to federal sharing of incident reporting.

- **Cost.** According to most participants, cost is a significant factor when dealing with cybersecurity regulations and the associated costs make it difficult to meet cybersecurity requirements. This is especially true for small organizations with fewer resources.

One Participant's View on the Impact of Current Federal Cybersecurity Regulations

"Do I focus on compliance, or do I focus on securing my infrastructure?"

Source: Participant in the industry panel on cybersecurity regulation harmonization. | GAO-26-108685

- **Time.** Several participants stated that time spent complying with potentially duplicative requirements and reporting to multiple agencies limits the time they can spend on incident response or strengthening cybersecurity infrastructure. For example, one participant stated that compliance requires cost and resource evaluation of what to address, which can lead to employees focusing less on security improvements.
- **Staff expertise.** Several participants stated that smaller organizations have difficulties meeting cybersecurity requirements due to the lack of resources. For example, several participants stated that small organizations may lack staff with the expertise needed to address reporting requirements.

Industry participants noted that unharmonized federal cybersecurity regulations have different impacts on organizations of varying sizes.

- **Small organizations** are generally required to follow the same regulations as larger organizations but often do not have the compliance staff necessary to do so. They often have fewer, if any, resources dedicated to compliance, which places a greater burden on these companies. Several participants stated that small organizations can sometimes lack the resources or specialized IT personnel needed to fully address federal cybersecurity regulations. For example, one participant stated that cybersecurity is rarely a priority due to a lack of training surrounding federal and state regulations. A few participants stated that diverting resources to focus on compliance can negatively impact organizations by removing resources from securing infrastructure.
- **Large organizations** typically have more resources dedicated to compliance; however, they are often subject to additional foreign regulations depending on their sector and whether they operate internationally. A few participants stated that larger organizations often have to comply with competing regulations and jurisdictions which can lead to increased costs. Participants noted that standardizing foreign and federal requirements and definitions would help to reduce regulatory burdens for businesses that operate internationally.

Federal Agencies Made Progress in Harmonizing Cybersecurity Regulations, but Work Remains

A few participants stated that federal government has demonstrated some interest in working with industry to provide guidance and resources on cybersecurity best practices. Specifically, a few participants agreed that the Cybersecurity and Infrastructure Security Agency had worked with industry to provide free cybersecurity assessments, tools, and guidance. One participant also noted that the agency, along with the Department of Energy's Office for Cybersecurity, Energy Security, and Emergency Response consistently coordinated with them on issues related to their sector, including providing guidance and best practices for supply chain security. Additionally, several participants agreed that the National Institute of Standards and Technology's Cybersecurity Framework has provided their industries with cybersecurity best practices and baseline security measures. However, several participants agreed that the federal government has made limited progress toward harmonizing cybersecurity regulations.

Federal Agencies Continue to Face Challenges to Harmonizing Cybersecurity Regulations

Industry participants identified a few challenges, including the following barriers, federal agencies face when harmonizing cybersecurity regulations:

- **Lack of standard definitions and information requirements.** Several participants felt that agencies at times develop unique cybersecurity definitions that differ from industry, resulting in inconsistent terminologies that cannot be widely applied and reused. Federal, state, and industry-specific standards may contain unique or special information, but a few participants stated this leads to unnecessary redundancies, and universal definitions would be helpful.

One Participant's View on the Challenges with Federal Cybersecurity Regulations

"When it comes to standards and definitions, you have a lot of different regulations [with] state and federal…and they're all basically saying the same thing. It's challenging to get through all the wordsmithing…some kind of standardization…across all the different [regulations] would be helpful."

Source: Participant in the industry panel on cybersecurity regulation harmonization. | GAO-26-108685

- **Agency reporting requirements compete with industry priorities.** Agencies want timely reporting about cyber incidents, but participants felt that these requirements often interfere with industry's priority to mitigate and resolve threats. Several participants said that their industries prioritize resolving cybersecurity risks over compliance. Further, several participants stated that meeting reporting requirements often take away from time and effort applied to securing cybersecurity infrastructure.

Industry Identified Additional Opportunities for Harmonizing Federal Cybersecurity Regulations

Industry participants identified near- and long-term opportunities for harmonizing federal cybersecurity regulations.

- **Harmonize incident reporting.** A few participants said that CIRCIA has potential to achieve harmonization among various regulations. For example, a few participants stated that such harmonization should include properly scoping reporting requirements with a clear understanding of the cybersecurity risk being mitigated.
- **Renew and revise legislation.** Several participants stated that the reauthorization of the Cybersecurity Information Sharing Act of 2015 was important to maintain industry protections for information sharing. One participant stated that that this legislation should be regularly updated to account for new or emerging technologies. A participant also stated that opportunities may exist to remove outdated requirements, such as those under the Health Insurance Portability and Accountability Act, to further harmonize future sets of requirements.
- **Consider establishing a working group of federal agencies to harmonize cybersecurity regulations.** One participant noted that additional progress in harmonizing federal regulations depends on agencies working together, such as through a working group or similar mechanism, to address differences between terminology, reporting requirements, and information sharing agreements. Additionally, one participant stated that establishing a single entity with authority over regulatory consistency could be beneficial for purposes of cybersecurity regulatory harmonization. However, several other participants stated that such an entity could be problematic for industry by offering a one-size-fits-all approach and a lack of specialization for each sector in regard to regulation.

- **Deconflict regulations.** Several participants noted that the Office of the National Cyber Director has the opportunity to work with other federal cybersecurity agencies to deconflict cybersecurity regulations. Specifically, these participants stated that it would be beneficial to industry to give the Office of the National Cyber Director a clear mandate to address differences within federal agency terminology, reporting regimes, and guidance to work toward harmonizing federal regulations.

One Participant's View on Opportunities to Harmonize Cybersecurity Regulations

"Giving the Office of the National Cyber Director a clear mandate and authority to manage independent regulatory agencies and others to harmonize reporting regimes would be a really big step forward [toward harmonization]."

Source: Participant in the industry panel on cybersecurity regulation harmonization. | GAO-26-108685

- **Establish metrics for regulatory effectiveness.** Several participants noted that metrics for how agencies assess the effectiveness of cybersecurity-related regulation could be helpful. One participant stated that evaluating the economic benefit of metrics measured against reporting timetables could help industry better understand the potential benefits of regulation. For example, one participant stated that it could be helpful to evaluate regulations based on their benefit to industry—specifically, whether there is economic benefit to reporting in 48 hours versus 72 hours.
- **Consolidate reporting.** A few participants stated that it would be helpful to centralize reporting through a single reporting mechanism managed by one functional regulator for each sector for ease of access, familiarity, and standardized industry requirements. This would reduce the need to complete multiple reports to different federal agencies.
- **Standardize terminology.** One participant stated that if the same terminology is used across different frameworks, then the definitions should be standardized. Another participant also noted that the rules under the Health Insurance Portability and Accountability Act may define reporting time frames of days while another regulation may use hours. Another participant also noted that aligning U.S.-based cybersecurity terminology with foreign definitions may be helpful in a regulatory context.
- **Make shared information confidential.** A few participants stated it would be important that cybersecurity incident information used by agencies will not be used to penalize or negatively impact entities who submit the information. One participant stated that without guarantees that the information is confidential, Freedom of Information Act exempt, and not to be used for enforcement action or retaliation, then it would be difficult to have conversations surrounding cybersecurity.[18] Additionally, a few participants stated that it would be important to separate the entities responsible for enforcement from those who are responsible for securing cybersecurity systems, otherwise industry may fear retaliation.

Third Party Comments

We provided a copy of this report to the seven panel participants for review and comment. Five of the participants provided comments via email, stating that they agreed with our characterization of their views in the report. The other two participants did not provide comments on the report.

[18]5 U.S.C. § 552. The Freedom of Information Act (FOIA) requires federal agencies to provide the public with access to certain government records with certain specified exemptions.

We are sending copies of this report to the appropriate congressional committees and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at HinchmanD@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. In addition, Joshua Leiling (Assistant Director), David Hong (Analyst in Charge), Amanda Andrade, Timothy Barry, Madison Brown, Brandon Cox, Jonnie Genova, Evan Nelson Senie, Sarah Ong, and Walter Vance made key contributions to this report.

//SIGNED//

David Hinchman
Director, Information Technology and Cybersecurity

Enclosures

Enclosure I: Objective, Scope, and Methodology

Our objective for this report was to summarize industry views on the impact of federal cybersecurity regulations and federal agencies' progress, challenges, and opportunities in harmonizing them. This is the second report in a series on this topic and summarizes the views shared by selected industry participants in a September 2025 panel. Our first report in this series was issued in July 2025.[19]

To conduct our work, we identified industry representatives based on public comments their organizations submitted to Regulations.gov during comment periods for the Cyber Incident Reporting for Critical Infrastructure Act reporting requirements posted by the Cybersecurity and Infrastructure Security Agency[20] and the Request for Information: Cyber Regulatory Harmonization posted by the Office of the National Cyber Director.[21] We then grouped the industry organizations and their representatives into different critical infrastructure sectors.

We removed comments that were not affiliated with an industry organization in one of the 16 critical infrastructure sectors as well as comments from the government services and facilities sector because our objective was focused on establishing an industry perspective. We screened comments to ensure they were from a relevant organization and that they contained substantive comments. This screening process led us to remove three other sectors because no substantive comments were found for the dams, commercial facilities, and emergency services sectors. These steps reduced the number of critical infrastructure sectors in our sample of comments from 16 to 12. We also removed comments provided by panelists who contributed to our July 2025 report.[22] This further reduced the number of critical infrastructure sectors in our sample from 12 to nine because there were no remaining comments from organizations affiliated with the defense industrial base, nuclear, and food and agriculture sectors.[23]

We then used a randomized, ordered list of the comments to select participants from organizations that provided comments and were associated with the nine remaining critical infrastructure sectors. In doing so, we contacted potential panelists via email. When potential panelists did not respond by the requested deadline or were not available, we continued our outreach to the next potential panelist in the randomized order list of comments. We repeated this process until we identified a stakeholder from each sector. While we contacted industry representatives in each of the nine sectors, only seven were available to participate in the panel. The seven sectors with an industry representative available to participate in the panel were communications, energy, financial services, healthcare and public health, information technology, transportation, and water and wastewater systems.

We then convened one 3-hour panel on September 17, 2025, with seven panelists representing industry organizations affiliated with the seven different sectors. We obtained a range of perspectives on the current state of federal cybersecurity regulations and how they impact

[19]GAO-25-108436.

[20]Notice of Proposed Rulemaking, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644 (Apr. 4, 2024).

[21]Request for Information on Cyber Regulatory Harmonization, Request for Information: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023).

[22]GAO-25-108436.

[23]The nine remaining sectors selected to participate in the panel include chemical, communications, critical manufacturing, energy, financial services, healthcare and public health, information technology, transportation, and water and wastewater systems.

different critical infrastructure sectors, the progress and challenges industry participants have seen from recent harmonization efforts, and opportunities they believe will come from continuing efforts. We reviewed the discussion of the panel and identified overlapping points and overarching themes for each topic. For the purposes of quantifying the number of industry participants who made certain statements during the panels, “few” means one to two participants, “several” means three to four, and "most" means five or more participants.

The information in this report summarizes the industry participants’ perspectives and the points that were raised. The summary of panelists’ viewpoints does not necessarily reflect a unanimous opinion of the panel or a collective view of the panelists’ respective sectors. We offered each participant the chance to present alternative views. We also committed to handle with confidentiality industry participants’ comments made during the panel discussion to encourage them to speak candidly, unless they otherwise agreed to attribution in specific cases. In addition to the panel, we also reviewed related GAO and federal agency reports related to cybersecurity harmonization.

We conducted our work from August 2025 to March 2026 in accordance with all applicable sections of GAO’s Quality Assurance Framework. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

Enclosure II: Panel Participation

We convened a 3-hour panel of industry participants from multiple critical infrastructure sectors, selected randomly from public comments on a proposed rule for CIRCIA implementation and a request for information from the Office of the National Cyber Director on views regarding cyber regulatory harmonization. The panel was held virtually on September 17, 2025. The seven industry participants who attended the panel and represented different critical infrastructure sectors are listed below.

- **Tara Hairston** Alliance for Automotive Innovation (transportation systems)
- **Stephanie Kiel** Google LLC (information technology)
- **Andrew Morris** America's Credit Unions (financial services)
- **Loretta Polk** NCTA - The Internet & Television Association (communications)
- **Dave Roberts** AlexRenew (water and wastewater systems)
- **Dr. Steven Waldren** American Academy of Family Physicians (healthcare and public health)
- **Bill Zuretti** Electric Power Supply Association (energy)