



The 10 Factors That Could Make or Break Your Next DOJ Investigation

On October 1, 2026, Assistant Attorney General Colin M. McDonald did something unusual – he handed government contractors a cheat sheet.

Directive 26-12, [Corporate Enforcement in the Fight Against Fraud](#), issued by the U.S. Department of Justice's (DOJ) National Fraud Enforcement Division (the Fraud Division), lays out in plain language 10 factors on which prosecutors "must place great weight" in deciding whether to bring charges against a company and in negotiating plea or other agreements.

Procurement and government-contract fraud is one of four named priorities, alongside health care fraud, tax and other significant revenue evasion, and tariff and trade fraud. Prosecutors are told to bring an "aggressive, all-tools approach" to each.

For government contractors, this is not just another policy memo to skim and file. The 10 factors function as a *de facto* scoring rubric for enforcement risk. Read them carefully, and you have a roadmap for an internal compliance audit that mirrors what a Fraud Division prosecutor will be looking for.

One scope note: the directive governs matters supervised by the Fraud Division. It does not extend to cases handled by a U.S. Attorney's Office that are not also supervised by the Fraud Division, although the Corporate Enforcement Section may assist U.S. Attorneys if helpful.

Here is what each factor means in practice and how it should shape in-house compliance programs.

Factor 1: Management Knowledge or Involvement

The directive places “knowledge of or involvement in fraud scheme by corporate management” at the top of the list.

Management complicity has always mattered under the Justice Manual’s Principles of Federal Prosecution of Business Organizations (§ 9-28.000). Directive 26-12 moves it from one consideration among many to the first factor prosecutors must weigh heavily.

Real-World Examples for Contractors: A program manager knows a subcontractor is not performing to specification but signs off on the deliverable anyway. A vice president directs staff to submit inflated cost estimates on a cost-reimbursable contract. A CEO is aware of cybersecurity deficiencies but approves the National Institute of Standards and Technology Special Publication 800-171 self-assessment score without correction.

The higher up the chain the knowledge goes, the worse the outcome. Contractors should ensure that compliance reporting lines reach senior leadership, and that senior leadership is trained to understand that willful ignorance is not a defense.

Factor 2: Concealment from Government Agencies or Auditors

Prosecutors must weigh “efforts to conceal fraud from government agencies or auditors or otherwise impede or obstruct a government function or oversight.”

Defense contractors live under continuous oversight from the Defense Contract Audit Agency (DCAA), the Defense Contract Management Agency (DCMA), contracting officers, and inspectors general.

Practical Application: Providing incomplete or misleading responses to a DCAA incurred-cost audit. Failing to disclose a known defect during a DCMA surveillance visit. Sanitizing internal emails before producing them in response to a contracting officer’s request for information.

Each of these scenarios transforms a potential billing dispute into something far more serious – an obstruction narrative that prosecutors will use to justify criminal

charges rather than a civil settlement under the False Claims Act (FCA), 31 U.S.C. §§ 3729–3733.

Factor 3: Schemes Lasting Three Years or More

“Conduct that furthers the scheme lasting three years or more” is a duration marker that DOJ is now treating as an aggravating circumstance.

This factor is particularly relevant for government contractors because many federal contracts, especially indefinite-delivery / indefinite-quantity vehicles and multiyear defense programs, run for five, seven, or even 10 years. On a long-running contract, a problem left uncorrected for three years can easily become a “scheme lasting three years or more” in a prosecutor’s telling.

The Lesson: Contractors cannot treat compliance as a one-time exercise at contract award. Ongoing monitoring, periodic internal audits, and refreshed risk assessments are the only way to keep a year one problem from becoming a year four aggravating factor.

Factor 4: Threats to Safety or Security, Including Military Readiness

Of all 10, this factor (“actions that threaten the safety or security of Americans, including military readiness”) is the one that should keep defense contractors up at night.

It has no analog in commercial contract disputes. A defective part that causes a warranty claim in the private sector becomes a national security issue when it is installed on a weapons system or used to support deployed troops.

Best Practices to Mitigate Risk: Contractors can mitigate risk by identifying red flags, such as improper product substitutions or fraudulent maintenance logs.

These fact patterns have driven some of DOJ’s most aggressive procurement prosecutions of the past decade. Under the directive, prosecutors will ask not just how much a fraud cost, but whether it put Americans’ safety or military readiness at risk. A robust culture of compliance is necessary to avoid these scenarios – or neutralize them if they arise.

Factor 5: Substantial Financial Hardship to a Government Program

“Conduct that causes substantial financial hardship to a taxpayer-funded program or government function” targets frauds that drain agency budgets: overbilling on cost-type contracts, mischarging labor hours, or inflating indirect cost rates in ways that ripple across an agency’s entire contract portfolio.

For contractors on cost-reimbursable vehicles, this factor is a reminder that the government’s financial exposure is essentially unlimited until final audit and closeout. A pattern of excessive or unallowable costs charged to a single program can trigger this factor even if the dollar amount, standing alone, seems moderate. The question is whether fraud meaningfully impaired the program’s ability to accomplish its mission.

Factor 6: Conduct Affecting Multiple Government Programs

Where Factor 5 focuses on depth of harm, Factor 6 targets breadth: “conduct that affects multiple taxpayer-funded programs or government functions.”

A contractor that submits false certifications across multiple contract vehicles (say, inaccurate cost or pricing data on three separate negotiated procurements, or false small business representations on awards from multiple agencies) is squarely in the crosshairs.

This factor also has implications for companies that provide shared services across contracts. If a deficient accounting system or flawed timekeeping practice affects billing under contracts with the U.S. Department of Defense, NASA, and a civilian agency, the multi-program impact alone will push the case up the enforcement priority ladder.

Factor 7: Conduct Spanning Three or More Federal Districts

Geographic reach, or “conduct that affects three federal districts or more,” is a scale indicator.

For large contractors, this factor is easy to reach. For a company headquartered in Virginia, administering a contract out of Alabama, with subcontractors in California,

almost any billing misconduct will affect at least three districts.

The practical significance is less about the geography itself and more about what it signals to prosecutors: a fraud that crosses district lines suggests organizational scope, not a one-off mistake by a single employee in a single office. It also gives DOJ flexibility in choosing where to bring charges, which can have significant strategic implications for the defense.

Factor 8: Financial Harm to 25 or More Victims or \$25 Million or More in Loss

This is the directive's clearest quantitative marker: "conduct that results in financial harm to 25 or more victims or \$25 million or more in loss."

For contractors, "victims" can include not just the contracting agency but also subcontractors, end users, and other contractors who lost competitive opportunities due to fraud. Set-aside fraud is a good example: when a company fraudulently claims small business status, the "victims" include every legitimate small business that lost a contract award.

Importantly, these numerical markers are weighting factors, not minimum thresholds, and the directive describes all 10 factors as a non-exhaustive list. Fraud involving fewer victims or less than \$25 million in loss is still prosecutable. But clearing this bar signals to prosecutors that a case warrants the Fraud Division's full attention and resources.

Factor 9: Exfiltration of Dollars to Foreign Adversaries

"Conduct that involves the exfiltration of American dollars to support foreign adversaries" reflects the administration's broader national security priorities.

Export controls, International Traffic in Arms Regulations, and supply chain integrity are where this factor bites. A contractor that funnels contract proceeds to an entity in a sanctioned country, or that uses a foreign subcontractor with undisclosed ties to a foreign government, could trigger this factor even if the underlying fraud would otherwise be treated as a garden-variety billing dispute.

Practical Takeaway: Diligence on foreign subcontractors and suppliers, including ownership, government ties, and payment flows, is now a fraud-risk control, not just an export-compliance exercise.

Factor 10: Immigration Offenses

The final factor, “conduct that involves immigration offenses,” is the most overtly policy-driven on the list.

Expect this to surface in workforce and clearance compliance: companies that use unauthorized workers on federal contracts, or that misrepresent the citizenship or clearance status of personnel performing on classified or sensitive programs. While this factor may seem peripheral to procurement fraud, its inclusion signals that prosecutors will look for immigration-related aggravators as a matter of course. Contractors should confirm that I-9 practices, subcontractor workforce certifications, and clearance representations would withstand scrutiny.

Your Score Is Not Final

The 10 factors set the severity score. Self-disclosure, cooperation, and remediation can still change the outcome. The directive expressly requires that “[i]n all circumstances,” prosecutors “follow and implement the [Corporate Enforcement Policy] CEP,” the department-wide Corporate Enforcement and Voluntary Self-Disclosure Policy.

Companies that uncover potential fraud and disclose it voluntarily, cooperate fully, and remediate the underlying problem can still earn significant credit, up to and including a declination of prosecution under the CEP framework.

This is the directive’s escape hatch. The 10 factors tell you how prosecutors will evaluate the severity of the misconduct. The CEP tells you how prosecutors will evaluate your response to the misconduct. A company that discovers a three-year billing fraud involving management knowledge but self-discloses promptly, cooperates meaningfully, and remediates effectively is in a fundamentally different position than a company that conceals the same facts and waits for a whistleblower to call DOJ.

The Institutional Infrastructure Behind the Factors

The 10 factors do not operate in a vacuum. Directive 26-12 also puts the Fraud Division's Corporate Enforcement Section (CES) at the center of corporate enforcement. Prosecutors must work with the CES at all phases of corporate investigations, report any ongoing corporate investigations to the CES Chief within seven days of the directive's issuance, and promptly notify the CES of new corporate investigations and major developments.

The CES will also have primary responsibility for evaluating compliance with corporate criminal resolutions, including whether companies are actually implementing or enhancing the compliance programs they promised and meeting their reporting obligations.

Meanwhile, the directive instructs division leadership to "design and implement policies and programs that appropriately incentivize whistleblowers to bring forward credible information pertaining to fraud," and states that the division's policies must encourage and protect disclosures by whistleblowers, "including by those who participated in the criminal conduct."

The details of these whistleblower programs have not yet been announced. When layered on top of existing *qui tam* provisions under the FCA (31 U.S.C. § 3730(b)-(d)), the programs will create additional channels for insiders to report fraud directly to DOJ. And through the National Fraud Detection Center, the Fraud Division says it is using data analytics to proactively generate leads and open new investigations "at a rapid pace." DOJ may identify your compliance problem before you do.

What Contractors Should Do Now

The 10 factors are not just a prosecutor's checklist – they are part of a compliance officer's toolkit. Contractors should take three immediate steps.

Conduct a gap assessment against the 10 factors. Walk through each factor and ask whether your company has exposure. Does management have visibility into contract performance, or are there layers of insulation that could look like willful blindness? Are your audit responses complete and candid? How long have your current contracts been running, and when was the last time you stress-tested the

underlying compliance assumptions? Are you performing on programs with military readiness implications? Map your risk profile against the directive's framework and prioritize remediation where the gaps are widest.

Strengthen internal reporting channels. With new whistleblower incentive programs on the horizon, the single most important thing a contractor can do is ensure that employees view internal reporting as a credible, responsive, and safe alternative to going directly to DOJ. That means accessible hotlines, genuine anonymity protections, prompt investigation of complaints, and visible anti-retaliation enforcement. If your employees do not trust the internal system, they will use the external one – and you will lose the opportunity to self-disclose first.

Revisit your voluntary self-disclosure calculus. The directive's emphasis on data analytics and whistleblower incentives means the window for self-disclosure is shrinking. Companies that discover potential fraud should evaluate disclosure decisions promptly and engage experienced counsel early. The CEP's benefits are real, but they require timely action – waiting until DOJ comes to you is the surest way to lose the credit that could make the difference between a declination and an indictment.

Directive 26-12 is the clearest signal yet that procurement fraud sits at the top of DOJ's enforcement agenda. Prosecutors will now evaluate your company factor by factor. The companies that fare best will be those that ran that evaluation first.

This article was drafted by [Diana Lyn Curtis Shutzer](#) and [Nick Solosky](#), leaders of the Spencer Fane Government Contracts team. For more information, visit spencerfane.com.