U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

July 22, 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: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements

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 these assets and systems. 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 from conflicting guidance, inconsistencies, increased compliance costs and redundancies.[2] Harmonization refers to the development and adoption of consistent standards and regulations. Such consistency is important to ensure that cybersecurity requirements do not overlap, duplicate, or conflict with each other.

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

[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).

implementing a national cybersecurity strategy was needed to protect the nation's information systems and infrastructure.[3]

You asked us to conduct a series of reviews of federal cybersecurity regulations to determine their impact on industry. As part of this work, we issued two reports in July 2025 and March 2026 that addressed your request to summarize industry perspectives on federal cybersecurity regulations.[4] Additionally, you asked us to review federal cybersecurity regulations to identify opportunities for regulatory harmonization. This report determines the extent to which federal cybersecurity regulations and requirements are potentially duplicative or conflicting for regulated private sector entities.

To identify relevant federal cybersecurity regulations,[5] we reviewed publicly available information on regulation harmonization including a Department of Homeland Security (DHS) report on incident reporting and public comments responding to ONCD's request for information on harmonizing cybersecurity regulations.[6] We also conducted keyword searches of information publicly available in the Electronic Code of Federal Regulations in December 2025.[7] The cybersecurity regulations we identified may not represent all federal cybersecurity regulations that exist due to the search parameters and timeframes of our search.

We then reviewed the scope, applicability, and details from each regulation to identify their cybersecurity-related requirements for industry and the critical infrastructure sectors they affected. We analyzed each regulation to determine whether it had one or more of three different types of reporting requirements for private industry to report to federal agencies—cybersecurity incidents; reviews, audits, or assessments; or cybersecurity plans or other technical information.

We reviewed plans and analyses conducted by ONCD and DHS to identify and streamline potentially duplicative and conflicting cybersecurity regulations. We reviewed those agencies' responsibilities, as outlined in relevant laws, executive orders, and the national cybersecurity strategy, and summarized their efforts to streamline regulations. We also interviewed relevant

---

[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).

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

[5]For this report, we refer to any regulation with a cyber-related requirement as cybersecurity regulations, though in many cases the cybersecurity provision may be a minor part of a larger regulation. To be consistent, and because these cybersecurity requirements vary in their structure and complexity, we identify these regulations in the appendix by the title and part of the Code of Federal Regulations in which they appear. Where appropriate, we also considered additional details from agency forms, security standards or directives, circulars, or other notices that expand upon or provide further details about cybersecurity-related requirements in a regulation.

[6]Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government*, (Washington, D.C.: Sept. 2023); 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).

[7]The Code of Federal Regulations is the official legal print publication containing the codification of the general and permanent rules published in the Federal Register by the departments and agencies of the Federal Government. The Electronic Code of Federal Regulations is a continuously updated online version of the Code of Federal Regulations, which can be found at https://www.ecfr.gov/.

officials from DHS and the Federal Communications Commission to better understand their roles and plans to harmonize regulations. In September 2025 and June 2026, we sought information from ONCD to better understand its role and related plans as the federal lead for coordinating efforts to harmonize cybersecurity regulations. As of June 2026, ONCD had not provided information in response to our questions. See enclosure I for additional information on our objective, scope, and methodology. The list of the federal cybersecurity regulations that we identified, grouped by infrastructure sector, and our analysis of those regulations, can be found in enclosure II.

We conducted this performance audit from August 2025 to July 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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 and contractors, 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.

DHS and various other 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, given the complex, interconnected, and interdependent nature of critical infrastructure, private sector entities may be subject to multiple regulations from federal agencies. As regulations are promulgated, industry has an opportunity to draw attention to duplication or other problems with proposed regulations or other existing requirements during the comment process.

We have previously identified concerns about potentially duplicative cybersecurity regulations and efforts to harmonize those regulations. 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.[8] Further, in June 2024, we testified that consistent cybersecurity regulations could help protect against the increasing risks that threaten our nation's critical infrastructure sector.[9] Additionally, in July 2024, we reported on DHS's efforts to implement federal cyber incident reporting requirements and the challenges with harmonizing those requirements.[10] We identified challenges including differences in definitions of reportable cyber incidents, timelines and triggers for when reports must be made, the contents of cyber incident reports, and how reports are submitted to federal agencies.

---

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

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

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

Additionally, in our July 2025 and March 2026 reports, we summarized the views of selected industry participants from panel discussions we held on cybersecurity regulations and harmonization.[11] Industry panelists expressed concerns about potentially duplicative regulatory requirements. Specifically:

- Panel participants felt that cybersecurity incident reporting is often duplicative, and that there are inconsistent incident reporting requirements among federal regulations. 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.
- 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.

Federal Cybersecurity Regulations in Multiple Sectors Contain Potentially Duplicative Requirements

More than One Hundred Federal Cybersecurity Regulations Exist, and Most of These Have Reporting Requirements

As of June 2026, we identified cybersecurity regulations established by 37 federal agencies for private entities within nine critical infrastructure sectors. Most of these 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 might lead to overlap and duplication in certain cases. Specifically, 80 of the 117 cybersecurity regulations we identified (about 70 percent) had, at least, one or more of the following three types of reporting requirements for private entities to proactively report

- cybersecurity incidents;
- cybersecurity plans or other technical information; or
- reviews, audits, or assessments.[12]

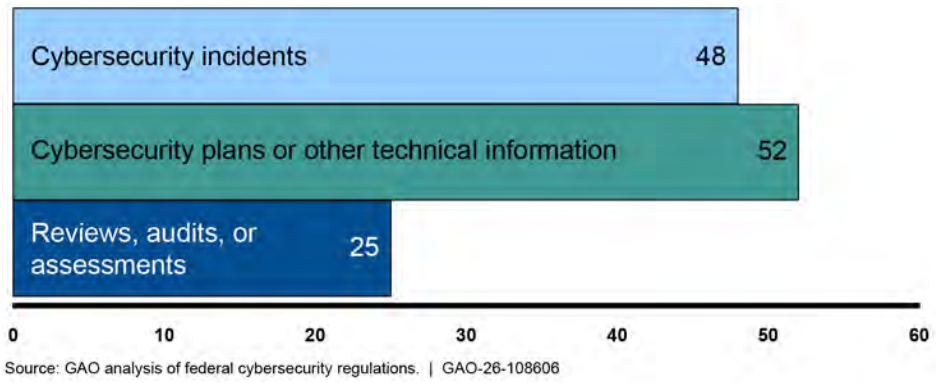
Combined, these 80 regulations had at least 125 requirements for private entities to report. Specifically, 48 required reporting on cybersecurity incidents; 52 required reporting on cybersecurity plans or other technical information; and 25 required reporting on cybersecurity reviews, audits, or assessments. Many regulations required multiple types of reporting. When multiple regulations have the same types of reporting requirements, particularly when the requirements affect entities within the same sector or across multiple sectors, those regulations have the potential to be duplicative or conflicting. Figure 1 illustrates the total number of federal cybersecurity regulations with each type of reporting requirement. As described below, we found

[11]GAO-25-108436; GAO-26-108685.

[12]We identified a total of 119 cybersecurity regulations, including 117 established and two proposed. For the purposes of our review, regulations were determined to have reporting requirements when they require a private entity to proactively provide information or documentation to a federal agency regarding these three categories of cybersecurity information. Of the 117 established regulations, there were 80 that had at least one of these three types of reporting requirements and 37 that did not have any of the three types. We did not include the two proposed regulations in our totals of regulations with each type of reporting requirement, as the proposed regulations' requirements are unsettled until finalized.

several instances where different cybersecurity reporting requirements are potentially duplicative.

Figure 1: Number of Cybersecurity Regulations with Reporting Requirements, as of June 2026



Source: GAO analysis of federal cybersecurity regulations. | GAO-26-108606

Note: Totals represent the number of regulations identified with each type of reporting requirement. Because some regulations contain more than one reporting requirement, those regulations may be counted in more than one category.

Cybersecurity incidents. More than a third of the 117 federal cybersecurity regulations that we identified contained requirements to report cyber incidents to federal agencies. Specifically, 48 required private entities to report, within various specified timeframes, cybersecurity incident information such as security breaches and actions taken to resolve the incident. These regulations included sector-specific and cross-sector reporting requirements from 27 federal agencies. As a result, private sector entities may be required to report similar or different cyber incident information to multiple agencies. According to DHS's report on federal cybersecurity incident reporting, entities subject to agencies' incident reporting requirements may be faced with potentially conflicting reporting requirements resulting from differences in the definition of cyber incidents and thresholds for reporting, timelines and triggers for when to report, and the contents of incident reports.[13]

For example, in the financial services sector, a private sector entity may have to comply with multiple cyber incident reporting requirements depending on which of the 15 regulations it is subject to from the Commodity Futures Trading Commission, Federal Deposit Insurance Corporation, Federal Trade Commission, Department of the Treasury, National Credit Union Administration, Office of the Comptroller of the Currency, Securities and Exchange Commission, and the Federal Reserve Board.[14] Additionally, private sector entities subject to one or more of these 15 regulations may also be subject to pending regulation from DHS's Cybersecurity and Infrastructure Security Agency (CISA) on covered cyber incident and ransomware payment reporting pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022

[13]DHS, *Harmonization of Cyber Incident Reporting to the Federal Government* (Washington, D.C.: Sept. 19, 2023).

[14]Commodity Futures Trading Commission 17 C.F.R. Parts 37, 38, 39, and 49; Department of Treasury 31 CFR Part 1020; Federal Deposit Insurance Corporation 12 C.F.R. Parts 304, 364; Federal Trade Commission 16 C.F.R. Part 314; National Credit Union Administration 12 C.F.R. Part 748; Office of the Comptroller of the Currency 12 C.F.R. Parts 30, 53; Securities and Exchange Commission 17 C.F.R. Parts 242, 248; Federal Reserve Board 12 C.F.R. Parts 225 and 234.

(CIRCIA).[15] When finalized, the CIRCIA rule is expected to apply to entities in a critical infrastructure sector, which may include public companies as well as other types of organizations in various sectors. As noted in CISA's proposed rulemaking, collectively, the financial services cybersecurity incident regulations and the CIRCIA cross-sector regulation have the potential to result in duplicative reporting of cybersecurity incidents to different federal agencies. In addition, the potential exists for CIRCIA to have varying requirements for when financial services sector entities are to report cybersecurity incidents, including what to report and how soon sector entities are expected to notify federal agencies.[16]

Cybersecurity plans or other technical information. Fifty-two federal cybersecurity regulations contained requirements to report cybersecurity plans or other information that does not involve incident reporting or reviews, audits, and assessments. Such reporting may include cybersecurity plans and planned changes to system security. These regulations included sector-specific and cross-sector reporting requirements from 26 federal agencies. As a result, sector entities may be required to provide the same cyber-related documentation to multiple agencies. For example:

- Information Technology (IT) sector: A federal contractor providing services to federal agencies may be required to provide documentation to potentially several different federal agencies indicating whether the contractor's IT security plans follow agency cybersecurity requirements.[17] As a result, a contractor doing business with more than one of the agencies may be required to report similar information multiple times.

- Cross-sector: Transportation systems sector entities are required to provide cybersecurity plans and other documentation to comply with as many as seven federal regulations.[18] While these regulations focus on different modes of transportation, regulations affecting all sectors may duplicate or conflict with regulations focused on a specific sector. For example, among other requirements, the Securities and Exchange Commission requires publicly traded companies to also provide cybersecurity plans.[19] Such cross-sector regulations have

[15]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). DHS stated that CIRCIA was intended to help preserve national security, economic security, and public health and safety by requiring certain entities to submit cyber incident reports to CISA, enabling CISA and the interagency to leverage the information for various cybersecurity purposes.

[16]Through its Notice of Proposed Rulemaking, CISA has sought public comments on implementing CIRCIA including ways to harmonize the rule with other requirements. According to CISA, it intends to explore options with the financial services sector to enable entities, with substantially similar reporting through exception, to comply with both regulatory reporting regimes through the submission of a single report to the federal government. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644 (Apr. 4, 2024).

[17]See, for example, Department of Transportation 48 C.F.R Part 1252 and Department of State 48 C.F.R Part 652.

[18]Coast Guard, 33 CFR Part 101: Maritime Security: General; Federal Aviation Administration, AC 119-1A: Operational Authorization of Aircraft Network Security Program; Federal Railroad Administration: 49 CFR Part 299: Texas Central Railroad High-Speed Rail Safety Standards; Transportation Security Administration: 1580-21-01E: Security Directive Enhancing Rail Security; 1582-21-01E: Enhancing Public Transportation and Passenger Railroad Cybersecurity; 49 CFR Part 1570: General Rules; Transportation Security Administration: Pipeline-2021-01G: Security Directive Enhancing Pipeline Cybersecurity.

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

the potential to duplicate or conflict with transportation-based regulations affecting airlines, shipping companies, and entities from other transportation modalities.

Reviews, audits, or assessments. Twenty-five federal cybersecurity regulations contained requirements for private sector entities to report cybersecurity reviews, audits, or assessments to demonstrate they met specific security protections. These regulations included sector-specific and cross-sector reporting requirements from 15 federal agencies. As a result, and depending on what regulations they are covered by, sector entities may be required to provide duplicative compliance data or conduct multiple compliance audits that could vary in scope, depth, and methodology to comply with multiple regulations. For example, within the IT sector, similar to requirements to report cybersecurity plans or other technical information, contractors providing services to federal agencies are required to provide documentation of completed cybersecurity reviews, audits, or assessments to several federal agencies.[20] As a result, a contractor doing business with more than one of the agencies may be required to report similar information multiple times.

We have ongoing work to obtain additional industry perspectives on federal cybersecurity regulations, including where they perceive overlap and duplication within selected critical infrastructure sectors. We expect to issue a report with those industry perspectives in fall 2026.

Executive Branch Efforts to Harmonize Regulations Have Made Limited Progress, but Pending Strategy Implementation Plan Could Help

Under federal law, ONCD is responsible for efforts to coordinate the streamlining of regulations relating to cybersecurity.[21] In addition, the April 2024 National Security Memorandum-22 stated that the National Cyber Director should coordinate with federal agencies for cybersecurity regulatory harmonization of security and resilience requirements.[22] Additionally, the memorandum called for DHS to develop a plan to harmonize cybersecurity regulations as part of a national plan for infrastructure risk management, which was to be issued by April 2025.[23]

Over the past several years, ONCD and other agencies within the executive branch have initiated several actions that were intended to help harmonize cybersecurity regulations. Figure 2 illustrates several of these actions.

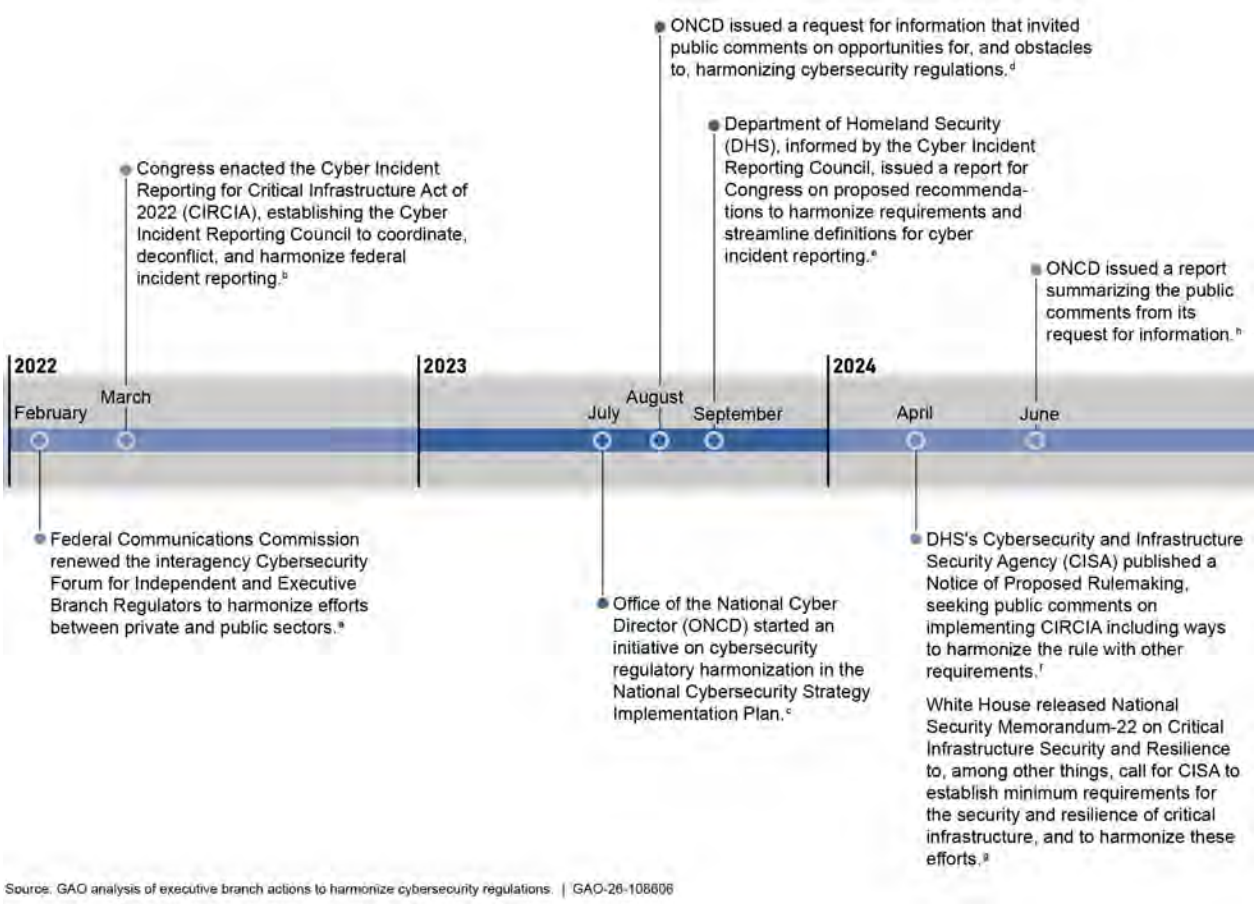
[20]Department of Commerce 48 C.F.R. Part 1352; Department of Defense 48 C.F.R. Part 204; Department of Education 48 C.F.R. Part 3439; Department of State 48 C.F.R Part 652; Department of Transportation 48 C.F.R. Part 1252.

[21]6 U.S. Code §1500.

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

[23]As of June 2026, National Security Memorandum-22 was under review and was no longer available on the White House's public website.

Figure 2: Federal Actions to Harmonize Federal Cyber Regulations



Source: GAO analysis of executive branch actions to harmonize cybersecurity regulations. | GAO-26-108606

[a]Federal Communications Commission, Chairwoman Rosenworcel to Lead Relaunched Federal Interagency Cybersecurity Forum (Washington, D.C.: Feb. 2022).
[b]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).
[c]The White House, *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).
[d]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).
[e]DHS, *Harmonization of Cyber Incident Reporting to the Federal Government* (Washington, D.C.: Sept. 19, 2023).
[f]Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23,644 (Apr. 4, 2024).
[g]The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum-22 (Washington, D.C.: Apr. 30, 2024).
[h]The White House, Office of the National Cyber Director, *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information* (Washington, D.C: June 2024).

However, many past federal efforts have experienced delays and made limited progress. For instance, according to CISA officials, after the release of Executive Order 14239 in March 2025, the executive branch paused activities associated with National Security Memorandum-22, including harmonization efforts, while the administration completes its review of the

memorandum.[24] As of June 2026, this review was still underway. With respect to CIRCIA, in February 2026 CISA planned to hold several townhalls with industry to obtain feedback on its proposed rule and then expected to finalize the rule in May 2026. In March 2026, CISA canceled town halls which were originally scheduled for March and April 2026 due to a lapse in appropriations. Additionally, CISA stated that the shutdown will likely delay the final rule for CIRCIA. CISA subsequently rescheduled the townhalls for June 2026. As of July 2026, CISA planned to issue its final rule in September 2026.

In addition, the Cybersecurity Forum for Independent and Executive Branch Regulators was intended to be a voluntary, interagency group to increase the overall effectiveness and consistency of regulatory agency cybersecurity efforts pertaining to U.S. critical infrastructure. According to Federal Communications Commission officials, the forum has informally explored ways to harmonize regulations, but it has not been active since late 2024.

Also, in CIRCIA, Congress established the Cyber Incident Reporting Council in 2022 to coordinate, deconflict, and harmonize federal incident reporting requirements. DHS, informed by the work of the council, issued a report in September 2023 that included eight recommendations that the federal government could adopt to streamline and harmonize cyber incident reporting. For example, the report recommended that the federal government adopt model definitions of a reportable cyber incident, reporting timelines, and reporting triggers. However, as of May 2026, DHS has not reported on the status of its efforts to address the recommendations from the council's September 2023 report.

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.[25] Specifically, the strategy created six pillars to guide the implementation of the strategy. For example, one of the strategy's pillars focused on harmonization and included plans to streamline cyber regulations to, among other things, reduce compliance burdens, better align regulators and industry, and streamline data.

As of July 2026, the administration has not yet released implementation plans for executing its strategy. As a result, the role ONCD and other agencies are to play in implementing and overseeing these efforts, which would have a direct impact on the private sector's responsibilities for securing our nation's critical infrastructure, remain unclear. According to its cyber strategy, the administration intends to release implementation plans, which could help clarify lead agency roles, responsibilities, and next steps. In addition to establishing implementation plans, it will be important for ONCD and other involved agencies to prioritize and follow-through on previously initiated efforts to harmonize cybersecurity regulations. Doing so will help achieve the goal of reducing potentially burdensome requirements on the private sector while enhancing the cybersecurity of the nation's critical infrastructure.

---

[24]Exec. Order 14239, *Achieving Efficiency Through State and Local Preparedness* 90 Fed. Reg. 13,267 (Mar. 18, 2025). Among other actions, the order calls for the Assistant to the President for National Security Affairs, in coordination with the Director of the Office of Science and Technology Policy and the heads of relevant agencies, to review all critical infrastructure policies and recommend to the President the revisions, recissions, and replacements necessary to achieve a more resilient posture.

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

Agency Comments

We provided a draft of this report to ONCD for review and comment. ONCD did not provide comments on the report.

- - - - -

We are sending copies of this report to appropriate congressional committees, the heads of agencies covered in our review, 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), Torrey Hardee (Analyst in Charge), Timothy Barry, Chris Businsky, Brandon Cox, Jonnie Genova, David Hong, and Walter Vance made key contributions to this report.

//SIGNED//

David B. Hinchman
Director, Information Technology and Cybersecurity
Enclosures – 2

Enclosure I: Objective, Scope, and Methodology

Our objective for this report was to determine the extent to which federal cybersecurity regulations and requirements are potentially duplicative or conflicting for regulated private sector entities. This is the third report in a series of reports reviewing the impact of federal cybersecurity regulations on industry. Our previous two reports in this series were issued in July 2025 and March 2026.[26]

To conduct our work, we reviewed publicly available information on regulation harmonization including agency websites, a Department of Homeland Security (DHS) report on incident reporting,[27] and public comments responding to the Office of the National Cyber Director's (ONCD) request for information on harmonizing cybersecurity regulations.[28] We also conducted keyword searches of information publicly available in the Electronic Code of Federal Regulations.[29] Specifically, we searched the Electronic Code of Federal Regulations in December 2025 using the following cyber-related keywords and phrases: "cyber," "cyber compliance," "cyber incident reporting," "cyber risk management," "cybersecurity," "cybersecurity compliance," "cybersecurity incident reporting," "cybersecurity risk management," "information technology security," and "operational technology security."

We defined cybersecurity regulations as those with cybersecurity-related requirements. We reviewed the scope, applicability, and details from each regulation to identify federal regulations that had cybersecurity-related requirements for industry and the critical infrastructure sectors they affected. For reporting purposes, we generally counted cybersecurity regulations as separate based on the individual parts within the Code of Federal Regulations with which they were associated. In several instances, we adjusted our regulation citations to directly cite agency forms, security standards or directives, circulars, or other notices that expand upon or provide further details about the cybersecurity-related requirements of an agency's regulation.

To determine the reliability of this data, we conducted a legal review of the regulations and their underlying requirements, which included identifying updates and associated supplementation to other material outside of the Electronic Code of Federal Regulations, where appropriate. We determined the data were sufficiently reliable for the purpose of our review. The cybersecurity regulations we identified may not represent all federal cybersecurity regulations that exist due to the search parameters and timeframes of our search.

We identified a total of 119 cybersecurity regulations, including 117 established and two proposed regulations. We then reviewed those regulations for cybersecurity reporting

---

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

[27]Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the Federal Government*, (Washington, D.C.: Sept. 2023).

[28]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).

[29]The Code of Federal Regulations is the official legal print publication containing the codification of the general and permanent rules published in the Federal Register by the departments and agencies of the Federal Government. The Electronic Code of Federal Regulations is a continuously updated online version of the Code of Federal Regulations, which can be found at https://www.ecfr.gov/.

requirements that applied to private industry and identified potentially duplicative or conflicting reporting requirements based on whether they had the same types of reporting requirements for private entities. To do this, we reviewed each regulation to identify whether it had reporting requirements for private entities to proactively report to federal agencies on cybersecurity incidents; cybersecurity plans or other technical information; or completed reviews, audits, or assessments.[30]

For the purposes of our review, regulations were determined to have reporting requirements when they call for a private entity to provide information or documentation to a federal agency across these three categories of cybersecurity information.[31] For example, requirements that call for private industry to notify one or more federal agencies of data or privacy breaches through direct reporting or other mechanisms were included in cybersecurity incidents; requirements that call for documentation to be submitted such as certifications, self-assessments, and analyses were included in completed reviews, audits, or assessments; and requirements that call for documentation to be approved such as information security plans, data use agreements, and other completed forms were included in cybersecurity plans or other technical information. Requirements like producing the documents only in response to a request from the regulator were not included. We also did not include other laws, regulations, and security policies incorporated by reference.

We also reviewed established plans and analyses conducted by the ONCD and DHS to identify and streamline potentially duplicative and conflicting cybersecurity regulations. We also reviewed those agencies' responsibilities, as outlined in relevant laws, executive orders, and the March 2026 national cybersecurity strategy, and summarized their efforts to streamline regulations. We interviewed relevant officials from DHS to better understand their roles and plans to harmonize regulations. We also interviewed officials from the Federal Communications Commission to discuss efforts of the Cybersecurity Forum for Independent and Executive Branch Regulators to harmonize cybersecurity regulations. In September 2025, we sought information from ONCD to better understand its role and related plans as the federal lead for coordinating efforts to harmonize cybersecurity regulations. As of June 2026, ONCD had not provided information in response to our questions.

We conducted this performance audit from August 2025 to July 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[30]Because regulations across the government are written and structured differently, analysis of certain regulations required judgment calls to categorize. Therefore, the results might not be precisely replicable and are designed to provide a starting point for harmonization efforts.

[31]Several regulations we identified incorporated the reporting requirements of the Federal Information Security Modernization Act of 2014 (FISMA). However, those requirements were not factored into our ratings across the three categories of reporting because our scope for this engagement was limited to regulations, along with limited reference to supporting materials. Laws incorporated by reference were considered out of scope.

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

Enclosure II: Federal Cybersecurity Regulations by Sector

Table 1: Summary Table of Total Federal Regulations with Cybersecurity Reporting Requirements by Sector

Sector	Total regulations	Cybersecurity incidents	Cybersecurity plans or other technical information	Reviews, audits, or assessments
Communications	8	1	5	2
Financial Services	19	15	8	2
Energy	19	2	5	1
Healthcare and Public Health	17	4	12	8
Information Technology	15	7	8	4
Nuclear Reactors, Materials, and Waste	3	1	3	1
Defense Industrial Base	5	3	2	2

Sector	Total regulations	Cybersecurity incidents	Cybersecurity plans or other technical information	Reviews, audits, or assessments
Transportation Systems	22	11	7	4
Food and Agriculture	1	0	0	0
Multiple Sectors[a]	4	2	0	1
All Sectors	4	2	2	0
Total	**117**	**48**	**52**	**25**

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

Note: We identified a total of 119 cybersecurity regulations, including 117 established and two proposed. From the 117 established regulations, we identified the total number of regulations that met each of the three types of reporting. Totals represent regulations that have each type of reporting requirement. Regulations may be counted in more than one column. Totals across the three types may be less than total number of regulations due to the lack of reporting requirements. We did not include proposed regulations in our totals of the three types of reporting requirements.

[a]Multiple category includes regulations that apply to two critical infrastructure sectors. These regulations are among the following sectors: Defense Industrial Base, Information Technology, Financial Services, and Food and Agriculture.

Table 2: Communications Sector Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Federal Communications Commission	47 CFR Part 1: Practice and Procedure (§1.50004)	No	Yes	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Federal Communications Commission	FR ID 309226: Modernization of the Nation's Alerting Systems[a]	No	No	No
Federal Communications Commission	47 CFR Part 15: Radio Frequency Devices (§15.407, §15.709, §15.713)	No	Yes	No
Federal Communications Commission	47 CFR Part 27: Miscellaneous Wireless Communications Services (§27.1414)	No	No	Yes
Federal Communications Commission	47 CFR Part 4: Disruptions to Communications (§ 4.2)	No	No	No
Federal Communications Commission	47 CFR Part 54: Universal Service (§54.308(g)-(h), §54.1022)	No	Yes	Yes
Federal Communications Commission	47 CFR Part 64: Miscellaneous Rules Relating to Common Carriers (§64.2010, §64.2011)	Yes	No	No
Federal Communications Commission	47 CFR Part 96: Citizens Broadband Radio Service (§96.39(g))	No	Yes	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Federal Communications Commission	FCC-25-49: Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks[b]	No	Yes	No

Source: GAO analysis of Federal Cybersecurity Regulations.| GAO-26-108606

[a]This proposed regulation is pending closure and may not be finalized. According to Federal Communications Commission (FCC) officials, FCC adopted an order that rejected the proposed regulation on June 25, 2026.
[b]According to FCC officials, FCC adopted regulation FCC-26-42 on June 25, 2026, which expands upon the cybersecurity reporting requirements in FCC-25-49 to include, among other updates, a standard related to cyber incident reporting.

Table 3: Defense Industrial Base Sector Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Department of Defense	32 CFR Part 117: National Industrial Security Program Operating Manual (§117.8, §117.12, §117.23, §117.18)	Yes	Yes	No
Department of Defense	32 CFR Part 170: Cybersecurity Maturity Model Certification (CMMC) Program (§170.5, § 170.7, §170.15-170.18, §170.20, §170.22, §170.21)	No	No	Yes
Department of Defense	32 CFR Part 236: Department of Defense, Defense Industrial Base Cybersecurity Activities (§236.4, §236.5, §236.7)	Yes	No	No

Department of Defense	48 CFR Part 252: Solicitation Provisions and Contract Clauses[a] (§§252.204-7008-252.204-7010, §252.204-7012, §252.204-7019, §252.204-7020, §252.239-7010, §252.239-7016)	Yes	Yes	Yes
Information Security Oversight Office	32 CFR Part 2004: National Industrial Security Program (§2004.24, §2004.26)	No	No	No

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

[a]As of June 2026, the Federal Acquisition Regulation (FAR) is currently undergoing substantial revisions. Current CFR sections from Title 48 may not be relevant, which could affect their applicability.

Table 4: Energy Sector Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Department of Energy	Form DOE-417: Electric Emergency Incident and Disturbance Report[a]	Yes	No	No
Federal Energy Regulatory Commission	18 CFR Part 12: Safety of Water Power Projects and Project Works (§12.10)	No	Yes	No
Federal Energy Regulatory Commission	18 CFR Part 284: Certain Sales and Transportation of Natural Gas Under the Natural Gas Policy Act of 1978 and Related Authorities (§284.12)	No	No	No
Federal Energy Regulatory Commission	18 CFR Part 35: Filing of Rate Schedules and Tariffs (Subpart K - Cybersecurity Investment Provisions)	No	Yes	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Federal Energy Regulatory Commission	18 CFR Part 38: Standards for Public Utility Business Operations and Communications	No	No	No
Federal Energy Regulatory Commission	18 CFR Part 39: Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards (§39.7)	No	Yes	No
Federal Energy Regulatory Commission	CIP-002-5.1a: Cyber Security -- BES Cyber System Categorization	No	No	No
Federal Energy Regulatory Commission	CIP-003-9: Cyber Security – Security Management Controls	No	No	No
Federal Energy Regulatory Commission	CIP-004-7: Cyber Security -- Personnel & Training	No	No	No
Federal Energy Regulatory Commission	CIP-005-7: Cyber Security Electronic Security Perimeter(s)	No	No	No
Federal Energy Regulatory Commission	CIP-006-6: Cyber Security -- Physical Security of BES Cyber Systems	No	No	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Federal Energy Regulatory Commission	CIP-007-6: Cyber Security -- System Security Management	No	No	No
Federal Energy Regulatory Commission	CIP-008-6: Cyber Security – Incident Reporting and Response Planning	Yes	Yes	No
Federal Energy Regulatory Commission	CIP-009-6: Cyber Security -- Recovery Plans for BES Cyber Systems	No	No	No
Federal Energy Regulatory Commission	CIP-010-4: Cyber Security — Configuration Change Management and Vulnerability Assessments	No	No	No
Federal Energy Regulatory Commission	CIP-011-3: Cyber Security — Information Protection	No	No	No
Federal Energy Regulatory Commission	CIP-012-1: Cyber Security – Communications between Control Centers[b]	No	No	No
Federal Energy Regulatory Commission	CIP-013-2: Cyber Security - Supply Chain Risk Management	No	No	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Rural Utilities Service	7 CFR Part 1730: Electric System Operations and Maintenance	No	Yes	Yes

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

[a]Although not a regulation, it is mandatory by Section 13(b) of the Federal Energy Administration Act of 1974 (Public Law 93-275) under certain circumstances.
[b]Expired on June 30, 2026.

Table 5: Financial Services Sector Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Commodity Futures Trading Commission	17 CFR Part 37: Swap Execution Facilities (Subpart O – System Safeguards)	Yes	Yes	No
Commodity Futures Trading Commission	17 CFR Part 38: Designated Contract Markets (Subpart U – System Safeguards)	Yes	Yes	No
Commodity Futures Trading Commission	17 CFR Part 39: Derivatives Clearing Organizations (§39.13, §39.18)	Yes	Yes	No
Commodity Futures Trading Commission	17 CFR Part 49: Swap Data Repositories (§49.24, §49.26, Appendix A to Part 49 – Form SDR)	Yes	Yes	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Department of Justice	28 CFR Part 202: Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (Subpart J - Due Diligence and Audit Requirements)	No	Yes	No
Department of the Treasury	31 CFR Part 1010: General Provisions (§1010.955, §1010.540)	No	Yes	No
Department of the Treasury	31 CFR Part 1020: Rules for Banks[a]	Yes	No	No
Federal Deposit Insurance Corporation	12 CFR Part 304: Forms, Instructions, and Reports (Subpart C - Computer-Security Incident Notification Rule)	Yes	No	No
Federal Deposit Insurance Corporation	12 CFR Part 364: Standards for Safety and Soundness (Appendix A - Interagency Guidelines Establishing Standards for Safety and Soundness, Appendix B - Interagency Guidelines Establishing Information Security Standards)	Yes	No	No
Federal Reserve Board	12 CFR Part 225: Bank Holding Companies and Change in Bank Control (Regulation Y) (Appendix F - Interagency Guidelines Establishing Information Security Standards, Subpart N - Computer-Security Incident Notification Rule)	Yes	No	No
Federal Reserve Board	12 CFR Part 234: Designated Financial Market Utilities Regulation HH (§234.3(a)(17)(vi))	Yes	No	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Federal Reserve Board	12 CFR Part 235: Debit Card Interchange Fees and Routing (Regulation II) (Paragraph 4(b)(2)(iv))	No	No	No
Federal Trade Commission	16 CFR Part 314: Standards for Safeguarding Customer Information	Yes	No	No
National Credit Union Administration	12 CFR Part 712: Credit Union Service Organizations (§712.3(d)(5)(ii))	No	Yes	No
National Credit Union Administration	12 CFR Part 748: Security Program, Suspicious Transactions, Catastrophic Acts, Cyber Incidents, and Bank Secrecy Act Compliance	Yes	No	Yes
Office of the Comptroller of the Currency	12 CFR Part 30: Safety and Soundness Standards	Yes	No	No
Office of the Comptroller of the Currency	12 CFR Part 53: Computer-Security Incident Notification Rule	Yes	No	No
Securities and Exchange Commission	17 CFR Part 242: Regulations M, SHO, ATS, AC, NMS, SE, and SBSR, and Customer Margin Requirements for Security Futures (Regulation SCI—Systems Compliance and Integrity)	Yes	Yes	Yes

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Securities and Exchange Commission	17 CFR Part 248: Regulations S-P,S-AM, and S-ID (Subpart A Regulation S-P: Privacy of Consumer Financial Information ("Reg. S-P"); Subpart C Regulation S-ID: Identity Theft Red Flags (Reg. S-ID); Appendix A to Subpart C of Part 248—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation)	Yes	No	No

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

[a]Department of the Treasury issued the Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (FIN-2016-A005) to clarify Suspicious Activity Report (SAR) obligations.

Table 6: Food and Agriculture and Healthcare and Public Health Sectors Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
National Oceanic and Atmospheric Administration	50 CFR Part 660: Fisheries of West Coast States[a] (§660.603)	No	No	No
Centers for Medicare and Medicaid Services	42 CFR Part 422: Medicare Advantage Program (§422.119, §422.120, §422.504)	No	No	No
Centers for Medicare and	42 CFR Part 495: Standards for the Electronic Health Record Technology Incentive Program[b]	No	No	Yes

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Medicaid Services				
Centers for Medicare and Medicaid Services	42 CFR Part 512: Standard Provisions for Mandatory Innovation Center Models and Specific Provisions for Certain Models (§512.760, §512.440, §512.740, §512.562)	Yes	Yes	Yes
Department of Health and Human Services	45 CFR Part 156: Health Insurance Issuer Standards Under the Affordable Care Act, Including Standards Related to Exchanges (§156.221, §156.715, §156.1105)	No	Yes	No
Department of Health and Human Services	45 CFR Part 164: Security and Privacy (Subpart C: Security Standards for the protection of Electronic Health Information; Subpart D: Notification in the case of Breach of Unsecured Protected Health Information; Subpart E: Privacy of Individually Identifiable Health Information)	Yes	No	No
Department of Health and Human Services	45 CFR Part 170: Health Information Technology Standards, Implementation Specifications, and Certification Criteria and Certification Programs for Health Information Technology (§170.202, §170.205, §170.210, §170.315, §170.403, §170.523, §170.550)	No	Yes	No
Department of Health and Human Services	45 CFR Part 172: Trusted Exchange Framework and Common Agreement (§172.201, §172.202, §172.301, §172.302)	No	Yes	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Drug Enforcement Agency	21 CFR Part 1311: Requirements for Electronic Orders and Prescriptions (§1311.25, §1311.30, §1311.55, §1311.105, §1311.110, §1311.115, §1311.116, §1311.120, §1311.150, §1311.300, §1311.302)	Yes	Yes	Yes
Federal Trade Commission	16 CFR Part 318: Health Breach Notification Rule	Yes	No	No
Food and Drug Administration	21 CFR Part 864: Hematology and Pathology Devices (§864.3750, Paragraph (b)(3)(F))	No	Yes	No
Food and Drug Administration	21 CFR Part 866: Immunology and Microbiology Devices (§§866.3172-866.3174, §866.3981, §866.5960, §866.6000)	No	Yes	Yes
Food and Drug Administration	21 CFR Part 870: Cardiovascular Devices (§870.1415, §870.2785, §870.2786)	No	Yes	Yes
Food and Drug Administration	21 CFR Part 878: General and Plastic Surgery Devices (§878.4961)	No	No	Yes
Food and Drug Administration	21 CFR Part 882: Neurological Devices (§882.1491, §822.5889)	No	Yes	Yes
Food and Drug Administration	21 CFR Part 884: Obstetrical and Gynecological Devices (§884.5370)	No	Yes	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Food and Drug Administration	21 CFR Part 886: Ophthalmic Devices (§886.1100)	No	Yes	No
Food and Drug Administration	21 CFR Part 892: Radiology Devices (§892.2060, §892.2070, §892.2090)	No	Yes	Yes

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

[a]This regulation is associated with the Food and Agriculture sector.

[b]The program that it governs has been superseded. Part 495 sets out reporting and other requirements for the Center for Medicare and Medicaid Services (CMS) Electronic Health Records (EHR) Meaningful Use (MU) Incentive program which is no longer in effect. Starting in 2011, the CMS MU program paid incentive payments to Medicare and Medicaid doctors and hospitals to adopt and use EHRs. The standalone incentive program was phased out over the years. Now, CMS still pays incentives to Medicare docs/hospitals for promoting interoperability (higher/better functionality usage of EHRs), but it's no longer a standalone program; it's been absorbed into a higher-level Medicare performance-based reimbursement program (related to EHRs/interoperability but also to other performance/patient measures). Some MU-related requirements have been incorporated into the current CMS "Promoting Interoperability" category of CMS's merit-based incentive payment system (MIPS) program Part 495 as it currently stands, is no longer applicable to current CMS programs.

Table 7: Information Technology Sector Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Department of Commerce	48 CFR Part 1352: Solicitation Provisions and Contract Clauses (§1352.239-72)	No	Yes	Yes
Department of Education	48 CFR Part 3404: Administrative and Information Matters (§3404.470-1, §3404.470, §3404.710)	Yes	No	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Department of Education	48 CFR Part 3439: Acquisition of Information Technology	Yes	Yes	Yes
Department of Housing and Urban Development	48 CFR Part 2439: Acquisition of Information Technology (§2439.107(b))	No	No	No
Department of Housing and Urban Development	48 CFR Part 2452: Solicitation Provisions and Contract Clauses (§2452.227-70, §2452.237-82, §2452.239-70)	Yes	Yes	No
Department of Justice	48 CFR Part 2839: Acquisition of Information Technology (§2839.102)	No	No	No
Department of State	48 CFR Part 639: Acquisition of Information Technology (§639.107-70)	No	No	No
Department of State	48 CFR Part 652: Solicitation Provisions and Contract Clauses (§652.239-70, §652.239-71)	No	Yes	Yes
Department of Transportation	48 CFR Part 1239: Acquisition of Information Technology (§1239.70, §1239.7202, §1239.7000, §1239.7002, §1239.7003, §1239.7102, §1239.7203, §1239.7204)	Yes	No	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Department of Transportation	48 CFR Part 1252: Solicitation Provisions and Contract Clauses (§§1252.239-70-1252.239-74)	Yes	Yes	Yes
Department of Veterans Affairs	48 CFR Part 804: Administrative and Information Matters (§804.1970)	Yes	Yes	No
Federal Communications Commission	47 CFR Part 8: Internet Transparency for Consumers (Subpart B - Cybersecurity Labeling Program for IoT Products)	No	Yes	No
National Aeronautics and Space Administration	48 CFR Part 1804: Administrative Matters (§1804.470-3)	No	No	No
National Aeronautics and Space Administration	48 CFR Part 1837: Service Contracting (§1837.203-70)	No	No	No
National Aeronautics and Space Administration	48 CFR Part 1852: Solicitation Provisions and Contract Clauses (§1852.204-76, §1852.223-75, §1852.237-72)	Yes	Yes	No

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

Note: As of June 2026, the Federal Acquisition Regulation (FAR) is currently undergoing substantial revisions. Current Code of Federal Regulations (CFR) sections from Title 48 may not be relevant, which could affect their applicability.

Table 8: Federal Cybersecurity Regulations and Reporting Requirements Applicable to All Sectors

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Bureau of Industry and Security	15 CFR Part 740: License Exceptions (§740.9)	No	No	No
Bureau of Industry and Security	15 CFR Part 748: Applications (Classification, Advisory, and License) and Documentation (Supplement 8: Information Required in Requests for VEU Authorization; Supplement 10: Data Center VEU Authorization Guidelines)	Yes	Yes	No
Cybersecurity and Infrastructure Security Agency	6 CFR Part 226: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements[a]	No	No	No
Office of Management and Budget	2 CFR Part 200: Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (§200.206, §200.303, §200.413)	No	No	No
Securities and Exchange Commission	88 FR 51896: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure[b]	Yes	Yes	No

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

[a]This regulation is proposed and has not yet been finalized.
[b]This final rule updates 17 CFR Parts 232, 240, and 249.

Table 9: Federal Cybersecurity Regulations and Reporting Requirements Applicable to Multiple Sectors

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Farm Credit Administration	12 CFR Part 609: Cyber Risk Management[a]	Yes	No	No
Department of Defense	48 CFR Part 204: Administrative and Information Matters[bc] (DFARS §240.370, §240.371)	Yes	No	Yes
Department of Defense	48 CFR Part 212: Acquisition of Commercial Products and Commercial Services[bd] (§212.205)	No	No	No
Department of Defense	48 CFR Part 239: Acquisition of Information Technology[be] (§239.7402, §239.7411, §239.7604, §239.7602)	No	No	No

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

[a]This regulation applies to the Food and Agriculture and Financial Services sectors.
[b]This regulation applies to the Defense Industrial Base and Information Technology sectors.
[c]As of June 2026, the Federal Acquisition Regulation (FAR) is currently undergoing substantial revisions. Current Code of Federal Regulations (CFR) sections from Title 48 may not be relevant, which could affect their applicability.
[d]As of June 2026, the FAR is currently undergoing substantial revisions. Current CFR sections from Title 48 may not be relevant, which could affect their applicability. Recently modified by Department of Defense, Class Deviation—Revolutionary Federal Acquisition Regulation (FAR) Overhaul Part 12, Defense FAR Supplement (DFARS) Part 212 Memo.
[e]As of June 2026, the FAR is currently undergoing substantial revisions. Current CFR sections from Title 48 may not be relevant, which could affect their applicability. Recently modified by Department of Defense, Class Deviation—Revolutionary Federal Acquisition Regulation (FAR) Overhaul Part 39, Defense FAR Supplement (DFARS) Part 239 Memo.

Table 10: Nuclear Reactors, Materials, and Waste Sector Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Nuclear Regulatory Commission	10 CFR Part 50: Domestic Licensing of Production and Utilization Facilities (§50.34, §50.54)	No	Yes	No
Nuclear Regulatory Commission	10 CFR Part 52: Licenses, Certifications, and Approvals for Nuclear Power Plans (§52.79)	No	Yes	Yes
Nuclear Regulatory Commission	10 CFR Part 73: Physical Protection of Plants and Materials (§73.54, §73.77, Subpart D: Protection of Safeguards Information)	Yes	Yes	No

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

Table 11: Transportation Systems Sector Federal Cybersecurity Regulations and Reporting Requirements

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Coast Guard	33 CFR Part 101: Maritime Security: General (§101.620, §101.625, §101.630, §101.635, §101.655, §101.650)	Yes	Yes	Yes
Coast Guard	33 CFR Part 160: Ports and Waterways Safety General (§160.216, §160.202)	Yes	No	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Coast Guard	33 CFR Part 6: Protection and Security of Vessels, Harbors, and Waterfront Facilities (§6.14, §6.16-1, §6.16-3)	Yes	No	No
Department of Homeland Security	19 CFR Part 111: Customs Brokers (§111.21, §111.25)	Yes	No	No
Department of Transportation	49 CFR Part 15: Protection of Sensitive Security Information (§15.9)	Yes	No	No
Federal Aviation Administration	AC 119-1A: Operational Authorization of Aircraft Network Security Program[a]	Yes	Yes	No
Federal Railroad Administration	49 CFR Part 214: Railroad Workplace Safety (§214.322)	No	No	No
Federal Railroad Administration	49 CFR Part 228: Passenger Train Employee Hours of Service; Recordkeeping and Reporting; Sleeping Quarters (§228.201, §228.203, Subpart D: Electronic Recordkeeping System and Automated Recordkeeping System)	No	No	No
Federal Railroad Administration	49 CFR Part 229: Railroad Locomotive Safety Standards (§229.136)	No	No	No
Federal Railroad Administration	49 CFR Part 237: Bridge Safety Standards (§237.155)	No	No	No

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Federal Railroad Administration	49 CFR Part 240: Qualification and Certification of Locomotive Engineers (§240.215)	No	No	No
Federal Railroad Administration	49 CFR Part 242: Qualification and Certification of Conductors (§242.203 (g))	No	No	No
Federal Railroad Administration	49 CFR Part 243: Training, Qualification, and Oversight for Safety-Related Railroad Employees (§243.203)	No	No	No
Federal Railroad Administration	49 CFR Part 245: Qualification and Certification of Dispatchers (§245.203 (g))	No	No	No
Federal Railroad Administration	49 CFR Part 246: Certification of Signal Employees (§246.203 (g))	No	No	No
Federal Railroad Administration	49 CFR Part 299: Texas Central Railroad High-Speed Rail Safety Standards (§299.449)	No	Yes	No
Transportation Security Administration	1580-21-01E: Security Directive Enhancing Rail Security	Yes	Yes	Yes
Transportation Security Administration	1582-21-01E: Enhancing Public Transportation and Passenger Railroad Cybersecurity	Yes	Yes	Yes

Agency	Regulation citation	Cybersecurity incidents?	Cybersecurity plans or other technical information?	Reviews, audits, or assessments?
Transportation Security Administration	49 CFR Part 1520: Protection of Sensitive Security Information (§1520.9)	Yes	No	No
Transportation Security Administration	49 CFR Part 1570: General Rules	Yes	Yes	No
Transportation Security Administration	EA23-01: Recommendation Regarding Emergency Action in Aviation	No	No	No
Transportation Security Administration	Pipeline-2021-01G : Security Directive Enhancing Pipeline Cybersecurity	Yes	Yes	Yes

Source: GAO analysis of Federal Cybersecurity Regulations. | GAO-26-108606

[a]This is not mandatory but may nonetheless be relevant because if an entity uses the means described in the Advisory Circular to obtain operational authorization, it must conform to it in totality.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on X, LinkedIn, Instagram, and YouTube. Subscribe to our Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/about/what-gao-does/fraudnet Automated answering system: (800) 424-5454
Media Relations	Sarah Kaczmarek, Managing Director, Media@gao.gov
Congressional Relations	David A. Powner, Acting Managing Director, CongRel@gao.gov
General Inquiries	https://www.gao.gov/about/contact-us