U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

September 28, 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: Industry Panelists Identify Duplication and Conflicts and Ways to Address Them

The nation increasingly depends on computer-based information systems and electronic data to execute fundamental operations and to process, maintain, and report crucial information. Nearly all federal and nonfederal operations, including the nation's critical infrastructure, are supported by these systems and data.[1] 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 it. However, according to the Office of the National Cyber Director (ONCD), when critical infrastructure sectors are subject to multiple cybersecurity regulations, the result can be additional administrative burdens due to conflicting guidance, inconsistencies, increased compliance costs, and redundancies.[2] Harmonization refers to the development and adoption of consistent standards and regulations.

GAO 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 area in 2015 to include protecting the privacy of personally identifiable information. In our most recent update 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.[3]

[1]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 services and facilities; health care and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

[2]The White House, Office of the National Cyber Director, *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information* (Washington, D.C: June 2024).

[3]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).

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 previous two reports in this series were issued in July 2025 and March 2026.[4] This is the third report in the series and summarizes the views shared by selected industry participants in a July 16, 2026, panel discussion. Participants commented on duplication or conflicts among federal cybersecurity regulations that affect selected critical infrastructure sectors, federal agencies' progress in harmonizing regulations, and further opportunities for harmonization.

The panel included six representatives from three different critical infrastructure sectors that our previous work had identified as subject to a significant number of cybersecurity regulations: energy, financial services, and healthcare and public health.[5] The representatives included chief and senior executives overseeing cybersecurity, medical, and other industry operations, as well as regulatory affairs and legal 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.[6] The summary of participants' viewpoints does not necessarily reflect a unanimous opinion of the panel or a collective view of the participants' 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 May 2026 to September 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.

These attacks are often focused on the nation's critical infrastructure sectors, which are described in figure 1 below.

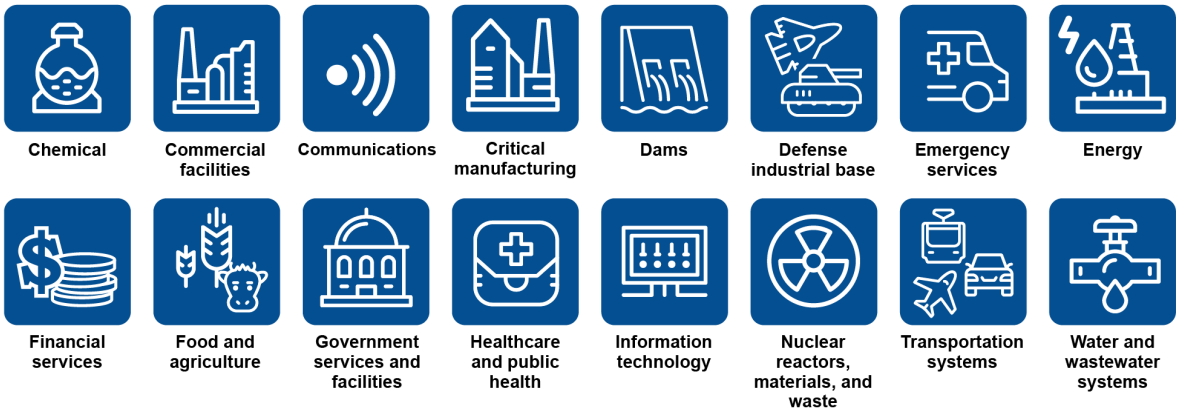
---

[4]GAO, *Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization,* GAO-25-108436 (Washington, D.C.: July 30, 2025) and *Cybersecurity Regulations: Additional Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization,* GAO-26-108685 (Washington, D.C.: Mar. 5, 2026).

[5]GAO, *Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements,* GAO-26-108606 (Washington, D.C.: July. 22, 2026).

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

Figure 1: The 16 Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-26-109197

Federal agencies have issued a variety of regulations to, among other things, help protect health data and ensure smooth operation of financial systems and other infrastructure that also have a cybersecurity component. However, given the complex, interconnected, and interdependent nature of these sectors, private entities may be subject to multiple regulations with cybersecurity requirements from cognizant federal agencies. As regulations are promulgated, industry has an opportunity to draw attention to duplication or other problems with proposed regulations during the comment process.

We have previously identified concerns about potentially duplicative or conflicting cybersecurity regulations and efforts to harmonize those regulations:

- 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.[7]
- In June 2024, we testified that consistent cybersecurity regulations could help protect against the increasing risks that threaten the nation's critical infrastructure sector.[8]
- 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 those requirements.[9]
- In July 2025 and March 2026, we summarized the views of selected industry participants from panel discussions we held on cybersecurity regulations and harmonization, in which industry participants expressed concerns about potentially duplicative or conflicting regulatory requirements, among other things.[10]

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

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

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

[10]GAO-25-108436 and GAO-26-108685.

- In July 2026, we identified 117 cybersecurity regulations established by 37 federal agencies for private entities, spanning nine critical infrastructure sectors. Most of those cybersecurity regulations either contain the same kind of reporting requirement applicable to a sector or the same reporting requirement as at least one other regulation, which may lead to duplication.[11]

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).[12] CIRCIA established a Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements.[13] CIRCIA requires the Cybersecurity and Infrastructure Security Agency, within the Department of Homeland Security, to issue regulations to implement the act's reporting provisions. As of August 2026, the final rule is expected to be finalized in September 2026.
- The White House issued a national critical infrastructure directive in April 2024.[14]
- In support of the previous national cybersecurity strategy, ONCD issued a request for information that invited public comments on opportunities for, and obstacles to, harmonizing cybersecurity regulations.[15]
- In July 2024, and then again in May 2025 during the following Congressional session, proposed legislation known as the Streamlining Federal Cybersecurity Regulations Act was introduced in the Senate, which included requirements aimed at reducing duplicative or conflicting cybersecurity regulations.[16]
- In March 2026, the White House issued a new national cyber strategy, which described cybersecurity priorities intended to increase coordination between the government and private sector, address adversarial threats, remove burdensome or ineffective regulations, and modernize information systems.[17]
- In June 2026, the Congressional Research Service identified several options for Congress to consider if it chose to address disparate cyber incident notification and response frameworks.[18] These options included codifying a harmonized incident reporting framework by statute, empowering ONCD with binding cross-agency authority over cybersecurity

[11]GAO-26-108606.

[12]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).

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

[14]The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum-22 (Washington, D.C.: Apr. 30, 2024). As of August 2026, National Security Memorandum-22 was under review and was no longer available on the White House's public website.

[15]88 Fed. Reg. 55,694 (Aug. 16, 2023).

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

[17]The White House, *President Trump's Cyber Strategy for America* (Washington, D.C: March 2026).

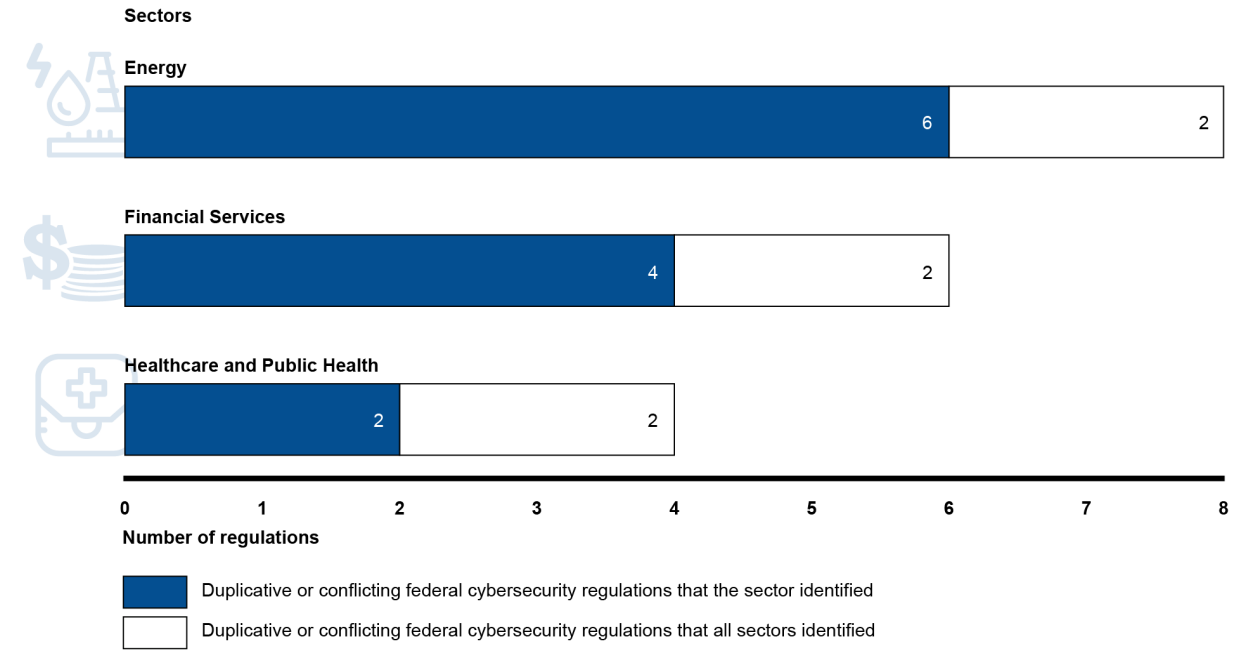
[18]Congressional Research Service, *Cybersecurity: Considerations on Regulatory Harmonization,* R49009 (Washington, D.C.: June 26, 2026).

harmonization, and evaluating whether the resulting rules, from legislation like CIRCIA, achieve sufficient harmonization before intervening legislatively.

Industry Identified Potentially Duplicative or Conflicting Regulations, Progress, and Opportunities for Harmonization

The industry participants from the three sectors on our panel—energy, financial services, and healthcare and public health—all identified potentially duplicative or conflicting federal cybersecurity regulations related to their sector and identified opportunities to harmonize them (see fig. 2). Specifically, the energy sector participants identified eight federal cybersecurity regulations they viewed as duplicative or conflicting, the financial services sector participants identified six, and the healthcare and public health sector participants identified four.[19] Of those, there were two cybersecurity regulations that were commonly identified among all sectors. Participants also identified the impact these regulations have on their respective industries. The views of participants in our July 2026 panel were generally similar to those expressed during our May 2025 and September 2025 panels, but participants offered several additional perspectives and specific regulatory examples from their industries.

Figure 2: Number of Duplicative or Conflicting Federal Cybersecurity Regulations Identified by Selected Industry Sectors



Sources: GAO analysis of industry panel on cybersecurity regulation harmonization; motorama/stock.adobe.com (icons). | GAO-26-109197

[19]Cybersecurity Maturity Model Certification requirements were included under the Defense Federal Acquisition Regulation Supplement and were considered a single requirement for the energy sector.

Duplicative or Conflicting Regulations

Industry participants identified potentially duplicative or conflicting regulations related to their sectors. For example:

- **All sectors (2).** Participants noted two instances of duplication and conflicts from regulations affecting multiple sectors. These regulations were related to timelines and thresholds for cybersecurity incident reporting. Specifically, most participants noted that the (1) Department of Homeland Security's proposed CIRCIA rule or the (2) Securities and Exchange Commission's (SEC) cybersecurity disclosure rules conflicted with their own sector's regulations.[20] For example, most participants noted that reporting thresholds, timelines, and definitions in these rules conflicted with regulations from their sector, making it difficult to fully satisfy all reporting requirements and remediate cyber threats within the required time frames.

- **Energy (6).** In addition to the two regulations discussed above, participants from the energy sector identified six instances of duplicative and conflicting regulations in the areas of cybersecurity incident reporting requirements, information sharing, and contracting requirements.[21] For example, a few stated that overlap between existing sector requirements often results in entities reporting the same incident to multiple agencies, each with their own requirements and timelines. Specifically, participants noted that the (1) North American Electric Reliability Corporation's Critical Infrastructure Protection standards,[22] (2) Department of Energy's form 417,[23] and (3) Transportation Security Administration cybersecurity pipeline requirements[24] contained duplicative and conflicting cyber incident reporting requirements. One participant noted conflict between the North American Electric Reliability Corporation's Critical Infrastructure Protection information safeguarding requirements and other information reporting requirements that call for industry to submit potentially sensitive information about cybersecurity incidents to regulators. One participant identified additional regulations as potentially duplicative or conflicting, including the (4) Federal Acquisition Regulation,[25] the (5) Defense Federal Acquisition Regulation Supplement,[26] (including the Contractor Compliance with the Cybersecurity Maturity Model

[20]Securities and Exchange Commission Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule, 88 Fed. Reg. 51,896 (Aug. 4, 2023). The rule requires cybersecurity disclosures for public companies subject to the reporting requirements of the Securities Exchange Act of 1934.

[21]One participant also noted state, local, and industry requirements that are duplicative with federal cybersecurity requirements.

[22]North American Electric Reliability Corporation, *Critical Infrastructure Protection Standards* (May 2, 2006).

[23]Department of Energy Form 417 is a mandatory emergency form filed by specific electric power industry actors when at least one qualifying criteria is met pursuant to Section 13(b) of Federal Energy Administration Act of 1974, Pub. L. No. 93-275 (15 U.S.C. §772).

[24]Security Directive Pipeline-2021-02G: *Renewal of the Security Directive Pipeline-2021-02 Series: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (Springfield, VA.: May 3, 2026).

[25]Federal Acquisition Regulation (FAR) 48 Code of Federal Regulations ch. 1 (2026). As of August 2026, the FAR was undergoing substantial revisions with interim replacement language being implemented through deviations.

[26]Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. ch. 2 (2026).

Certification clause),[27] and (6) General Services Administration Controlled Unclassified Information Requirements.[28]

- **Financial services (4).** In addition to the two regulations affecting all sectors discussed above, participants from the financial services sector identified four instances of conflicting timelines and thresholds for reporting obligations, tension between confidential reporting and public disclosure, and multiple reporting obligations for cybersecurity events. For example, a few participants stated that a cyber-related disruption may require them to comply with several requirements including the (1) National Credit Union Administration (NCUA) incident reporting[29] and (2) Bank Secrecy Act[30] requirements. Additionally, one participant stated that they may have to comply with several additional requirements including SEC disclosure rules affecting all sectors, the (3) Federal Trade Commission Safeguard Rule,[31] and the (4) Gramm-Leach-Bliley Act.[32] Participants noted that these requirements have conflicting timelines for when to report and thresholds on what constitutes an incident. For example, a few participants stated that the differing regulations require them to report cybersecurity incidents within 72 hours per the NCUA, 24 to 72 hours per the proposed CIRCIA rule depending on the type of incident, and 4 business days per the SEC. Additionally, the participants noted that definitions of what constitutes a reportable incident are inconsistent, and that it is difficult to work with law enforcement, meet multiple reporting requirements, and secure the cybersecurity breach within the required time frames. Further, one participant noted potential conflict between confidential reporting requirements that are contained in suspicious activity reports and SEC public disclosure rules that could result in the public release of potentially confidential information.[33]

- **Healthcare and public health (2).** In addition to the two regulations affecting all sectors, discussed above, participants from the healthcare and public health sector identified two instances of duplicative and conflicting regulations in the areas of incident reporting timelines, differences in definitions for what constitutes a breach, and tension between sharing information versus protecting information. For example, one participant stated that the timelines for incident reporting under the proposed CIRCIA rule, SEC disclosure rules,

[27]Contractor Compliance with the Cybersecurity Maturity Model Certification (CMMC) Level Requirements 48 C.F.R. § 252.204-7021 (2026).

[28]General Services Administration, *Controlled Unclassified Information (CUI) Policy*, CIO 2103.2 (Washington, D.C.: April 2021).

[29]National Credit Union Administration 12 C.F.R. Part 748.1(c): Security Program, Suspicious Transactions, Catastrophic Acts, Cyber Incidents, and Bank Secrecy Act Compliance.

[30]Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-24 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.). Regulations implementing the Bank Secrecy Act primarily appear in 31 C.F.R. Ch. X. The Bank Secrecy Act defines financial institutions as insured banks, licensed money transmitters, insurance companies, travel agencies, broker-dealers, and dealers in precious metals, among other types of businesses. See 31 U.S.C. § 5312(a)(2).

[31]Federal Trade Commission 16 C.F.R. Part 314: Standards for Safeguarding Customer Information.

[32]Gramm-Leach-Bliley Act, Pub. L. No. 106-102, tit. V, subtit. A, 113 Stat. 1338, 1436-1445 (1999) (codified as amended at 15 U.S.C. §§ 6801-6809); Fair Credit Reporting Act, Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1127-1136 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

[33]Department of the Treasury 31 C.F.R Part 1020: Rules for Banks.

and (1) Health Insurance Portability and Accountability Act of 1996 (HIPAA) breach rules differ and conflict making it difficult to fully satisfy all requirements.[34] Participants noted that (2) information blocking rules from the Office of the National Coordinator, which prevent practices that affect the access, exchange, or use of health information, may be interpreted as conflicting with HIPAA security and privacy requirements that limit the release of information.[35] One participant stated that there may be actual conflict in certain circumstances, while another stated that—especially for smaller healthcare practices with limited compliance staff—the mere confusion and concern over potential conflict can lead to delays in meeting reporting timelines even if no actual conflict exists. Additionally, one participant noted a conflict across the CIRCIA, SEC, and HIPAA requirements in the definition of a reportable cybersecurity incident. The participant stated that CIRCIA defines the reporting threshold more broadly than the other two regulations which can result in multiple legal analyses and inconsistent public messaging about the same cybersecurity event.

Participant's View on the Duplication or Conflict in Federal Cybersecurity Regulations

"We have tensions between reliability and modernization. Companies are encouraged to adopt [emerging] technologies, but must do so with existing reliability and cybersecurity compliance frameworks that may not evolve at the same pace."

Source: Participant in the industry panel on cybersecurity regulation harmonization. | GAO-26-109197

Industry Identified Limited Progress in Harmonizing Cybersecurity Regulations

Most participants stated that there has been some progress made in working toward federal cybersecurity regulatory harmonization for their respective sectors over the past year. However, several participants agreed that the federal government's progress has been limited in harmonizing existing duplication and addressing conflicts among cybersecurity regulations. One participant noted that there have been some interagency efforts involving the Federal Financial Institutions Examination Council (FFIEC)[36] to direct institutions or examiners to look at FFIEC's information technology handbook to provide guidance on evaluating security programs.[37] The participant also noted interagency efforts to offer increased regulatory guidance for complying with the Bank Secrecy Act and related anti-money laundering requirements.[38] A few participants

[34]The HIPAA Privacy, Security, Enforcement, and Breach Notification Rules were issued at 45 C.F.R. Parts 160 and 164 and were updated at 78 Fed. Reg. 5566 (Jan. 25, 2013) and 79 Fed. Reg. 7290 (Feb. 6, 2014).

[35]Department of Health and Human Services 45 C.F.R. Part 171: Information Blocking.

[36]The Federal Financial Institutions Examination Council is an interagency body that focuses on promoting consistency in examination activities. The Council is comprised of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau.

[37]Federal Financial Institutions Examination Council, *Information Security Booklet*, (Washington, D.C.: September 9, 2016).

[38]The FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual provides guidance for carrying out examinations related to the Bank Secrecy Act requirements.

from the healthcare and public health sector noted that HIPAA regulations are currently undergoing potential significant updates but also noted that the timeline for completion of that work was unclear to them.[39]

One Participant's View on Opportunities to Harmonize Cybersecurity Regulations

"The objective should be one report that satisfies multiple federal requirements where information is [substantially] the same. This would allow [entities] to focus on responding to incidents while ensuring the government receives timely and actionable information."

Source: Participant in the industry panel on cybersecurity regulation harmonization. | GAO-26-109197

Industry Identified Opportunities to Harmonize Federal Cybersecurity Regulations

Industry participants in our July 2026 panel identified opportunities to harmonize federal cybersecurity regulations.

- **Harmonize incident reporting.** Most participants stated that cybersecurity incident reporting and the related reporting time frames, thresholds, and definitions should be harmonized. Specifically, most participants noted that the use of substantially similar definitions for reporting time frames and thresholds can reduce the need for duplicative and multiple reporting obligations. Additionally, one participant stated that CIRCIA's "substantially similar reporting" provision could offer a positive opportunity for streamlining requirements to reduce duplication.[40]

- **Consolidate agency authority**. Most participants stated that establishing a single entity with authority over regulatory consistency could be beneficial for purposes of cybersecurity regulatory harmonization. For example, most participants agreed that a coordinated federal cybersecurity reporting model could be helpful whereby an agency with leading authority, such as the Cybersecurity and Infrastructure Security Agency, could receive incident reporting information to coordinate or disseminate the information to other federal agencies.

- **Increase collaboration.** Additionally, most participants stated that increasing collaboration between government agencies and industry could be helpful for harmonization. Specifically,

[39]Through its Notice of Proposed Rulemaking, the Department of Health and Human Services sought comments in March 2025 on a proposal to modify the Security Standards for the Protection of Electronic Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009. The proposed modifications would revise existing standards to better protect the confidentiality, integrity, and availability of electronic protected health information. As of August 2026, the final rule is expected to be released in July 2027. HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898 (January 6, 2025).

[40]Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), a covered entity that reports a covered cybersecurity incident, ransom payment, or information otherwise required in a supplemental report to another federal agency does not have to report the same information to the Cybersecurity and Infrastructure Security Agency (CISA) if the entity is required by law, regulation, or contract to report substantially similar information to another federal agency in a substantially similar time frame as it would report to CIRCIA, and if CISA and the agency have in place an information sharing mechanism and information sharing agreement. As of August 2026, the final CIRCIA rule has not been released and this provision is subject to change.

participants noted that ongoing engagement between government agencies and industry for harmonization efforts would be beneficial.

Third Party Comments

We provided a copy of this report to the six panel participants for review and comment. Two of the participants provided comments via email, stating that they agreed with our characterization of their views in the report. An additional participant provided technical comments, which we incorporated as appropriate. The other three 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 Media Relations may be found on the last page of this report. In addition, Joshua Leiling (Assistant Director), David Hong (Analyst in Charge), Timothy Barry, Brandon Cox, Jonnie Genova, Torrey Hardee, Smith Julmisse, Evan Nelson Senie, and Walter Vance made key contributions to this report.

//SIGNED//

David B. Hinchman
Director, Information Technology and Cybersecurity

Enclosures

Enclosure I: Objective, Scope, and Methodology

Our objective for this report was to summarize industry views from selected critical infrastructure sectors on duplication or conflicts among federal cybersecurity regulations. This is the third report in a series on this topic and summarizes the views shared by selected industry participants in a July 2026 panel. Our previous two reports in this series were issued in July 2025 and March 2026.[41]

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[42] and the Request for Information: Cyber Regulatory Harmonization posted by the Office of the National Cyber Director.[43] We then grouped the industry organizations and their representatives into different critical infrastructure sectors.

We then identified three key critical infrastructure sectors for participation in our panel: energy, financial services, and healthcare and public health. These three sectors were among those with a significant number of federal cybersecurity regulations according to our recent review of those regulations, which was issued in July 2026.[44] We contacted industry organization representatives from those three sectors via email who had either previously participated in our prior two panels or noted their interest in participating but were not previously selected due to space limitations. When potential participants did not respond by the requested deadline or were not available, we continued our outreach to the next potential participant in a randomized order list of comments. We repeated this process until we identified two stakeholders from each sector.

We then convened one 3-hour panel on July 16, 2026, with six participants representing industry organizations affiliated with the three different sectors. We obtained a range of perspectives on federal cybersecurity regulations that participants identified as duplicative or conflicting and how they impact different critical infrastructure sectors. We also gathered perspectives on the progress industry participants have seen from recent harmonization efforts, and opportunities they believe could come from continuing efforts. We reviewed the panel discussion 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, “a few” means one to two participants, “several” means three, and "most" means four or more participants.

The information in this report summarizes the industry participants’ perspectives and the points that were raised. The summary of participants’ viewpoints does not necessarily reflect a

[41]GAO, *Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization,* GAO-25-108436 (Washington, D.C.: July 30, 2025) and *Cybersecurity Regulations: Additional Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization,* GAO-26-108685 (Washington, D.C.: Mar. 5, 2026).

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

[43]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).

[44]GAO, *Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements,* GAO-26-108606 (Washington, D.C.: July 22, 2026).

unanimous opinion of the panel or a collective view of the participants' 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 May 2026 to September 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 July 16, 2026. The six industry participants who attended the panel and represented the three selected critical infrastructure sectors are listed below.

Denny Brennan	Massachusetts Health Data Consortium (healthcare and public health)
Jennifer DeCesaro	Edison Electric Institute (energy)
Jeremy Greenberg	America’s Credit Unions (financial services)
Rick Van Luvender	Fiserv (financial services)
Dr. Steven Waldren	American Academy of Family Physicians (healthcare and public health)
Bill Zuretti	Electric Power Supply Association (energy)