This material from *The Government Contractor* has been reproduced with the permission of the publisher, Thomson Reuters. Further use without the permission of the publisher is prohibited. For further information or to subscribe, call 1-800-328-9352 or visit https://legal.thomsonreuters.com. For information on setting up a Westlaw alert to receive *The Government Contractor* in your inbox each week, call your law librarian or a Westlaw reference attorney (1-800-733-2889).

THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

NOVEMBER 4, 2026 | VOLUME 68 | ISSUE 41

¶ 263 FEATURE COMMENT: Cybersecurity In 2026: When CMMC Paused, DOJ Kept Playing

One of us loves listening to jazz, one is a drummer and musician, and one of us frequently uses jazz hands (we'll let the reader figure out who's who) . . . so between us, it was hard to look back at federal cybersecurity in 2026 without hearing a familiar sound: people working from the same chart, arguing over the tempo, and trying to figure out who is supposed to come in next.

The Government Contractor is not printed the week containing Veterans Day. The next issue will be dated November 18, 2026.

For the uninitiated, jazz isn't music without rules like many would have you believe. Listen to someone like Bill Evans at the piano, and you'll hear how much freedom can live inside a familiar song. The melody wanders, sure. The rhythm section sometimes answers in odd ways. But the tune doesn't cease to exist, does it? That was the very puzzle facing contractors this year. How do you keep playing when the bandleader walks off the stage mid-set and nobody tells you whether the gig is over?

This year, while the Pentagon put the next stage of Cybersecurity Maturity Model Certification (CMMC) on ice, the Justice Department found its tempo by bringing cases under the False Claims Act for failure to meet security obligations already written into contracts. The two 2026 settlements put numbers on that disconnect. LOGZONE, Inc. agreed to pay $507,144 for allegedly failing to implement required controls while giving itself a perfect score for cybersecurity. Honeywell Aerospace Inc. agreed to pay just over $2 million to resolve allegations involving security on a network supporting defense work. Not surprisingly, neither case needed CMMC Phase 2 to proceed. The DOJ band could keep jamming without the promised new conductor.

CMMC Missed Its Entrance. The Contract Kept Time—After years of buildup, CMMC finally appeared in defense contracts in November 2025. Phase 1 allowed contracting officers to require certain Level 1 and Level 2 self-assessments, with the related status records and affirmations. The next change, scheduled for Nov. 10, 2026, would have expanded mandatory third-party assessments.

Then came July 13.

The Pentagon suspended Phase 2 and ordered a 60-day review, citing burdens on smaller and newer suppliers. That was consequential news for companies trying to schedule and pay for assessments. It was not a cancellation of their existing security obligations. Phase 1 remained, Defense Federal Acquisition Regulation Supplement 252.204-7012 remained, and existing contract terms did not vanish just because the Pentagon announced a review.

At the same time, the FAR overhaul also changed the layout of some defense cyber rules during 2026. Under the Part 240 class deviations, the National Institute of Standards and Technology (NIST) assessment clause appeared as DFARS 252.240-7997 in applicable new solicitations, rather than the familiar 252.204-7020. But this change for new solicitations didn't change the terms of existing awards.

For contractors, the paperwork was already complicated enough. One award may use familiar DFARS assessment clauses, another may use the newer deviation language, and an older contract may still contain an unmodified CMMC provision. The operative requirements for each award aren't modified by somebody's upbeat take on the latest announcement. They are memorialized in each contract. Think of a Supplier Performance Risk System (SPRS) score as a tune on the album's tracklist, not a private rehearsal note. The Government expects to hear the tune it paid for. The score rests on a specific assessment, set of systems and supporting evidence. Whoever affirmed it ought to be able to explain all three.

One number still matters, and will continue to matter: 2017. DFARS 252.204-7012 required implementation of applicable NIST SP 800-171 protections by the end of 2017 along with its 72-hour incident-reporting requirement, subject to the clause's exceptions and approved alternatives. The CMMC pause didn't change those terms or erase scores already posted in SPRS. So while the Phase 2 review was welcome news to some contractors, it never meant they could stop checking to see whether sensitive data was actually protected.

DOJ Stayed on the Beat—If CMMC sounded uncertain in 2026, DOJ was locked in the pocket. In June, DOJ announced the LOGZONE settlement over alleged cyber failures on Navy contracts. The company's self-reported perfect score and the Government's negative-170 assessment were so far apart that the score itself became the story. No whistleblower was needed to bring the discrepancy to light. DOJ pursued enforcement under the FCA on its own initiative.

September brought Honeywell. The company agreed to pay $2,042,518 to resolve allegations involving NIST SP 800-171 requirements on a defense contract from April 2020 through December 2023. A former Honeywell employee filed a whistleblower suit under the FCA. DOJ intervened in part, on a theory turning on compliance with the terms of the contract, not an SPRS score, and Honeywell agreed to a settlement without admitting liability. The whistleblower was awarded $375,823 for her efforts.

Taken together, the cases show two ways a contractor can end up in trouble. A posted score may not survive an assessment. Or the Government may allege that the contract's promised protections were missing, score or no score. Because the claims were pursued by DOJ under the FCA, neither route was closed by the CMMC pause.

Cyber enforcement had been building momentum well before this year and DOJ delivered a strong setlist showing how costly the gap between documented compliance and actual security practices can become. DOJ announced its Civil Cyber-Fraud Initiative in 2021, promising to use the FCA to pursue Government contractors and grant recipients who put U.S. information or systems at risk by providing deficient cybersecurity products or services, misrepresenting their cybersecurity practices, or violating obligations to monitor and report cybersecurity incidents. DOJ reported more than $6.8 billion in FCA settlements and judgments for fiscal 2025, a record total across all kinds of cases, not a cyber-only figure.

That year saw MORSECORP, Inc. paying $4.6 million after leaving an inflated SPRS score in place despite an outside assessment revealing serious deficiencies; Georgia Tech Research Corp. set-

© 2026 Thomson Reuters

tling for $875,000 over allegations that its reported score did not reflect a properly defined assessment boundary; and Raytheon and Nightwing paying $8.4 million to resolve allegations involving inadequate security on a development system supporting 29 defense contracts and subcontracts. Aero Turbine, Inc. and its private equity owner took a different approach, voluntarily disclosing deficiencies and cooperating with DOJ before reaching a $1.75 million settlement, and Penn State's $1.25 million settlement in late 2024 raised similar concerns about corrective-action plans and cloud security. Although none of these settlements are trial verdicts, they show where DOJ has focused its attention: inaccurate assessments, poorly defined system boundaries, unaddressed security gaps, and representations that don't match reality. They also make clear that universities, subcontractors, and smaller suppliers face the same scrutiny as major defense contractors, and that voluntary disclosure and timely corrective action can matter when problems come to light.

A Good Score on the Wrong System—Imagine a company builds a secure enclave for Government work. It has the right tools, an attractive diagram, and a system security plan (SSP) that reads beautifully. Then an engineer sends project files through the company's ordinary email system, another uses a shared development machine, and a subcontractor stores a copy in its cloud service. The result is a stellar enclave with a completely inaccurate drawing.

DFARS 252.204-7012 defines a covered contractor information system by whether it processes, stores, or transmits covered defense information. That is a fact about the data and the system, not a label chosen for the SSP. CMMC's Level 2 scoping guidance recognizes "contractor risk managed assets," systems able to handle controlled unclassified information (CUI) but not intended to do so under company policies and practices. Those assets aren't simply invisible or automatically outside scope; they have to be documented, and an assessor may check them when the documentation or other findings raise questions. If CUI is actually moving through the system, its designation needs to be revisited.

There is a musical version of this problem. Guaraldi's recordings with Brazilian guitarist Bola Sete move comfortably between traditions, but the players are still listening to the same performance. Cybersecurity boundaries don't benefit from that kind of generous interpretation. If the work and data are elsewhere, an impeccable enclave assessment can't stand in for them. The system in the report must be the system doing the work.

One of the largest issues most third-party assessors will tell you about is that scoping tends to drift. An enclave created for one program later supports a second program. A subcontractor is given access for a short task, and nobody closes it when the task ends. A reorganization or acquisition adds identities and systems. A vendor changes how a service is hosted. Engineers move files to a development platform to meet a deadline. Each change can affect the actual footprint of covered data without triggering a corresponding rewrite of the SSP. An annual review that checks only whether the same diagram is still on file will miss that drift.

The Moment the Problem Becomes More Than Technical—Now, just to be clear (and calm some nerves), a missed control in and of itself isn't automatically an FCA case. Liability requires a little bit more and depends on the legal elements, including knowledge and materiality. But the difference between a fixable security problem and a difficult fraud investigation often shows up in an ordinary email, like someone explaining that the picture was wrong, and the company kept using it anyway. MORSE's old score illustrates the point almost to the "T." A consultant reaches a new conclusion, but the company leaves the earlier statement in place. It's one thing to learn that a control is missing; it's another thing altogether to keep describing the environment as if nobody had learned it.

A record that shows a known deficiency followed by an unchanged representation is what the public settlements have in common. A company can make legitimate choices about costs and priorities, and a spending decision is not a false statement. The exposure is the representation that stayed in place.

The newly unsealed *Tenney* complaint gives Honeywell's story a human voice. Former Honey-

© 2026 Thomson Reuters

well project management specialist Rachel Tenney alleged that the company protected commercial operations more aggressively than the Gray Network supporting sensitive Government quantum computing work. She also challenged the company's response to suspicious activity tied to the SolarWinds episode. In the complaint's account, the disagreement wasn't simply over software. It was over what people knew, what they were prepared to investigate, and what they would tell the Government. Those are allegations, not conclusions established by the settlement.

Art Pepper could make one saxophone sound unmistakably personal even in a crowded band. An internal security objection can be just as hard to ignore once it is in writing. According to her complaint, Tenney was later removed from the work, and she eventually filed suit. Several of the other cyber cases also began with people close to the systems. A technical warning deserves a documented answer, not a reflexive personnel solution. Separately, DFARS 252.204-7012 starts a 72-hour clock on discovery of a reportable cyber incident. Not every alert qualifies, but a company should be able to show how it reached its decision. The question isn't "Could we explain this today?" It's "Could we show, from records made at the time, what we knew and why we acted, or didn't?"

A good investigation separates three questions that often get mixed together. What did the contract require at the relevant time? What was technically true about the systems and data? What did the company tell the Government or an assessor? When those answers don't line up, the mismatch is the reason to investigate thoroughly. Dates and supporting records matter more than confident after-the-fact summaries.

What an Investigation Actually Sounds Like—McCoy Tyner's playing could be powerful without losing its harmonic center. An investigation needs that kind of steadiness. Its work is less glamorous than a courtroom drama: compare what the contract required, what the systems did, and what the company said about them, then put dates next to the answers.

The SPRS record shows what the contractor reported and when. Technical reports show whether its people later reached a different conclusion. The SSP and assessment boundary show which assets were included and which were left out. Contract files show which obligations applied at the time. Invoices show what the Government paid after a concern emerged.

An accurate chronology also includes budget decisions, postponed fixes, rejected recommendations, and incident-response records. Those documents can support the company just as much as they can hurt it, if they show a serious investigation and prompt action. A record with no dated decisions leaves far more room for competing stories. Everyone in the loop about any discrepancies has a financial incentive to go to the Government when the company fails to take appropriate action.

The number of affected contracts matters. A shared service may support dozens of awards. Raytheon's 2025 settlement involved 29 contracts and subcontracts. Penn State's involved Department of Defense and NASA work. One technical environment can touch several COs, more than one inspector general and a collection of primes or subcontractors. A single companywide score does not mean the same clauses apply to every award.

For a company contracting with multiple agencies, the contract map is a business continuity tool as well as a legal document. It identifies where the questionable system was used, which COs may have to be told, whether option decisions are approaching, and which prime contractors may need separate notice. That is far more precise than treating the full federal portfolio as tainted, or assuming a flaw on a single project cannot matter elsewhere.

That last distinction is critical. The company needs a contract map based on the actual clauses and modifications, not broad assumptions from award year or agency. A statement about an SPRS score may be relevant to some contracts and irrelevant to others. Scope the possible claims as carefully as the network.

Coming Clean Without Losing Track of the Form—FAR 52.203-13, when applicable, requires timely written disclosure to the agency IG, with a

© 2026 Thomson Reuters

copy to the CO, when the contractor has credible evidence of specified federal criminal violations or a civil FCA violation connected to contract work. The clause does not impose that duty for every technical deficiency. The facts need investigation, and the trigger is credible evidence of a covered violation.

The clause is also more flexible about multiple contracts than it may first appear. Its internal-control provision allows a disclosure involving more than one federal contract to go to the OIG and CO responsible for the largest-dollar affected contract. For certain orders placed through Governmentwide, multi-agency or schedule vehicles, it specifically calls for notifying both the ordering agency's IG and the IG responsible for the underlying contract, along with the relevant COs. Those rules make the ordering vehicle and the exact clause language important. The routing provision narrows the recipients, not the contracts a disclosure must cover.

DOJ is playing on another stage. Its policies recognize voluntary disclosure, cooperation and remediation when considering appropriate credit. A mandatory inspector-general disclosure is not a voluntary self-disclosure to DOJ, and talking with DOJ does not replace what a contract clause requires. There is no rule that every company should notify every possible office at precisely the same moment. The facts and the applicable clauses determine the path.

Verizon, which self-disclosed shortfalls in its trusted internet connection service and received cooperation credit in a 2023 settlement, and Aero Turbine show the value of getting ahead of an issue. They do not promise the same outcome for every company. A disclosure can still bring an investigation and a settlement. Waiting until every technical problem is fixed can be equally risky if the duty to disclose has already arisen. Experienced counsel should help determine the trigger, recipients, and timing while the company keeps remediation moving.

Coordination matters even when notification obligations differ. An agency OIG, CO, and DOJ lawyer should not receive inconsistent versions of the same factual story. Contract-specific details can vary; the underlying chronology should not.

In practice, that calls for one verified set of underlying facts and a separate routing plan for each required notice. The plan should identify the agency, contract, clause, recipient and deadline rationale. It should also show what remains unknown. COs can make their own decisions on administration and future awards, while DOJ evaluates civil fraud exposure. One office's reassurance should not be treated as a release binding every other office.

The strongest voluntary-disclosure record is not a polished apology. It is evidence that the business recognized a concern, tested it, stopped any ongoing misstatement, protected relevant information and did useful repair work. None of those actions guarantees credit. They make it easier to show what the company actually did instead of relying on assurances about its intentions.

The Settlement Is Not the Whole Bill—Civil penalties and damages can be substantial, and an FCA case can involve many claims for payment. The publicly announced settlement is only the visible portion of the business impact. Companies may also face investigation costs, technical remediation, strained customer relationships, disputes with primes and harder questions during renewals or acquisitions.

Suspension and debarment deserve particular attention. A settlement does not automatically exclude a contractor, but the Government can separately examine present responsibility. FAR 9.406-1 directs attention to matters such as voluntary reporting, cooperation and corrective measures. The company's record after discovering a problem may matter as much to future business as the cash payment.

The reputational bill can be harder to count. A prime may need assurances before letting a supplier continue to handle information. An acquirer may ask whether old scores covered all the systems behind the revenue it is buying. A CO may request a detailed corrective-action history. Those questions arrive even where the Government has not made a finding of fraud. Clear records make them answerable without reinventing the story every time.

Executives are not outside the frame, either. Civil

© 2026 Thomson Reuters

liability can extend to individuals who knowingly cause false claims, depending on the facts. Criminal liability under federal false-claim and false-statement laws has separate requirements, and these civil settlements should not be described as criminal prosecutions. The concern is a deliberate false statement or claim, not a disagreement over priorities.

DOJ also revised its Justice Manual in September 2026 to emphasize that sub-regulatory guidance alone cannot create new legal duties. That is an important reminder to distinguish binding contract language and regulations from explanatory agency guidance. It does not erase duties a contractor actually accepted in its award.

Before the Next Chorus—Start with the record the Government can already see. Pull the company's SPRS history, the underlying assessments and the affirmations. Match them to the systems and CAGE codes they covered. If an old number no longer reflects what the company knows, determine whether a correction is needed and document why, or why not. Then test the real boundary. Trace where covered defense information is stored, processed and transmitted. Include email, cloud services, developer tools and subcontractor handoffs. Compare that map against the SSP and any CMMC assessment scope. Confirm the contractual basis for external cloud security claims rather than relying on a sales sheet.

Build a clause-by-clause picture of the affected awards. Capture the relevant versions of DFARS 252.204-7012, assessment provisions, CMMC clauses and FAR 52.203-13 where they appear. Do not assume every contract in a portfolio contains the same text or the same disclosure terms.

Give internal warnings a formal route to resolution. Preserve the evidence before changing the environment, including logs needed to assess a possible incident. Record what was found, who reviewed it and what the company decided. Fix the controls that can be fixed now. Keep dated evidence of work that is still in progress.

If credible evidence of a covered legal violation emerges, make the disclosure decision promptly with counsel. Identify the contract-specific recipients. Decide separately whether to approach DOJ. Be clear about what is known, what remains under investigation and how the company is addressing the problem. Do not present incomplete work as finished.

There is a temptation to wait for Washington to finish rewriting the chart. But a contractor cannot control when the Pentagon restarts its assessment program, when an employee calls an IG, or when an assessor asks to see the basis for an old score. It can control whether the score reflects the actual systems, whether people raising concerns get serious answers, and whether the records show what happened next.

Sonny Rollins could turn a familiar melody inside out and still leave listeners knowing exactly what song they were hearing. That sort of freedom comes from knowing the music. Federal contractors will need to keep improvising as cybersecurity rules and assessment programs change. There is room for judgment in how to meet an obligation. There is much less room for invention in describing whether it has been met. Jazz can reward a daring departure from the tune. The FCA is not so forgiving.

♦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by **Alex Major, Zachary A. Myers,** ***and*** **Franklin Turner.** ***Mr. Major and Mr. Turner are partners and Co-Chairs of the Government Contracts & Global Trade practice at McCarter & English, LLP, in Washington, D.C. Mr. Myers is a partner and Co-Leader of the Cybersecurity & Data Privacy Group at McCarter & English, LLP, in Indianapolis, Ind., and former U.S. Attorney for the Southern District of Indiana.***

© 2026 Thomson Reuters