



TECHNICAL BRIEF · BASED ON GAO-26-109197 · GOVERNMENT-WIDE

SIX INDUSTRY PANELISTS TOLD GAO CYBER RULES DUPLICATE OR CONFLICT

6 panelists

INDUSTRY REPRESENTATIVES FROM THREE CRITICAL INFRASTRUCTURE SECTORS WHO
TOLD GAO ON JULY 16, 2026 THAT FEDERAL CYBER RULES DUPLICATE OR CONFLICT

In July 2026, six industry panelists from energy, financial services, and healthcare told GAO that federal cyber rules duplicate or conflict, with incident reporting timeframes among the examples. GAO made no recommendations, so the signal for a bid is what the panel asked for.

THE FINDING

On September 28, 2026, GAO published [Cybersecurity Regulations: Industry Panelists Identify Duplication and Conflicts and Ways to Address Them](#) (GAO-26-109197). It is the third GAO report in a series on industry views of cyber regulation, after panels reported in [July 2025](#) (GAO-25-108436) and [March 2026](#) (GAO-26-108685). This one summarizes a July 16, 2026 panel of six industry representatives from three critical infrastructure sectors: energy, financial services, and healthcare and public health.

The panelists identified federal cyber regulations in their sectors as duplicative or conflicting, which made it hard to meet reporting requirements while responding to a live threat. Two rules came up across sectors: DHS's proposed cyber incident reporting rule and the SEC's cyber disclosure rules. A few financial services participants set out the clocks side by side: 72 hours at NCUA, 24 to 72 hours under the proposed rule, four business days at the SEC.

Most participants said timeframes, thresholds, and definitions should be harmonized. Most also backed a model where one agency, such as CISA, receives incident reports and passes them to the others. GAO made no recommendations.

WHY IT KEEPS HAPPENING

The panel's account is that rules arrived one regulator at a time. Participants said thresholds, timelines, and definitions differ from rule to rule, so a single event can set off several reports with different deadlines and different content.

Some of the conflicts are not about timing. Panelists pointed to suspicious activity report confidentiality running into public disclosure under the SEC rules, HIPAA breach rules running against the proposed federal incident rule, and an energy-sector standard on safeguarding information that collides with incident reporting.

Nobody owns the seams. Most participants said a single entity with authority over regulatory consistency would help. Several agreed that federal progress on existing duplication and conflicts has been limited, though most saw some progress over the past year.

Read the panel for what it is. GAO drew its six participants from public comments, did not select them to be statistically representative, and says the summary does not reflect a unanimous view.

WHY IT MATTERS TO YOUR BID

No federal contractor sat on this panel, and the report says nothing about bids. The link is narrower. One energy participant listed the FAR, DFARS including the CMMC certification clause, and GSA's controlled unclassified information requirements among the overlapping rules, so contract requirements stack the same way regulations do. GAO also notes that, as of August 2026, the FAR was undergoing substantial revisions through deviations, so clause numbers can move under a proposal.

For a prime, the collision shows up in three kinds of requirements. Incident response plan deliverables must define what counts as reportable. Cloud and SaaS task orders carry notification terms between provider, prime, and agency. And systems a contractor operates for an agency fall under [FISMA's agency-wide information security program](#), which covers information systems operated "by a contractor of an agency."

An evaluator reading a technical volume looks for an offeror that knows its reporting duties. A single "we report within X hours" line, when the team also answers to other regimes, signals a scope the offeror has not mapped.

TECHNICAL APPROACH

The method below comes from Avalon's [FISMA, FedRAMP and NIST 800-53 Compliance Audits service](#), delivered against [NIST SP 800-53 Rev. 5](#) and the SP 800-53A assessment procedures. It describes how the work is done. Avalon does not assess a system whose plan it wrote, so it takes one role per system.

1. **Fix the scope in the assessment plan.** Confirm the boundary, the FIPS 199 categorization, the 800-53 release, and any overlays, and write them into the Security Assessment Plan, which is signed before fieldwork. Confirming the release at kickoff keeps findings from being relitigated at the outbrief.
2. **Test IR-8 and IR-6 as written.** IR-8 requires the incident response plan to define reportable incidents. IR-6 has two parameters: the time period in which personnel report to the incident response capability, and the authorities that receive incident information. NIST's own guidance says the types, timeliness, and authorities reflect applicable laws, directives, and regulations. The assessor examines the plan, the system security plan narrative, and past incident records, interviews the people who report, and tests the path.
3. **Compare the stated windows with the clocks the agency identifies.** The assessor records the IR-6 time period and reporting authorities the system security plan states, and compares them with the reporting clocks the agency or prime says apply. If one authority wants a report in 72 hours and the internal window leaves it no time, that is a finding. Each result carries its 800-53A procedure and evidence reference in the workpapers.
4. **Review the provider's side for cloud-bound systems.** In a package review, read the provider's package and customer responsibility matrix for who notifies whom and when. FedRAMP certification covers the provider's offering, not the agency's system, so the matrix shows what the agency still owns.
5. **Report conflicts as findings.** Each conflict between two reporting duties becomes a risk-rated finding in the Security Assessment Report (SAR), with a recommended corrective action and a POA&M input file. Which

rule governs is a decision for the agency's counsel, the contracting officer, and the Authorizing Official, not the assessor.

WHAT "FIXED" LOOKS LIKE

GAO has no closure evidence to cite because it made no recommendations. These are targets, built from what the panelists asked for and from what the assessment can show on a single system.

- Reporting timeframes, thresholds, and definitions that match across the rules a system answers to, which only rulemakers can deliver.
- A designated lead agency to receive and route incident reports, also a rulemaker's decision.
- At the system level, an IR-6 narrative that names every authority and its clock, and an internal reporting window shorter than the shortest of them.
- Every conflict the assessment finds carried in the POA&M with an owner and a decision date.

STATUS CHECK

OPEN GAO-26-109197 contains no recommendations, so there is no status to track. As of the report's September 2026 publication, GAO described DHS's incident reporting rule as proposed. This brief did not verify any later stage. The panel's view of progress, limited according to several participants, is opinion, not a GAO finding.

TEAMING FIT

NAICS	541519, 541512
AVALON'S SUB ROLE	Independent assessment of incident reporting controls (IR-6, IR-8) against the clocks a system answers to, a SAR with risk-rated findings, and POA&M input files, under the prime's authorization or compliance task
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151HACS Highly Adaptive Cybersecurity Services); GSA MAS (SIN 54151S IT Professional Services); GSA OASIS+

If incident response plans, contractor-operated systems, or a FISMA compliance audit are in your capture plan, Avalon teams as the sub that tests the incident reporting controls against the clocks the system answers to and hands the agency a risk-rated report and POA&M inputs it can act on.

BRANDON IRELAND, FOUNDER · CONTACT@AVALONTECHSERVICES.COM · AVALONTECHSERVICES.COM

This brief analyzes publicly released oversight reports. It does not describe work Avalon performed for any agency named.