U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

July 30, 2025

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

Cybersecurity Regulations: 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]

We have also issued numerous reports that identified concerns around varying federal cybersecurity requirements, often rooted in regulation, and the implementation of those requirements. For example, in May 2020 we identified adverse impacts that varying cybersecurity requirements issued by four selected federal agencies had on state government agencies.[2] Further, in July 2024, we reported on the Department of Homeland Security's efforts to implement federal cyber incident reporting requirements and challenges with harmonizing these requirements.[3] Those challenges included 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.

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. This is the first such report and summarizes the views

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

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

shared by selected industry participants in May 2025 on the impact of federal cybersecurity regulations and federal agencies' progress, challenges, and opportunities in harmonizing these regulations in accordance with national cybersecurity policy and strategy.

To gather these perspectives, GAO convened two panel discussions on May 28 and May 29, 2025. Each panel included six representatives from industry organizations for a total of 12 representatives across the two panels. The representatives included directors of cybersecurity-related functions; chief executive officers; regulatory affairs specialists; and those in similar roles across multiple critical infrastructure sectors. We committed to treat industry participants' comments made during the panels 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.[4] The summary of panelists' viewpoints does not necessarily reflect a unanimous opinion of the panels 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 April 2025 to July 2025 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 more 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, it is vital that the public and private sectors work together to protect these assets and systems.[5] 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, this can result in conflicting guidance, inconsistencies, and redundancies.

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

[5]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.

Harmonization refers to the development and adoption of more consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations so that these guidelines 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.[6] At that time, we also discussed the importance of harmonized regulations in avoiding adverse impacts, such as conflicting incident reporting requirements.

There are several actions that 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).[7]
- The White House established a national cybersecurity strategy in March 2023 and national critical infrastructure policy in April 2024.[8]
- In support of the national cybersecurity strategy, the Office of the National Cyber Director (ONCD) issued a request for information that invited public comments on opportunities for, and obstacles to, harmonizing cybersecurity regulations.[9]
- In July 2024 and May 2025, proposed legislation known as the Streamlining Federal Cybersecurity Regulations Act was introduced in the Senate, which included goals for reducing duplicative or contradictory cybersecurity regulations.[10]

Industry Identified the Varying Impacts, Progress, Challenges, and Opportunities of Harmonizing Cybersecurity Regulations

Multiple and Varying Cybersecurity Regulations Have Had Negative Impacts on Industry

While the impacts identified were mostly negative, industry participants did identify several positive impacts of cybersecurity regulations:

- **Driving behavioral changes.** A few participants stated that before federal cybersecurity regulations were implemented, it was difficult for industry to get executives to invest in their organization's cybersecurity infrastructure.

---

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

[7]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).

[8]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).

[9]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).

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

- **Cross-sector interaction.** According to a few participants, industry has become more aware of best practices and the importance of having cybersecurity protections due to the information sharing across sectors regarding cybersecurity regulations. Additionally, participants noted that CISA's efforts to collaborate and build trust through the Cybersecurity Information Sharing Act of 2015 have been successful.[11]
- **More secure cyber landscape.** A few participants believed that implementing all-inclusive cybersecurity regulations increases industry's ability to work toward having more comprehensive cybersecurity.

However, industry participants identified negative impacts that their industries experience with multiple and varying cybersecurity regulations and how this can result in overlap, duplication, and conflicts:

- **Number of regulations.** According to several participants, the number of cybersecurity regulations varies among sectors—one participant cited as many as 13 regulations while another cited a single regulation. Several agencies regulating a sector's cybersecurity could result in overlap and potentially duplicative cybersecurity requirements.
- **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, certain participants reported greater use of operational technology, which has different safety and cybersecurity needs compared to traditional IT systems.[12] Inflexible cybersecurity requirements may not be applicable for certain sectors, and agencies may present conflicting views regarding what is required and not required for specific industries. Federal requirements may also conflict with foreign requirements, such as the General Data Protection Regulation, which may cause conflict for organizations that operate in covered countries.[13]
- **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. Participants felt that incident reporting is often duplicative, and that there are inconsistent incident reporting requirements. For example, a few participants pointed to different regulations promulgated by the Securities and Exchange Commission[14] associated with incident disclosures and the Department of Health and Human Services regarding

[11]Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2242, 2936-56 (2015) (codified at 6 U.S.C. §§ 1501-10).

[12]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.

[13]The European Union's General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, applies to private and public companies that control or process data or offer services to European Union citizens. GDPR can apply to entities in the United States that process data or engage in business in the European Union.

[14]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.

breaches of health data.[15] Participants also believed that requirements in federal acquisition regulations created additional duplication, including different versions of incident reporting requirements for defense contracts. They were also concerned about additional proposed CIRCIA requirements that are planned to take effect in calendar year 2026.[16]

- **Audits and assessments.** According to a few participants, regulatory compliance audits and assessments can vary from no assessment required to self-attestations or independent reviews by the regulatory agency or a third-party. One participant stated that an organization in their sector could have up to seven different auditors request the same information. Having multiple agencies assessing an organization could indicate overlap and duplicative requests for information.

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

"[The impact of federal cybersecurity regulations is] additional spending, additional resources, additional time, and making sure that we are appropriately responding and reporting when necessary."

Source: Participant in the industry panels on cybersecurity regulation harmonization. | GAO-25-108436

While difficult to estimate the impact of cyber regulations due to variances among sector entities, 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:

- **Spending.** According to a few participants, organizations are spending, in some cases, tens of millions of dollars on efforts to comply with cybersecurity regulations, creating a large financial burden for industry stakeholders. Hiring third-party entities and paying compliance staff to adhere to multiple or overlapping regulations is using financial resources and impacting internal budgets.

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

"We are spending money on compliance that would better be spent on cybersecurity."

Source: Participant in the industry panels on cybersecurity regulation harmonization. | GAO-25-108436

- **Time.** A few participants stated that significant time is used by staff to identify duplicative regulations, confirm the definitions and language used, fill out different reporting requirements, and meet different deadline thresholds. A few participants noted that upwards of 50 percent of their staff's time is spent on cybersecurity regulatory compliance. Senior

[15]The Department of Health and Human Services is responsible for overseeing and enforcing the Health Insurance Portability and Accountability Act (HIPAA) which includes rules related to a breach of protected health information. Specifically, the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

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

leadership and employees in crucial positions are splitting their time between resolving a cyber incident and completing the requirements of reporting a cyber incident.

- **Staff expertise.** A few participants discussed that internal staff hired for their cybersecurity expertise are often reassigned from their duties of identifying and mitigating threats to complete compliance tasks.

Industry participants noted that unharmonized federal cybersecurity regulations impact organizations of varying sizes differently.

- **Small organizations** generally are required to follow the same regulations as larger organizations but often do not have the compliance staff necessary to do so. They generally have fewer, if any, resources dedicated to compliance, which places a larger burden on these companies. Participants noted that smaller organizations also may not be fully aware of cybersecurity regulations they are subject to, due to a lack of expertise in identifying and understanding regulations, as well as lacking a sufficient budget available to fully fund such efforts. Several participants said that diverting resources (such as money and staff) from security to compliance can negatively impact their organization's bottom line and thus adversely impact their ability to be competitive in their market.
- **Large organizations** typically have more resources to dedicate to compliance, yet they may also be subject to additional regulations depending on their sector and if they operate internationally.

Federal Agencies Have Made Limited Progress in Harmonizing Cybersecurity Regulations

A few industry participants stated that over the past decade, cyber risk has significantly evolved, and federal cybersecurity regulations have aimed to better protect against increasing risk. However, the federal government has made limited progress to harmonize various cybersecurity regulations.

One Participant's View on the Progress of Federal Cybersecurity Regulation Harmonization

"We are no closer today than we were 10 years ago on creating a solution for harmonization."

Source: Participant in the industry panels on cybersecurity regulation harmonization. | GAO-25-108436

A few participants agreed that one aspect of progress in aligning federal cybersecurity regulations is that regulations are written with more consistent terminology. However, a few participants felt that there are still gaps, due in part to regulators lacking a full understanding of specific industry risk. One participant mentioned that the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, while not a regulation, has helped their sector find alignment among different regulations and requirements.[17] The Federal Financial

[17]National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (Gaithersburg, MD: Feb. 26, 2024).

Institutions Examinations Council IT handbook was also identified as an example of progress in harmonization in the financial sector.[18]

Several industry participants generally agreed that there is some promise that CIRCIA could result in greater harmonization of cybersecurity incident reporting if implemented effectively. However, they did not identify other current efforts to harmonize federal cybersecurity regulations.

One Participant's View on the Evolution of Federal Cybersecurity Regulations

"We suffer from an absence of meaningful evolution in the regulations, and an absence of support in implementing them."

Source: Participant in the industry panels on cybersecurity regulation harmonization. | GAO-25-108436

A few participants noted that additional progress in harmonizing federal cybersecurity regulations depends on a federal entity having the leadership and centralized authority to direct other agencies to further harmonize and reciprocate, as the individual agencies will not do this on their own. Participants emphasized that there needs to be significant progress in creating reciprocity, or mutual agreement to accept each other's security assessments, among regulating entities and their requirements. According to participants, this remains the area of harmonization that has made the least progress. Without such reciprocity, multiple agencies could be regulating one entity in different ways, which leads to duplicative and conflicting requirements.

Federal Agencies Face a Variety of Challenges to Harmonizing Cybersecurity Regulations

Industry participants discussed the following challenges as the largest barriers to federal agencies when harmonizing cybersecurity regulations:

- **Lack of standard definitions and information requirements.** Several participants felt that agencies develop unique cybersecurity definitions that differ from industry, resulting in inconsistent terminologies that cannot be widely applied and reused. Agencies may assume they have unique or special information requirements, but certain industries believe they often send agencies the same information in different formats. A few participants noted that there is uncertainty in their respective industries on which parts of certain regulations apply to specific subsectors. One participant also noted that the federal government does not adequately leverage existing regulations or standards, such as the NIST Cybersecurity Framework.[19]

- **Lack of incentives and mechanisms for coordination.** A few participants believed that agencies' needs for information often have overlap; however, there is a lack of incentive within the federal government to bring industries together to create a common and more manageable framework for agencies to coordinate. For certain sectors, multiple agencies can regulate the same organization but do not appear to be sharing information from their compliance reviews. Participants stated that individual federal agencies are too focused on

[18]Federal Financial Institutions Examination Council, *IT Examination Handbook Infobase, https://ithandbook.ffiec.gov/* (accessed July 7, 2025).

[19]National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (Gaithersburg, MD: Feb. 26, 2024).

their own needs and lack incentives to work with each other when regulating industry. Moreover, the federal government lacks an effective mechanism to drive coordination among individual agencies.

- **Gaps in knowledge and skills within agencies.** Several participants said that agencies generally lack understanding of how industry manages cybersecurity risk. Several participants noted that there is a fundamental lack of federal engagement with industry so that regulators can understand the nuances of specific industries (e.g., the definition of information technology as opposed to operational technology). According to participants, agencies seem to be focusing on details they likely do not need to assess overall cybersecurity risk and outcomes. Expertise varies, but certain regulators may not have sufficient personnel with requisite skills to regulate cybersecurity. A few participants said that the federal government lacks knowledgeable personnel within agencies that can understand the nuanced information industries provide when complying with federal cybersecurity regulations.

One Participant's View on the Need for a Federal Workforce to Implement Harmonization

"While harmonization among government entities and process is important to increase efficiency and usefulness of data received from regulated entities, without an adequate [federal] workforce, these efforts become hampered."

Source: Participant in the industry panels on cybersecurity regulation harmonization. | GAO-25-108436

- **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. According to participants, industries want rapid response and information sharing from agencies they report to, but federal agencies often take too long to share information or release reports in response to threats. As a result, industries may have already taken action to address the threat themselves long before agencies are able to respond.

Industry Identified Near- and Long-term Opportunities for Harmonizing Federal Cybersecurity Regulations

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

Near-term opportunities

- **Prioritize cybersecurity harmonization through existing and upcoming cybersecurity regulations.** Several participants said that CIRCIA, if implemented effectively, has significant potential to achieve harmonization among various regulations. One participant also noted how NIST has been a basis for many cybersecurity programs already, and thus harmonization efforts done in conjunction with industry standards would be particularly beneficial.

- **Reauthorize legislation.** A few participants noted that the Cybersecurity and Information Sharing Act of 2015 should be reauthorized to keep industry protections when sharing

cybersecurity information with federal agencies, which would further collaboration with the federal government.[20]

Long-term opportunities

- **Identify or establish a single entity that has primary, consolidated authority over various federal agencies** that promulgate and enforce cybersecurity regulations. A few participants noted that additional progress in harmonizing federal cybersecurity regulations depends on a federal entity having the leadership and centralized authority to direct other agencies to further harmonize and reciprocate. One participant noted that establishing a single entity that can manage cybersecurity efforts across the federal government would be the primary indicator that an effort to harmonize regulations has been made.

- **Identify a single reporting mechanism as the primary interface with sector entities** regarding cybersecurity regulations. A few participants noted that having a single reporting mechanism would allow industries to report a particular cybersecurity incident once instead of having to report to multiple agencies across multiple time periods.

- **Standardize cybersecurity terminology and information needs across various federal agencies.** Several participants also noted that federal cybersecurity regulations could be adapted to use a performance-based approach and recognize industry standards, stating that a clear and concise standardized reporting structure would eliminate overlap and confusion across organizations in the same industry. Participants suggested consolidating regulation requirements into one singular certification or other indicators of compliance. Additionally, participants said that having a single method (e.g., centralized web portal) and format for reporting cybersecurity information to the federal government would reduce costs and put limited resources to maximum use. One participant noted that one such way to achieve this consolidated requirement is to conduct a single federal assessment of regulated entities that holistically addresses all cybersecurity information needs and requirements. One participant also noted this opportunity could be accomplished by adopting and adhering to the NIST Cybersecurity Framework because that framework was already viewed as a standard in their industry.[21]

One Participant's View on Harmonized Cybersecurity Regulations

"[Cybersecurity regulations should be] risk-based, threat-informed, and based on standards."

Source: Participant in the industry panels on cybersecurity regulation harmonization. | GAO-25-108436

- **Consider liability protections** (e.g., "safe harbor" provisions) or other incentives in conjunction with federal cybersecurity regulations and standards. One participant said that requirements may be harmful if it costs a company greatly to be in full compliance while competing with companies who do not invest in being fully compliant. One participant also said that without liability protections, some organizations would not participate in certain regulatory programs. A few participants believed that implementing an incentive such as

[20]Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2242, 2936-56 (2015) (codified at 6 U.S.C. §§ 1501-10).

[21]National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (Gaithersburg, MD: Feb. 26, 2024).

liability protections can provide a new framework for developing a common regulatory model across industry.

Third Party Comments

We provided a copy of this report to the 12 panel participants for review and comment. Six of the participants provided comments via email, stating that they agreed with our characterization of their views in the report. The other six participants did not provide comments on the report.

- - - - -

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 Public Affairs 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, Jonnie Genova, Sarah Ong, and Walter Vance made key contributions to this report.

Sincerely,

//SIGNED//

David Hinchman
Director, Information Technology and Cybersecurity

Enclosures

Enclosure I: Objective, Scope, and Methodology

Our objective for this report was to gather perspectives from knowledgeable industry participants on how industry views the impact of federal cybersecurity regulations and federal agencies' progress, challenges, and opportunities in harmonizing federal cybersecurity regulations in accordance with national cybersecurity policy and strategy.

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[22] and the Request for Information: Cyber Regulatory Harmonization posted by the Office of the National Cyber Director.[23] 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. Thus, 12 of the 16 critical infrastructure sectors were included in our sample of comments.

After we determined the valid and relevant comments, we then randomly selected participants who had made comments and whose affiliations were associated with the selected critical infrastructure sectors. We invited participants to share their perspectives on the impact current federal cybersecurity regulations have on their industry and the government's harmonization efforts. We then convened two separate 3-hour panels. Each panel included six representatives from industry organizations affiliated with different sectors. In total, the two panels included 12 industry representatives.

We obtained a range of perspectives on the current state of federal cybersecurity regulations and how they impact 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 discussions of each panel and identified overlapping points before consolidating them together to form overarching themes for each topic. For the purposes of quantifying the number of industry participants who made certain statements during the panels, "few" means two to four participants, "several" means five to eight, and "most" means nine 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 panels or a collective view of the panelists' respective sectors. We offered each participant the chance to present alternative views. We also committed to handle industry participants' comments made during the panels with confidentiality to encourage them to speak candidly, unless they otherwise agreed to attribution in specific cases. In addition to

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

[23]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).

the panels, we also reviewed related GAO and federal agency reports related to cybersecurity harmonization.

We conducted our work from April 2025 to July 2025 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 two separate, 3-hour panels of industry participants from multiple critical infrastructure sectors, selected randomly from public comments on a proposed rule for CIRCIA and a request for information from the Office of the National Cyber Director on views regarding cyber regulatory harmonization. The panels were held virtually on May 28 and May 29, 2025. The 12 industry participants who attended the panels and represented different critical infrastructure sectors are listed below.

Scott Algeier	Food and Agriculture Information Sharing and Analysis Center (Food and Agriculture)
Denny Brennan	Massachusetts Health Data Consortium (Healthcare and Public Health)
Patrick Cuff	Fiserv, Inc. (Financial Services)
John DeGour	National Rural Water Association (Water and Wastewater Systems)
Peter Ferrell	National Electrical Manufacturers Association (Critical Manufacturing)
Bill Gulledge	American Chemistry Council (Chemical)
Trey Hodgkins	National Defense Industry Association (Defense Industrial Base)
Sascha Kylau	Alarm Industry Communications Committee (Communications)
Nick Leiserson	Institute for Security and Technology and Cyber Threat Alliance (Information Technology)
Richard Mogavero	Nuclear Energy Institute (Nuclear Reactors, Materials, and Waste)
Marty Reynolds	Airlines for America (Transportation Systems)
Terri Zimmerman	Cummins, Inc. (Energy)