

BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

Beyond The Firewall: Effective Mitigation Of Organizational Conflicts Of Interest In Federal Contracting

By Michael W. Mutek*

The Federal Acquisition Regulation (FAR) defines an organizational conflict of interest (OCI) as a situation where, due to other activities or relationships with other persons, a person (which includes an organization) is unable or potentially unable to render impartial advice or assistance to the government, perform contract work without impaired objectivity, or submit proposals for potential work without having an unfair competitive advantage.¹

OCI rules protect the integrity of the federal acquisition system,² but compliance is not necessarily satisfied simply by identifying a potential conflict scenario and relying upon a standard firewall. For contractors, the challenge is to identify OCI risk early, disclose it accurately, and develop mitigation measures that address the specific OCI concern.

For one thing, it may not be readily apparent that a contractor's business practices, external relationships, or other activities make the contractor unable to render impartial assistance or advice to the government in a particular situation.

Identifying an OCI that may exist could involve reviewing issues beyond the operation seeking a contract. That is because the potential unfair competitive advantage or the possible impairment could result from other operations or affiliates that could be geographically separated from the operation seeking the contract. The broader enterprise must be pulsed because OCI situations can arise not only from the work a business performs directly, but also from the work of affiliates, parents, subsidiaries, teammates, and subcontractors. Reviewing the entire enterprise including teammates and subcontractors is especially important when a

IN THIS ISSUE:

I. The OCI Rules	3
II. OCI Compliance In Practice	7
III. Mitigation Plans: Design, Substance, And Execution	9
IV. Conclusion: Be Prepared To Go Beyond The Firewall	15
V. Practical Guidelines For OCI Compliance	15

*Michael Mutek is senior counsel in the government contracts practice group at Womble Bond Dickinson (US) LLP located in Huntsville, Alabama. His practice spans government contracts, compliance and ethics, bid protests, claims, internal investigations and disclosures, formation and dissolution of teaming agreements, and dispute resolution. Michael also serves as an expert witness, mediator, and arbitrator.

contractor supports source selections, develops requirements, performs systems engineering work, evaluates products or services, or has access to nonpublic information that may be competitively useful. In those settings, mitigation must address how people, information, decision making authority, incentives, and corporate relationships operate in practice.

The consequences of getting an OCI analysis wrong are substantial and can include exclusion from competition, adverse responsibility or eligibility determinations, corrective action requirements, bid protests, and disputes over mitigation sufficiency. There also are business and reputational consequences, especially when a contractor's role across multiple programs or corporate entities draws scrutiny from lawmakers, the press, competitors, and customers. A mitigation plan that appears adequate on paper may still fail if it is generic, unsupported by facts, or not implemented as an operational control system.

As a practical matter, OCI compliance must be addressed early. OCI review should be built into bid/no-bid decisions and should continue through capture planning, teaming due diligence, proposal development, negotiation, award, and contract performance. Contractors also should assume that competitors will actively police OCI issues and may challenge whether a proposed firewall, recusal, separation arrangement, or other mitigation measure is sufficient.

OCI issues receive attention and there is considerable literature on the topic.³ Congress, for example, has examined OCI risk in the context of major defense acquisition programs and contractor advisory roles,⁴

while media coverage has highlighted concerns about contractor influence over requirements, evaluations, and lifecycle support.⁵ That outside scrutiny reinforces the central premise of this BRIEFING PAPER: effective OCI mitigation requires more than planning to erect a firewall. OCI mitigation requires a documented, tailored, and verifiable compliance approach that fits the actual conflict.

This BRIEFING PAPER provides a comprehensive overview of OCI mitigation in federal procurements, detailing the regulatory frameworks under the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), key protest decisions shaping OCI practice, and best practices for early identification, tailored mitigation plan design, and effective operational compliance to ensure procurement integrity and avoid competitive unfairness in complex contractor environments involving affiliates, subcontractors, and multi-entity relationships. The PAPER begins with the FAR and DFARS frameworks, then turns to protest decisions that have filled regulatory gaps and informed compliance strategies. It concludes by addressing mitigation plan design, including how to identify OCIs, select tools appropriate to the type of conflict, structure mitigation plans, and conduct reviews to determine whether those plans are working. Throughout, the goal is to frame OCI compliance as an operational governance function rather than a proposal formality, so that practitioners counseling contractors and business teams pursuing federal work can translate legal requirements into credible mitigation practices.

Editor: Valerie L. Gross

©2026 Thomson Reuters. All rights reserved.

For authorization to photocopy, please contact the **Copyright Clearance Center** at 222 Rosewood Drive, Danvers, MA 01923, USA, <http://www.copyright.com>, Toll-Free US +1.855.239.3415; International +1.978.646.2600 or **Thomson Reuters Copyright Services** at 2900 Ames Crossing Rd, Suite 100, Eagan, MN 55121, USA or copyright.west@thomsonreuters.com. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered; however, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

I. The OCI Rules

OCIs are not new. The issue gained recognition during the Cold War as the military increasingly relied on private think tanks and aerospace companies to help define technical specifications for military systems. Policymakers recognized that those same companies could gain an unfair advantage if they later competed to build the very systems that they helped shape.⁶ That concern led to the original OCI framework in the 1960s.⁷ From the early 1960s until the FAR became effective in 1984,⁸ relatively few OCI-related protests succeeded because protest forums rarely overturned contracting officer (CO) determinations.⁹ After the FAR was issued, OCI coverage expanded to civilian agencies¹⁰ and protest forums played a larger role in shaping OCI policy.¹¹

A. FAR Framework

Current OCI rules are found in FAR Subpart 9.5, *Organizational and Consultant Conflicts of Interest*, including FAR 9.500 through 9.508. Although the FAR does not create an exhaustive set of rules, it establishes the core architecture that governs OCI analysis today.

The key provisions:

- FAR 9.501 defines core terms, including “organizational conflict of interest.”
- FAR 9.502 addresses applicability.
- FAR 9.503 provides for agency waiver.
- FAR 9.504 assigns to COs responsibility to identify and evaluate potential OCIs and, where appropriate, avoid, neutralize, or mitigate them.
- FAR 9.505 states the general rules and provides examples.

FAR Subpart 9.5 reflects an effort to protect fairness in federal competitions.¹² Over time, three OCI categories have been recognized from the FAR text and from protest decisions applying the FAR in disputes over OCIs:

1. *Unequal access to information*—where a con-

tractor obtains or has access to competitively useful nonpublic information.

2. *Biased ground rules*—where a contractor had the ability to shape the competition to its advantage.
3. *Impaired objectivity*—where a contractor’s judgment may be biased because it is evaluating its own work, an affiliate’s work, or a competitor’s work.

The FAR’s approach is principles-based and flexible. The principles-based approach to OCI is evident because the FAR’s OCI coverage focuses on broad objectives rather than a strict checklist. This gives COs the authority to analyze each situation based on common sense and specific facts. The FAR distills its OCI policy down to two overriding principles:

- *Preventing unfair competitive advantage*: Ensuring no bidder wins due to biased rules or the possession of data unavailable to others.
- *Ensuring objectivity*: Guaranteeing the government receives impartial, unbiased advice from contractors.¹³

Because every procurement is unique, the FAR grants COs flexibility to identify and resolve conflicts early in the acquisition cycle. That flexibility is useful because OCI problems arise in highly fact-specific ways. But it also means that OCI outcomes often turn on the quality of the CO’s investigation, the adequacy of the record including the contractor’s mitigation efforts, and the agency’s willingness to engage in concrete mitigation analysis rather than rely on conclusory statements.¹⁴

The general rules in FAR 9.505 “prescribe limitations on contracting as the means of avoiding, neutralizing, or mitigating organizational conflicts of interest that might otherwise exist in the stated situations.”¹⁵

- *FAR 9.505-1* addresses systems engineering and technical direction work. It notes that where a contractor helps direct the development of a system, it “shall not—(1) [b]e awarded a contract to supply the system or any of its major components; or (2) [b]e a subcontractor or consultant to

a supplier of the systems or any of its major components.”¹⁶

- *FAR 9.505-2* addresses contractors that prepare specifications or work statements, reflecting the biased ground rules concern. It states that “if a contractor prepares and furnishes complete specifications covering nondevelopmental items, to be used in a competitive acquisition, that contractor shall not be allowed to furnish those items, either as a prime contractor or subcontractor, for a reasonable period of time.”¹⁷
- *FAR 9.505-3* addresses evaluation services. It states that such contracts “shall not be awarded to a contractor that will evaluate its own offers for products or services, or those of a competitor, without proper safeguards to ensure objectivity.”¹⁸
- *FAR 9.505-4* addresses access to proprietary information, which commonly requires non-disclosure commitments and information controls to prevent unfair competitive advantage. It also notes that marketing consultants may be the source of proprietary and sole-source information, which “may give the contractor an unfair advantage.”¹⁹

These examples show that the FAR treats mitigation as more than an abstract assurance of fairness. Depending on the facts, mitigation may require limits on future work, restrictions on access to information, exclusion of some personnel from proposal or performance activity, recusal from evaluation tasks, independent review, or other restraints tailored to the conflict.

The appropriate remedy must match the specific OCI concern: an information access problem may be addressed through a firewall and non-disclosure controls, while a biased ground rules or impaired objectivity concern may require task restructuring, exclusion from certain work, or a limitation on future contracting opportunities. There can be situations where mitigation is not possible.

Agency guidance seeks to assist COs in addressing OCIs. For example, the National Aeronautics and

Space Administration’s Guide on Organizational Conflicts of Interest “provides guidance on implementing the requirements in subpart 9.5 of the Federal Acquisition Regulation (FAR) on Organizational and Consultant Conflicts of Interest and provides tools to COs, attorneys, and requiring technical organizations on identifying conflicts and designing resolution strategies that best suit each circumstance.”²⁰ It also assists contractors in addressing OCI situations.

FAR 9.506 “Procedures” and FAR 9.507 “Solicitation provisions and contract clause” make clear that mitigation plan obligations become part of the procurement record and, when appropriate, part of the solicitation and contract. If a significant potential OCI exists, the CO must develop a written analysis and recommended course of action, including any proposed solicitation provision or contract clause.²¹ The solicitation provision should identify the potential conflict, state the proposed restraint on future activities, and explain whether the restriction or clause is negotiable.²² If the contractor proposes a mitigation plan, that plan should be specific enough for the CO to evaluate, and if accepted, the plan may become an enforceable contract obligation.²³

For contractors, the practical consequence of the requirements is that a FAR-based mitigation plan should be drafted as if it will serve three functions: first, to assist COs in fulfilling their pre-award responsibility to identify, evaluate, and resolve the OCI; second, to create a protest-resistant record showing why the conflict was avoided, neutralized, or mitigated; and third, to establish operational obligations that the contractor can implement and monitor during performance.

The FAR also recognizes that, in some circumstances, the government’s interests may justify accepting a situation that presents an OCI. FAR 9.503 allows waiver of a FAR Subpart 9.5 rule or procedure where the agency head or designee determines that application of the rule would not be in the government’s interest.²⁴ By contrast, the DFARS limits waiver authority and prohibits waiver of certain OCI restrictions on Major Defense Acquisition Programs (MDAPs).²⁵

B. DFARS And DoD-Specific Evolution

For defense contractors and practitioners advising them, OCI analysis cannot stop with the FAR. DFARS Subpart 209.5 reflects the sensitivity of the Department of Defense (DoD) to specific OCI problems, particularly related to major acquisition programs, lead system integrators, systems engineering, technical advisory work, and contractor access to proprietary technical data.

Relevant provisions include DFARS 209.570, DFARS 209.571, DFARS 209.505-4, DFARS 209.503-70, and related solicitation provisions and contract clauses such as DFARS 252.209-7008 and DFARS 252.209-7009.²⁶

The DFARS framework is significant in several respects. First, it reflects concern with lifecycle conflicts where a contractor may advise the government on technical matters and may later seek to compete for follow-on development or production work. Second, it focuses on structural conflicts involving entities that occupy influential positions in system design, integration, requirements development, or evaluation support. Third, compared with the FAR's general framework, DFARS is more explicit in addressing certain contractor roles, illustrating DoD's desire to impose restrictions where it sees competitive integrity at stake.²⁷

C. FAR And DFARS: Comparison And Key Lessons

Several examples illustrate the key points. A contractor performing lead system integrator functions on a major DoD system may be restricted from having a direct financial interest in the development or construction of the systems being integrated.²⁸ That restriction responds to the concern that an integrator with financial interests in component development could shape integration decisions in a way that benefits its own products or affiliates.

A second example involves systems engineering and technical assistance (SETA) work for a major defense acquisition program or pre-major defense acquisition program. DFARS 252.209-7008 gives offerors notice that, if awarded the SETA contract, the contractor or

its affiliates may be prohibited from participating as a prime contractor or major subcontractor in development or production of the weapon system unless an acceptable OCI mitigation plan is submitted and approved.²⁹ DFARS 252.209-7009 carries that restriction into the contract and makes compliance with an incorporated mitigation plan a material contract requirement.³⁰

A third example involves contractor access to third-party proprietary technical data or restricted computer software. DFARS 209.505-4 points to technical data and computer software clauses that address non-disclosure obligations when support contractors obtain access to information belonging to other contractors including non-disclosure agreements with the third party asserting restrictions.³¹ In practical terms, this is a DFARS-specific reminder that unequal access to information concerns often arise from the government's need to use support contractors while protecting proprietary information submitted by other industry participants.

A fourth example is waiver authority. Although FAR 9.503 provides general waiver authority, DFARS 209.503-70 narrows the waiver path for certain consulting services by requiring approval at a senior DoD level. This structure reflects a policy judgment that some advisory or consulting relationships present sufficiently sensitive conflict risks that ordinary waiver discretion should be elevated. It serves as a DFARS mandate that overrides the standard waiver allowances found in FAR 9.503.³² Under DFARS 209.503-70, the authority to approve OCI waivers for consulting services (as defined under DFARS 209.572(b)) is strictly limited. It cannot be delegated below a Senate-confirmed official appointed by the President.

Taken together, these examples show why DFARS analysis often has a different practical feel from FAR Subpart 9.5 analysis. The FAR asks whether the CO has identified, evaluated, and avoided, neutralized, or mitigated an OCI. The DFARS, in some DoD settings, may prescribe more concrete consequences: notice provisions, mandatory clauses, restrictions on future participation, senior-level waiver requirements, and incorporation of an OCI mitigation plan as a material contractual obligation.

DFARS OCI provisions provide three practical lessons:

- First, DoD may convert what looks like a mitigation issue into an eligibility or future participation restriction, especially for lead system integrators and SETA contractors supporting major defense acquisition programs.³³
- Second, an approved OCI mitigation plan may become part of the contract, making compliance a material contractual obligation rather than merely a proposal representation.³⁴
- Third, DFARS analysis often requires attention to statutory limits, senior-level approvals, and program-level consequences that are not always present in ordinary FAR Subpart 9.5 analysis. In practical terms, a defense contractor should treat DFARS OCI review as both a protest risk exercise and a contract performance obligation.³⁵

The FAR and DFARS pursue the same basic objective, which is to protect the integrity of the procurement process, and they do so in a complementary fashion:

- FAR provides the foundational doctrine and broad principles.
- FAR focuses on the three traditional categories (biased ground rules, impaired objectivity, unequal access to information).
- FAR instructs COs to insert OCI restrictions in proposals and contracts but does not provide uniform, pre-written contract clauses.
- DFARS applies those principles in a more defense-specific way, particularly where advisory roles, systems integration, and major acquisition programs create heightened concern.
- DFARS explicitly states that for MDAPs, the DFARS rules take legal precedence over any inconsistent provisions in the FAR.³⁶
- DFARS mandates two non-negotiable clauses for certain systems engineering contracts.³⁷
- In practice, the FAR often frames the analysis,

while the DFARS can shape the outcome through more tailored restrictions or representations.

D. The Impact Of The Revolutionary FAR Overhaul On OCI Rules

Government contracting currently is undergoing the Revolutionary FAR Overhaul, or “RFO,” initiated by Executive Order 14275, *Restoring Common Sense to Federal Procurement*, issued on April 15, 2025.³⁸ Under that Executive Order, the Federal Government is undertaking an extensive overhaul of the FAR. Led by the Office of Federal Procurement Policy (OFPP) and the Federal Acquisition Regulatory Council (FAR Council), this initiative seeks to return the FAR to its statutory roots, rewrite it in plain language, and remove most non-statutory rules. In addition, non-regulatory buying guides will provide practical strategies while remaining outside the FAR.³⁹

The RFO effort raises a legitimate question whether OCI rules will change. The RFO seeks to reduce regulatory text, increase CO discretion, and move detailed guidance outside the FAR. At the same time, OCI rules over time have addressed specific congressional mandates that seek to impose disclosure and conflict mitigation requirements.⁴⁰ As a result, it is unlikely that the RFO will eliminate OCI requirements.

The RFO materials released by the FAR Council and posted through Acquisition.gov at the time this article was drafted do not indicate that the OCI framework will be rewritten. They do, however, suggest important changes: FAR OCI coverage may move within the FAR, and OCI consideration and review may become more directly integrated into procurement planning.⁴¹

More specifically, the proposed rules reveal relocation of OCI coverage from FAR 9.5 to FAR Part 3. FAR Subpart 9.5 focuses broadly on contractor qualifications and administrative responsibility determinations. The RFO will move the entire OCI framework into FAR Part 3 (*Improper Business Practices and Personal Conflicts of Interest*). This relocation aligns OCIs directly with procurement ethics, business integrity, and personal conflicts of interest.⁴²

Although the FAR is being aggressively streamlined

and simplified under the RFO, defense-specific statutes cannot be erased by Executive Order. As a result, the DFARS prohibition that bars a SETA contractor on a major defense program from participating in the development or production of that weapon system remains in place. The DFARS notes that this requirement cannot be waived because it is anchored directly in federal statute.⁴³

E. The Importance Of Early OCI Analysis

OCI analysis begins when a contractor first becomes aware of the opportunity. Requests for proposals (RFPs) and other solicitation vehicles often require potential contractors to disclose known conflicts, explain corporate relationships, identify access to nonpublic information, and submit mitigation plans before award.⁴⁴ Government agency guidance points out the issue of OCI “should be addressed during the source selection process.”⁴⁵

Key points to consider include:

- First, capture teams, lawyers, and compliance personnel need to assess OCI risk early in the pursuit process before teaming is finalized and well before proposal submission.
- Second, the quality and specificity of a contractor’s pre-award OCI submission can materially shape the CO’s understanding of the risk including whether it can be mitigated.
- Third, because the record created at the solicitation and evaluation stages often becomes important in a protest, companies need to create and implement effective mitigation plans that are well developed and clear enough to withstand later scrutiny.
- Fourth, OCI disputes often arise from role combinations that a company may view as operationally sensible, but that an agency, competitor, GAO, or court may view as threatening procurement integrity.

II. OCI Compliance In Practice

OCI compliance has developed in part through

protest decisions. The decisions have shaped practical OCI compliance and have provided guidance by filling gaps in the regulatory framework. The decisions also show how agencies and protest forums evaluate risk, assess mitigation, and determine whether the contractor and agency complied with OCI requirements.

The focus of this BRIEFING PAPER is on effective mitigation and not on a review of case law; however, the following are some key cases that have shaped OCI compliance and informed mitigation practices.

A. Unequal Access To Information

In *Aetna Government Health Plans, Inc.*,⁴⁶ GAO addressed a significant OCI where an affiliate of one of the procurer’s major subcontractor evaluated proposals for the procuring agency. The procurement involved managed health care and associated administrative services, and the conflict arose because the agency relied on a consultant affiliated with a proposed major subcontractor for the awardee. GAO sustained the protest, concluding that the agency acted unreasonably by failing to make an independent effort to gather relevant facts, and by relying on materials prepared by the private firms whose affiliation created the conflict.

The proposed mitigation, which involved the severing of communication between the affiliates and relying on the absence of direct financial interests by the evaluating affiliate’s employees, was not enough. The case illustrates a recurring protest risk: when the mitigation record is built largely by the conflicted parties themselves, GAO may question whether the agency independently assessed the conflict.

B. Biased Ground Rules

In *Lucent Technologies World Services Inc.*,⁴⁷ GAO examined a classic “biased ground rules” concern. Lucent had performed design-build communications work in Iraq and had helped validate concepts, assess communications infrastructure, and prepare analysis involving technologies later reflected in the procurement for Terrestrial Trunked Radio devices for the Advanced First Responder’s Network. The agency excluded Lucent from competing, and GAO denied the protest after concluding that the agency reasonably

determined that Lucent's prior preparation of technical specifications created an OCI.

The example is useful because it shows that exclusion may be sustained even without proof that the contractor intentionally skewed the procurement. For mitigation planning, the lesson is that contractors performing requirements definition, systems architecture, technical assessment, or statement of work functions should evaluate whether later participation in implementation or supply competitions will be barred or require a carefully documented mitigation strategy.

C. Impaired Objectivity

In *Alion Science & Technology Corp.*,⁴⁸ GAO addressed impaired objectivity in a procurement for electromagnetic spectrum engineering services for the Defense Information Systems Agency's Joint Spectrum Center. The awardee was affiliated with a manufacturer and marketer of spectrum-dependent products, and the work required subjective judgments that could affect the use, sale, or evaluation of products made by the awardee, its competitors, and its customers. GAO sustained the protest because the record did not support the agency's assessment of the "maximum potential" for OCIs.

The decision underscores that impaired objectivity mitigation must address incentives and judgment, not merely information transfer. A later *Alion* decision denying a protest after corrective action also illustrates the other side of the point: when an agency meaningfully identifies affected products, customers, competitors, and tasks, and documents why firewalled subcontractors can perform conflicted work without undermining performance, GAO may defer to the agency's mitigation judgment.⁴⁹

D. Adequacy Of Mitigation And Waiver Documentation

The *Dell Services Federal Government, Inc.* line of decisions illustrates how OCI issues can persist through multiple protest rounds if the agency record does not address the conflict in a disciplined way.⁵⁰ In the 2017 decision, GAO sustained a protest where the record showed access to nonpublic, competitively use-

ful information and possible involvement in developing requirements, yet the agency had not meaningfully evaluated whether unequal access to information or biased ground rules OCIs existed or taken steps to avoid, neutralize, or mitigate them.⁵¹

In 2018, GAO again sustained a protest where an individual involved in the awardee's proposal had access to competitively useful, nonpublic information about the protester under another contract.⁵² Later, GAO denied a protest challenging the agency's written waiver because the waiver was in writing, set forth the extent of the conflict, and was signed by an authorized official.⁵³ The practical lesson is that OCI mitigation must be supported by a record that explains who had what information, when they had it, how it could be competitively useful, what restrictions were imposed, and why the agency believed the conflict was resolved or waived.

Certain themes are seen in OCI protest decisions:

- *Documentation matters.* OCI outcomes frequently turn on the adequacy of the CO's record. Contractors play an important role in the creation of this record.
- *Appearance can be enough.* Protest forums do not always require proof of actual bias where the structure of the work creates a meaningful potential conflict. The appearance of conflict matters.
- *Mitigation must be real and appropriate to the situation.* Boilerplate firewalls and generic promises carry less weight than targeted measures tailored to the actual conflict. Prior experience with OCI mitigation can be a factor.
- *Corporate relationships matter.* Parent, subsidiary, and affiliate structures may complicate OCI analysis, particularly where personnel, information systems, or incentives overlap. This can make mitigation and firewall creation challenging.

Courts and protest forums examine OCI issues through a traditional administrative law analysis, focusing on whether the agency's decision was rational

and adequately supported. That framework gives agencies room to exercise judgment, but only where the record shows that they examined the issue and reached a reasoned decision.⁵⁴

For mitigation plan drafting, these cases point to a practical rule. Contractors should assume the mitigation plan will be read by the CO, a disappointed offeror, and GAO or the Court of Federal Claims after award. The plan should therefore do more than promise ethical behavior. It should identify the hard facts supporting the OCI analysis, explain why the selected controls address the actual conflict, preserve evidence of implementation, and give the CO a record sufficient to defend the agency's decision if challenged. A plan that does not help the agency write a reasoned OCI determination may reduce neither protest risk nor performance risk.

E. Key Case Lessons

The principal lesson is that OCI mitigation succeeds or fails on the record. Other key lessons include:

- *Aetna* shows that agencies cannot rely uncritically on conflicted parties to build the mitigation record.
- *Lucent* shows that biased ground rules concerns may justify exclusion where a contractor helped shape technical requirements used in the competition.
- *Alion* shows that impaired objectivity concerns require analysis of incentives, affected products, customers, competitors, and tasks—not just information barriers.
- The *Dell Services* decisions show that OCI issues can survive multiple protest rounds unless the agency identifies who had what information, whether it was competitively useful, what restrictions were imposed, and whether any waiver or mitigation decision is documented by an authorized official.
- Taken together, the cases reinforce that a mitigation plan should supply hard facts, tailored

controls, implementation evidence, and a record the CO can defend.

F. Congressional Attention And Policy

OCI requirements have not developed in a vacuum. OCI concerns have caught the attention of Congress, which has focused on OCI risk through oversight hearings, defense acquisition reform efforts, and statutory direction, for example, a law tied to the management of major defense programs.⁵⁵ Concerns about contractors serving both advisory and execution roles, or about the concentration of technical expertise in a small number of integrated firms, have fed an ongoing policy debate.⁵⁶

Oversight pressure tends to push agencies toward greater care.⁵⁷ This can be seen in demands for explicit documentation, skepticism of informal mitigation, and willingness to ask difficult questions about corporate structure, data access, and independence of judgment. Media scrutiny reinforces this same dynamic by making OCI disputes visible to the public.⁵⁸

III. Mitigation Plans: Design, Substance, And Execution

A. Design Starts With Accurate OCI Identification

OCI mitigation plan design work begins with identification of an actual or perceived OCI scenario. Effective identification is necessarily enterprise-wide and not limited to the specific business unit, location, or division considering the pursuit of a contract.⁵⁹

Identification also extends beyond the contractor's enterprise. Teaming partners and subcontractors need to be pulsed as well. Today, it is common for teaming agreements to expressly address OCI. An OCI provision in a teaming agreement can protect the parties by facilitating early identification and treatment of OCI issues. Teaming agreement OCI provisions generally outline how the parties will handle actual or potential conflicts.⁶⁰ OCI provisions in teaming agreements serve as an early warning radar system. Often, they include a requirement to cooperate to seek a mitigation plan but also allow disengagement if mitigation is

deemed too difficult or would jeopardize the team's ability to succeed in capturing the contract award.⁶¹

An OCI review typically focuses on these questions:

1. *What work is the company seeking now, and what related work may it seek in future?* This is the basic lifecycle contract question. OCI risk often emerges when advisory or evaluation work early in a program's lifecycle overlaps with an intention to compete for implementation, production, sustainment, or follow-on support.⁶²

2. *What information does the company, or any affiliate, or any team member or supplier, have that competitors do not possess?* Unequal access to information OCI analysis requires careful attention not only to what information a business unit has, but to what the broader corporate family and team members may possess, how data is stored, and who can access it. Possession of information may be permissible and allowable, such as the "incumbent advantage."⁶³ The natural advantages of incumbency do not create an impermissible OCI. GAO has stated that "hard facts" that reveal unfairness must be proven to sustain an OCI allegation.⁶⁴

3. *Who is evaluating whom?* Impaired objectivity risk often turns on whether a contractor's work requires it to assess its own products, services, personnel, or affiliates. This question becomes especially acute in large enterprise structures.⁶⁵ The question extends beyond the contractor's organization and considers whether the work would require assessment of a competitor. The concern is the inability to render impartial work due to a relationship that creates an economic incentive to do something.⁶⁶

4. *How do others, including the government and competitors, view the role?* Contractors sometimes focus on whether they believe they can behave objectively and defend participation in a competition despite possession of information not available to other competitors or having conflicting roles. The better question often is how the agency, a disappointed offeror, GAO, or a court would characterize the role combination. OCI analysis must therefore account for perception as well. Competitors actively police OCIs

during the competition to identify the advantages that others may possess and seek to assess the legitimacy of such advantages.

An effective corporate OCI identification process requires close coordination among legal, ethics/compliance, contracts, business development, and operational leadership. OCI identification is the diagnosis; mitigation plan design is the treatment.

An OCI mitigation plan is more than a document prepared for a procurement file. It is an operational control framework specific enough to guide behavior, credible enough to reassure the CO, and durable enough to survive performance.⁶⁷

B. Due Diligence Checklists

Due diligence checklists can assist in identifying OCIs and preparing mitigation plans. Companies with formal OCI policies and procedures often develop checklists to help identify potential conflicts. Although any checklist should be tailored to the procurement and corporate structure, the corporate template can provide a useful starting point.

Examples exist, including the Space Systems Command *Organizational Conflicts of Interest Mitigation Plan Checklist*, Rev. Nov. 2013.⁶⁸ That checklist provides a structured framework for contractors to identify, avoid, and mitigate institutional conflicts of interest in connection with covered acquisitions.

The Space Systems Command checklist outlines requirements for the prime contractor and any subcontractor or teammate to identify, avoid, and mitigate OCIs. It requires the contractor to identify actual or potential OCI situations involving its own work and the work of teammates or subcontractors, propose an OCI mitigation plan for inclusion in the resulting contract, complete the checklist as an appendix to the plan, and identify where each checklist requirement is addressed in the plan. If teammates or subcontractors submit their own OCI plans, those plans also must include completed checklists. The checklist therefore operates as both a drafting guide and a compliance test.

Examples of checklist items include a senior corpo-

rate official's written commitment to continuously identify, avoid, or mitigate OCI situations; annual certification of compliance with the OCI plan; an explanation of the performing business unit's position within the broader corporate structure; organizational charts for the parent organization and performing business unit; and letters of commitment from teammates and subcontractors or separate OCI plans from those entities.

The checklist also addresses OCI mitigation plan administration. It calls for identification of the individual responsible for oversight and administration of the OCI plan, identification of the individual responsible for maintaining plan documentation, specification of where OCI plan records will be maintained, and a commitment that those records will be accessible to the CO or a government auditor. It requires identification of corporate OCI-related policies and procedures and a description of the processes used to execute the plan.

Personnel management examples are important. The checklist expects the plan to address OCI training and awareness, non-disclosure agreements, access restrictions, and procedures for ensuring that personnel understand their responsibilities. It also reinforces the importance of flow-down obligations by requiring the prime contractor to commit to imposing OCI plan requirements on teammates and subcontractors. These items show why the checklist fits the "beyond the firewall" theme: it treats mitigation as a managed compliance system involving leadership commitment, documentation, training, implementation, flow-down, and review.

The checklist also helps reduce protest risk because it prompts the contractor to create the kind of record that a CO can rely on if the award is challenged. By requiring cross-references to the mitigation plan, senior-level commitments, organizational charts, responsible officials, documentation locations, flow-down obligations, training controls, and access restrictions, the checklist makes it harder for a protester to characterize the plan as conclusory or undocumented. It also helps the agency show that it examined the relevant facts rather than merely accepting a contractor's assurance that a firewall or corporate separation exists.

C. Core Mitigation Tools

Common OCI mitigation tools or mechanisms include:

- *Information firewalls* are the most common strategy for mitigating unequal access to information OCI scenarios. An information firewall segregates data, systems, and personnel to appropriately limit the exchange of information between personnel and as needed, parts of the overall entity, to address the OCI issue.
- *Organizational separation* (sometimes called a structural firewall) is also a common mitigation strategy. Separation is established between business units or reporting chains.
- *Recusal provisions* exclude conflicted personnel or entities from certain work.
- *Independent review structures* can be developed and implemented for tasks involving evaluation or assessment.
- *Training and certifications* are designed to implement the plan and ensure that employees understand the importance of the OCI mitigation plan and their responsibilities.
- *Management oversight and audit mechanisms* are used to test compliance, highlight issues, identify potential disclosure mandates, and suggest improvements.

The most effective OCI mitigation plans are plans specifically created to address the type of OCI presented and the corporate structure involved. The several OCI mitigation mechanisms, such as firewalls, reporting chain modifications, or physical and organizational separation, are tools utilized to accomplish a goal.

There has been a tendency to assume that a firewall will solve any OCI issue. That assumption is mistaken. A firewall is a mitigation tool,⁶⁹ not a universal cure. Firewalls often are accepted for unequal access to information situations, but they are frequently viewed as inadequate without more for impaired objectivity con-

cerns⁷⁰ and may not mitigate biased ground rule situations. In those more challenging situations, the problem is not information transfer; it is the contractor's economic incentive and ability to exercise independent judgment.

In one of the most frequently cited modern decisions addressing the limits of firewalls, GAO upheld the Air Force's determination that a proposed subcontractor created impaired objectivity and unequal access to information concerns. GAO further concluded that proposed firewall and recusal measures were insufficient, emphasizing that structural conflicts affecting a contractor's judgment often cannot be cured through information segregation alone.⁷¹

Some other considerations on mitigation based upon experience and review of case law include:

- Generally, unequal access to information OCI is the simplest OCI category to mitigate because they often can be addressed with adequate information controls and firewalls.
- Impaired objectivity concerns may require role redesign, independent review, or exclusion from certain tasks.
- Biased ground rules issues are often the most difficult to mitigate. If mitigation is possible, it may require creative use of third parties or government involvement in certain tasks. In some cases, the most appropriate mitigation is to forgo the opportunity.
- The mere existence of an OCI mitigation plan may not be enough to pass muster.⁷² The government has discretion in making that determination, but the record should show a reasoned analysis.⁷³
- Examination of OCI mitigation during a bid protest indicates agencies must actively analyze the specific scenario to determine if a firewall or mitigation strategy will prevent competitive harm.⁷⁴

D. The Risk Of Boilerplate

The risk of using boilerplate is that specific facts of

the present OCI situation may not be addressed. The strongest OCI mitigation plans are not boilerplate mitigation plans or recycled versions of plans used in different procurements. They are tailored and identify the relevant entities, define the restricted information or restricted tasks, state the precise concern, specify who may and may not access information or personnel, explain reporting lines, address subcontractor and affiliate interactions, and provide practical escalation procedures when questions arise. They also address retention, monitoring, retraining, and remediation.

A mitigation plan should be drafted with the understanding that a protest forum may later examine whether the agency acted reasonably in relying on the plan. For that reason, the plan should identify the conflict, state the relevant facts, explain why the mitigation tools fit the risk, document implementation steps, and make clear how compliance will be verified.

This protest risk perspective affects both substance and tone. A plan that relies on conclusory statements such as "no competitive advantage exists," "personnel will not communicate," or "the affiliate is separate" invites scrutiny if it does not explain the factual basis for those assertions. By contrast, a plan that maps personnel, systems, reporting lines, restricted data, conflicted tasks, subcontractor roles, certifications, training, audit rights, and escalation procedures gives the CO concrete facts to evaluate and gives the company a defensible framework if the award is challenged.

E. Merger And Acquisition Activity And OCIs

Another consideration is whether the contractor is involved in merger or acquisition activity. In that context, not only the CO representing the buying agency, but additional federal agencies may review and approve the transaction.

This is a fact that the CO would need to know because the CO would need to determine whether the merger or acquisition raises an OCI concern, and, if so, whether it can be mitigated.⁷⁵ The FAR directs COs to identify and evaluate potential OCIs as early as possible and to avoid, neutralize, or mitigate significant conflicts.⁷⁶

Mergers and acquisitions can trigger additional government review. Where government contracts are involved, agencies may examine whether the transaction creates new OCIs through the combination of affiliates, access to nonpublic information, or overlapping advisory and performance roles. Agencies charged with reviewing a merger or acquisition may want to understand how any potential OCI is being addressed and whether the combination in the merger or acquisition raises additional conflict concerns.⁷⁷

F. Additional Considerations For Affiliate And Parent Conflicts And Merchant Supplier Firewalls

OCIs can arise in additional settings. Affiliate, parent company, and merchant supplier scenarios arise with enough frequency to warrant separate attention.

1. *Affiliate and Parent Company Firewalls.* Affiliate and parent company conflicts are challenging because they consider and expose what can be complex corporate relationship issues. A plan that simply asserts that two entities are legally distinct or located in different places or work under different management is unlikely to be persuasive if personnel, systems, leadership, incentives, or privileged information flow across those entities in practice.

A well-designed affiliate and parent company firewall plan typically must do more than describe legal separateness. It should explain actual operating separation: who reports to whom, which data repositories are segregated, how access is restricted, what approvals are required, how shared functions are handled, and what happens when personnel move between affiliated organizations. It should also address how compliance is monitored and how exceptions are escalated.

In the author's experience, affiliate and parent company conflicts can arise when one part of a company seeks to compete for a prime contract while another part seeks a subcontract award from a competitor pursuing the same prime contract. Similar issues can arise during merger and acquisition activity when the acquiring company and target are both pursuing the

same award, submitting separate proposals, or participating on competing teams.

This type of situation requires careful analysis. Participation on competing teams may be pro-competitive because it may create a stronger competitive marketplace that gives the government meaningful alternatives. At the same time, the potential for inappropriate information flow exists, as does the appearance of conflict particularly if there is concern that the corporate parent is favoring one team.

One lesson from affiliate and parent company conflicts is the value of showing strong corporate parent support for the implementation of an effective firewall or mitigation plan, including evidence that leadership understands, supports, and will enforce the controls.

2. *Merchant Supplier Firewalls.* The term "merchant supplier" is a supply chain term sometimes used to describe a manufacturer that sells finished goods rather than one that sells raw material. For example, in the defense industry, the term merchant supplier is used to describe a supplier of solid rocket motors (SRMs) who is independent of the prime contractors buying the SRMs and incorporating them into the missiles that are being manufactured by the prime contractor.⁷⁸

Where a company supplies products or services to multiple prime contractors competing for the same procurement, conflict analysis and mitigation can become unusually sensitive. Even when the supplier is not competing as a prime, there may be concern that the merchant supplier could favor one competitor during the procurement or inadvertently disclose one prime contractor's nonpublic information to personnel supporting another competing prime.

A merchant supplier firewall plan therefore should demonstrate competitive neutrality. Relevant issues include customer-by-customer information segregation, equal access to commercially available inputs, controls on pricing and proposal support information, limits on personnel crossover and reassignment, and clear rules prohibiting the use of one competitor's procurement sensitive information to benefit another. The strength of such a plan often depends on whether

it can demonstrate not only confidentiality, but neutrality across competing customers.

G. Best Practices

The objective of an OCI mitigation plan is not merely to check a box so that a company can compete for a government contract. The objective is to create a plan tailored to the situation, capable of implementation, and sufficient to address the government's concern. An OCI mitigation plan is credible only if it works in practice.

Several best practices emerge from experience:

- *Start early.* OCI analysis should begin at the start of a contract pursuit, not during final proposal preparation. OCI issues may be solicitation requirements, may require an extensive and potentially costly mitigation plan, and may support a no bid decision.
- *Understand and map the entire enterprise.* Effective OCI review requires visibility into affiliates, parents, subsidiaries, joint ventures, subcontractor arrangements, supply chain relationships, and recent or pending acquisitions.
- *Draft the plan for the specific facts.* The best mitigation plans respond to the actual conflict, not to OCI categories in the abstract. A plan that worked in a previous competition may not be sufficient for the present procurement.
- *Train personnel.* A firewall that exists only in legal files is unlikely to survive scrutiny. Training is important, and training records should be maintained. Periodic retraining is a best practice.
- *Preserve the record.* Contemporaneous documentation can be important in a protest or agency review. Keep the materials needed to show what information was reviewed, who participated, what restrictions were imposed, how personnel were trained, and how the company confirmed that the plan was followed.

H. Formal Corporate OCI Compliance Programs

Companies that address OCI mitigation plans can benefit from the creation of a formal corporate OCI compliance program supported by policies, procedures, guidance, and subject matter experts. This is particularly useful if the nature of the company's work raises OCI scenarios on a regular basis or the company's organizational structure includes divisions and affiliates that may compete.

An OCI program supported by policies and procedures should codify how the company reviews contract opportunities for potential OCI scenarios, allocates responsibilities among corporate functions, develops and implements mitigation plans, and conducts mitigation plan reviews.

I. Reviewing Operating Mitigation Plans

The process of reviewing operating mitigation plans deserves more attention. Every OCI mitigation plan should address a process of regular reviews. Whether called an audit, review, assessment, or monitoring, the process should test whether controls are functioning as designed. Reviews may include examination of access logs, personnel assignments, recusal compliance, training completion, management certifications, and exception handling.

Interviews are a common tool of such reviews because interviews allow employees who implement the mitigation plan to share experiences, concerns, and recommendations. The review's objective is not simply to prove that the company drafted an acceptable plan, but to confirm that the plan remains aligned with real operations, note concerns, and recommend improvements.

Periodic review is especially important where organizations grow through acquisition, change reporting structures, launch new business lines, or shift personnel among affiliated entities. OCI mitigation that was sufficient at one point in time may not be sufficient if the underlying business architecture changes.

IV. Conclusion: Be Prepared To Go Beyond The Firewall

OCI law has traveled from a relatively concise regulatory framework in FAR Subpart 9.5 to a significant body of protest decisions, DFARS provisions, and congressional mandates that collectively require contractors and agencies to engage in more disciplined conflict analysis.

Also, mitigation strategies have traveled from simple firewall creation to more complex mitigation plans that incorporate firewalls as one tool among several. It has moved beyond the firewall. One clear trend emerges from that evolution: OCI mitigation must be detailed, tailored, and capable of operating in practice.

The traditional OCI categories—unequal access to information, biased ground rules, and impaired objectivity—remain useful guideposts. But the business settings in which those categories arise have become more complex. Large enterprises, affiliates, joint ventures, subcontractor networks, merchant suppliers, shared data systems, and acquisition-driven restructuring can all create conflict scenarios that do not yield to a generic mitigation response. Clearly in complex scenarios, a firewall alone is not sufficient.

For that reason, the central lesson is that contractors must move beyond the firewall as a conflict mitigation tool. Firewalls remain important, particularly for unequal access to information concerns, but where the issue involves influence over ground rules, evaluation of one's own work, affiliate incentives, or competing economic interests, effective mitigation may require organizational separation, recusal, independent review, role restructuring, enhanced oversight, or, in some cases, declining the work.

A credible OCI mitigation plan should not be treated as a simple and reusable form. It should be a documented operating system that identifies the specific conflict, explains why the selected controls fit that conflict, assigns responsibility, trains personnel, restricts access or participation where needed, preserves the record, and provides a method to test whether the controls are functioning.

This is why verification matters. A mitigation plan that is not monitored, audited, updated, or enforced may be vulnerable even if it appears adequate when submitted. The strongest plans demonstrate not only how information is protected, but also how judgment is preserved, corporate influence is controlled, exceptions are escalated, and compliance is confirmed over time.

Looking ahead, the Revolutionary FAR Overhaul may relocate or streamline OCI coverage, but it is unlikely to eliminate the need for early identification, disclosure, mitigation, and record support. Agencies and protest forums will continue to focus on whether the CO reasonably examined the conflict and whether the mitigation approach was sufficient for the facts. Contractors should expect continued scrutiny of corporate affiliation, data access, advisory roles, and multiple relationships within the same procurement ecosystem.

For lawyers, compliance professionals, and business leaders, OCI compliance is best understood as an enterprise governance function. The best positioned contractors to manage OCI risk will be those that can translate regulatory principles into credible operational practices and plans that go beyond the firewall, address the actual conflict, and prove that mitigation works in practice.

V. Practical Guidelines For OCI Compliance

The following *Guidelines* provide practical compliance steps. They reflect the FAR and DFARS framework, protest decisions, and experience with OCI mitigation plans, with emphasis on early identification, tailored controls, operational execution, and verification. They are not, however, a substitute for professional representation in any specific situation.

1. Begin OCI analysis well before the bid decision. Treat OCI review as part of capture strategy, teaming, and bid/no-bid analysis. For example, a company considering SETA, requirements development, evaluation support, or incumbent follow-on work should decide before proposal submission whether the opportunity creates a later participation restriction,

requires a mitigation plan, or supports a no-bid decision.

2. *Map the full enterprise.* Look beyond the bidding entity to parents, subsidiaries, affiliates, joint ventures, subcontractors, shared services, reporting relationships, data systems, and recent or pending acquisitions. For example, a proposal team should identify whether an affiliate supports a competing team, whether a parent company controls shared information systems, or whether a subcontractor has access to another offeror's proprietary information.

3. *Classify the conflict correctly.* Determine whether the issue is unequal access to information, biased ground rules, impaired objectivity, or a combination of those categories. For example, access to a competitor's pricing data points toward unequal access to information; drafting a performance work statement points toward biased ground rules; evaluating an affiliate's product points toward impaired objectivity. The mitigation tool should follow the actual risk.

4. *Read the solicitation carefully.* Identify all OCI disclosure, certification, mitigation plan, and update requirements early, and build the proposal record around those requirements.

5. *Base mitigation on facts, not assumptions.* OCI conclusions should be supported by hard facts about work performed, information accessed, personnel involved, affiliate relationships, and the actual flow of data or influence.

6. *Draft mitigation plans for the specific conflict.* Avoid generic firewall language. For example, a plan addressing unequal access should define restricted information, identify restricted personnel, describe system controls, and require certifications; a plan addressing impaired objectivity may need independent review, recusal, task reassignment, or exclusion from certain work.

7. *Make the mitigation plan operational.* A plan should function as an operating control system, not simply as a proposal attachment. Include training, access controls, certifications, recusal procedures, management oversight, exception reporting, and conse-

quences for noncompliance. For example, the plan should state who grants access to restricted repositories, who maintains access logs, who approves personnel transfers, and who reports exceptions to the CO.

8. *Preserve the record.* Assume the CO's analysis and the contractor's submission may later be reviewed by GAO or a court. Maintain contemporaneous documentation showing what was reviewed, what risks were identified, why mitigation was adequate, and how the plan was implemented. Examples include meeting notes, access lists, training records, certifications, subcontractor acknowledgments, audit reports, and exception logs.

9. *Account for perception as well as actual bias.* OCI rules protect procurement integrity and competitive fairness. Contractors should evaluate how the role combination may appear to the agency, competitors, protest forums, and outside reviewers.

10. *Pay special attention to affiliate and parent company conflicts.* Formal corporate separateness is rarely enough by itself. Mitigation should address actual operating separation, shared systems, shared leadership, incentives, and personnel movement.

11. *Maintain neutrality in merchant supplier situations.* Suppliers supporting multiple competitors should demonstrate customer-by-customer information segregation, equal treatment, pricing controls, personnel restrictions, and procedures preventing one customer's information from benefiting another.

12. *Review and audit mitigation performance.* Periodically test whether firewalls and other controls are working through access log reviews, interviews, training records, certifications, exception reports, and management reviews. For example, a quarterly review might compare access logs against approved personnel lists, confirm that recused employees did not participate in restricted tasks, and document any corrective actions.

13. *Update mitigation when the business changes.* Reassess OCI controls when the company acquires businesses, reorganizes, changes reporting chains, shifts personnel, adds new programs, or pursues related follow-on work.

14. Know when mitigation may not be enough. Some conflicts cannot be cured by information controls alone. For example, a contractor that helped define the technical requirements may be unable to compete for the resulting development work, and a contractor asked to evaluate its own product may need role restructuring, independent review, waiver consideration, or exclusion from the work.

15. Treat OCI compliance as an enterprise governance function. Mature contractors should integrate OCI review into ethics, legal, contracts, capture, business development, information security, supply chain, mergers and acquisitions, and enterprise risk processes.

16. Recognize that OCI mitigation goes beyond the firewall. It requires a managed compliance system involving and integrating leadership commitment, documentation, training, implementation, flow-down, and review.

17. Recognize the value of company OCI policies and procedures. Corporate commitment to OCI compliance should include policies, procedures, checklists, responsible officials, training expectations, escalation paths, and periodic reviews that help identify conflicts and verify that mitigation works in practice.

Exhibit 1

Simple Firewall Plan Example

ORGANIZATIONAL CONFLICT OF INTEREST (OCI) FIREWALL PLAN

Program Name: [Program Name]

Agency: [Agency Name]

Effective Date: [Date]

OCI Compliance Officer: [Compliance Officer Name]

Firewall Administrator: [Insert Name/Title, often Contracts]

1. Purpose & Scope

[Company name] “Company” intends to compete for the [Program Name] “Program.” To do so, the Company must address an Organizational Conflict of Interest (OCI). [Describe OCI scenario, e.g., certain employees worked on a different program that provided the employees with access to non-public information.]

This Plan establishes a legally binding operational firewall within the Company to isolate and protect non-public, proprietary, or Source Selection Sensitive Information (collectively, “Protected Information”) related to the Program.

The purpose of this Firewall Plan is to eliminate any potential for an “Unequal Access to Information” OCI under FAR Subpart 9.5.

2. Firewall Team Segregation (Separation of Employees)

To prevent the flow of Protected Information, the Company is divided into two distinct, non-communicating teams regarding this effort:

- **Firewalled Team (The “Access to Information” Team):** [Insert Name(s) of personnel who had access to the information or government].
- **Proposal Team (The “Clean” Team):** [Insert Name(s) of proposal writers, managers, and capture staff].

3. Controls [How the Firewall Works]

A. Physical and Digital Data Isolation

- **Digital Locks:** All electronic files, databases, shared drives, and emails related to the Protected Information are restricted via user-access permissions.
- **No Cross-Server Sharing:** Proposal Team members are explicitly blocked from accessing directories, SharePoint sites, or repositories accessed by the Firewalled Team.
- **Physical Security:** Firewalled Team members will work in separate office locations or secure designated areas. Physical documentation regarding the project must be kept in locked filing cabinets.

B. Communication & Non-Disclosure Agreements (NDAs)

- **Mandatory NDAs:** Every employee, whether assigned to both the Firewalled Team or the Proposal Team, must sign a project-specific OCI Ac-

knowledge and Confidentiality Agreement (see Appendix A).

- **Zero-Communication Rule:** Firewalled Team members are strictly prohibited from discussing, transferring, hinting at, or otherwise communicating any aspect of their work or Protected Information to any member of the Proposal Team.
- **No Dual Roles:** No individual may serve on both teams simultaneously, nor may any individual move from the Firewalled Team to the Proposal Team for the duration of this procurement.

C. Management and Supervisory Firewalls

- **Independent Reporting Structures:** Members of the Firewalled Team and the Proposal Team report to entirely different corporate vice presidents.
- **No Executive Crossover:** The executive overseeing the Proposal Team's bid strategy will have no oversight, review authority, or access to performance metrics regarding the Firewalled Team's current project.

4. Monitoring, Compliance, and Self-Reporting

- A. **OCI Compliance Officer:** [Insert Name/Title, e.g., General Counsel] is appointed as the OCI Compliance Officer. The OCI Compliance Officer shall oversee the Company's compliance with the requirements of this firewall plan.
- B. **Firewall Administrator:** [Insert Name/Title, e.g., Contracts Manager] is appointed as the OCI Administrator. The Firewall Administrator shall be responsible for the day-to-day operation of this firewall plan.
- C. **Audits:** The Compliance Officer will conduct, or request that the Administrator conduct, random, bi-weekly audits of data access logs and employee logs to verify firewall integrity.
- D. **Breach Protocol:** If any employee suspects a firewall breach (accidental or otherwise), the

employee must report it to the Administrator or Compliance Officer within 24 hours. If a breach is suspected to have occurred, the Company will immediately investigate and determine whether a breach has occurred.

- E. **Notification:** If a breach has been determined to have occurred, the Company will notify the government Contracting Officer (CO) with an impact assessment including proposed remedial effort.

5. Term and Termination

- A. **Term:** This firewall plan shall begin on the Effective Date stated above.
- B. **Termination:** This firewall plan shall remain in effect until Company's work on pursuit of the program (1) is formally terminated by the Company, or (2) the agency has made a final award and any protest or any protest period is over, or (3) the program is formally terminated by the agency, and (4) the Company communicates this termination to the two teams.

Appendix A: Employee OCI Acknowledgement & Confidentiality Agreement

I, [Employee Name], acknowledge that I have been assigned to the [Firewalled Team or Proposal Team] for [Project Name].

1. I received a copy of the Organizational Conflict of Interest (OCI) Firewall Plan for the [Program Name].
2. I acknowledge that I have received training under this Firewall Plan.
3. I understand that the Company is seeking a contract award and to succeed this Firewall Plan must be followed.
4. I understand that I am strictly prohibited from discussing any proprietary, non-public, or sensitive information regarding this project with members of the [state Firewalled or Proposal] team.

5. I certify that I will not access, or attempt to access, any electronic or physical files outside of my authorized team scope.
6. I understand that violating this agreement may result in corporate disciplinary action, up to termination, and could disqualify the company from federal contract awards.

Employee Signature: _____

Title: _____

Date: _____

Exhibit 2

Example of Impaired Objectivity Restrictions

For an impaired objectivity OCI, the mitigation plan must do more than isolate information. It should remove or neutralize the contractor's ability to evaluate, recommend, approve, inspect, test, audit, score, or otherwise influence decisions affecting its own work, affiliates, teammates, products, systems, or financial interests.

For example, the below are draft clauses that could be used as appropriate in a mitigation plan addressing impaired objectivity:

Impaired Objectivity Restriction. The Company shall not assign any employee, consultant, subcontractor, affiliate, or team member to perform evaluation, assessment, inspection, testing, validation, audit, source-selection support, requirements development, recommendation, approval, or oversight functions where that person or entity would be reviewing or influencing a government decision concerning:

1. the Company's own products, services, systems, proposals, or contract performance;
2. the work of any parent, subsidiary, affiliate, joint venture member, subcontractor, or teaming partner;
3. any vendor, supplier, or solution in which the Company has a financial, contractual, or competitive interest; or
4. any matter where the Company's business interests could reasonably be perceived as impairing independent judgment.

Recusal and Reassignment. Any individual who has a personal, financial, contractual, organizational, or prior-work connection to a matter under review shall immediately disclose that connection to the OCI Compliance Officer and shall be recused from the affected task. The Company shall reassign the work to personnel who are independent of the affected interest and who have no role in developing, selling, managing, or benefiting from the product, service, contract, or contractor being evaluated.

Independent Review Function. Where the Company is required to provide analysis, recommendations, testing, validation, or advisory support that could affect its own interests or those of an affiliate, teammate, subcontractor, or competitor, the Company shall establish an independent review function approved by the OCI Compliance Officer. The independent reviewer shall have no reporting relationship to the affected business unit and shall not be evaluated, compensated, or managed based on the outcome of the matter being reviewed.

Prohibited Recommendations. The Company shall not make, draft, edit, approve, or materially influence recommendations to the Government that would favor the Company, an affiliate, teammate, subcontractor, or proprietary solution unless the potential conflict has been disclosed to the Contracting Officer and the Government has approved a mitigation approach in writing.

Disclosure to the Government. If the Company identifies an actual, potential, or apparent impaired objectivity OCI, the OCI Compliance Officer shall promptly notify the Contracting Officer and provide a proposed mitigation plan. The Company shall not proceed with the affected work unless and until the Contracting Officer authorizes performance, approves the mitigation measures, or directs an alternative course of action.

Certification. Before performing any evaluation, advisory, inspection, testing, validation, audit, or recommendation function, assigned personnel shall certify that they have disclosed all relevant organizational, financial, contractual, and personal interests and that

they can perform the assigned work objectively and independently.

ENDNOTES:

¹FAR 2.101.

²FAR Subpart 9.5 (and the proposed reorganization to FAR 3.12) sets out the responsibilities for identifying, evaluating, and resolving OCIs. See Federal Acquisition Regulation: Preventing Organizational Conflicts of Interest in Federal Acquisition, 90 Fed. Reg. 4,376 (Jan. 15, 2025) (proposed rule).

³See Geldon & Conroy, “Organizational Conflicts of Interest Edition VI: Is the Pendulum Swinging Back at the GAO?” 18-13 Briefing Papers 1 (Dec. 2018); Cairnie & Kessler, “Organizational Conflicts of Interest/Edition V,” 12-13 Briefing Papers 1 (Dec. 2012); Cantu, “Organizational Conflicts of Interest/Edition IV,” 06-12 Briefing Papers 1 (Nov. 2006); Madden, Pavlick & Worrall, “Organizational Conflicts of Interest/Edition III,” 94-08 Briefing Papers 1 (July 1994); Taylor, “Organizational Conflicts of Interest/Edition II,” 84-8 Briefing Papers 1 (Aug. 1984).

⁴Press Release, H. Comm. on Oversight & Reform, Democratic Staff, Committee Releases Report Uncovering Significant Conflicts of Interest at McKinsey & Co. Related to Work for FDA and Opioid Manufacturers (Apr. 13, 2022), <https://oversightdemocrats.house.gov/news/press-releases/committee-releases-report-uncovering-significant-conflicts-of-interest-at>.

⁵Miller, “Three reasons why organizational conflict of interest is back in the spotlight,” Federal News Network (Aug. 15, 2022), <https://federalnewsnetwork.com/reporters-notebook-jason-miller/2022/08/three-reasons-why-organizational-conflict-of-interest-is-back-in-the-spotlight/>.

⁶Congress initially flagged OCIs when the military began heavily relying on private entities because it became clear that the same entities would have an unfair advantage if they also sought to pursue productions contracts. This concern led to the creation of the original OCI framework in the 1960s.

⁷DOD Directive 5500.1000, Appendix G, Armed Services Procurement Regulation (June 1, 1963). This is the foundation of OCI rules. It represents the first formal, government-wide regulatory framework to define and control OCIs. The June 1, 1963, directive outlined four specific scenarios where an OCI was presumed to exist, imposing strict restrictions on contractors:

The Systems Engineering Rule: If a contractor was hired to provide entirely independent systems engineering and technical direction for a weapons system, they were

barred from supplying the components or production hardware for that system.

The Specifications Rule: If a contractor was hired to draft the technical specifications or Statements of Work for a future competitive procurement, they were prohibited from competing as a prime contractor or subcontractor for that ultimate procurement.

The Evaluation Rule: If a contractor was hired to perform independent technical evaluations of competing products or technologies, they could not evaluate their own products or those of a direct corporate affiliate.

The Proprietary Data Rule: If a contractor gained access to another company’s proprietary or trade-secret information while performing a government contract, they were legally restricted from using that data to gain a commercial advantage in future bidding.

⁸48 Fed. Reg. 42,103 (Sept. 19, 1983) (The FAR became effective April 1, 1984).

⁹See Geldon & Conroy, “Organizational Conflicts of Interest Edition VI: Is the Pendulum Swinging Back at the GAO?,” 18-13 Briefing Papers 1, at 2 (Dec. 2018).

¹⁰FAR subpt. 9.5; see Taylor, “Organizational Conflicts of Interest/Edition II,” 84-8 Briefing Paper 1 (Aug. 1984).

¹¹Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, § 1402, 108 Stat. 3243, 3290 (1994) (amending 31 U.S.C.A. § 3553).

¹²See FAR 9.505(a)–(b), 9.505-1 to -4. FAR 9.505 identifies the two central principles of OCI doctrine: preventing conflicting roles that may bias contractor judgment and preventing unfair competitive advantage. FAR 9.505-1 addresses systems engineering and technical direction; FAR 9.505-2 addresses preparing specifications or work statements; FAR 9.505-3 addresses evaluation services; and FAR 9.505-4 addresses access to proprietary information. These provisions correspond to the familiar practice categories of biased ground rules, impaired objectivity, and unequal access to information.

¹³See FAR 9.505(a)–(b), 9.505-1 to -4. FAR 9.505 identifies the two central principles of OCI doctrine: preventing conflicting roles that may bias contractor judgment and preventing unfair competitive advantage. FAR 9.505-1 addresses systems engineering and technical direction; FAR 9.505-2 addresses preparing specifications or work statements; FAR 9.505-3 addresses evaluation services; and FAR 9.505-4 addresses access to proprietary information. These provisions correspond to the familiar practice categories of biased ground rules, impaired objectivity, and unequal access to information.

¹⁴See generally FAR 9.506; FAR 9.507-1 to -2;

FAR 9.508. These provisions address solicitation-stage procedures, solicitation provisions, contract clauses, and examples. They are important because OCI disputes often turn on what the solicitation required offerors to disclose, how the agency evaluated those disclosures, and whether the resulting record shows a reasoned CO judgment. FAR 9.508's examples also help translate the general FAR principles into recognizable acquisition scenarios, including work involving specifications, evaluation assistance, and access to proprietary or source-selection information.

¹⁵FAR 9.505.

¹⁶FAR 9.505-1(a).

¹⁷FAR 9-505(2)(a)(1).

¹⁸FAR 9.505-3.

¹⁹FAR 9.505-4(c).

²⁰Nat'l Aeronautics & Space Admin., National Aeronautics and Space Administration's Guide on Organizational Conflicts of Interest 4 (Mar. 2010), <https://www.nasa.gov/wp-content/uploads/2023/09/nasa-organizational-conflicts-of-interest.pdf> [hereinafter NASA Guide].

²¹FAR 9.506(b); see FAR 9.506(c), (d) & (e).

²²See FAR 9.507-1.

²³See NASA Guide, ch. 3.

²⁴See FAR 9.501, 9.502(b)–(c), 9.503, 9.504(a), 9.505.

²⁵DFARS 209.571-7(b)(1) & (2).

²⁶See DFARS subpt. 209.5, Organizational and Consultant Conflicts of Interest; DFARS 209.570; DFARS 209.571; DFARS 252.209-7008; DFARS 252.209-7009. The DFARS supplements the FAR by addressing DoD-specific OCI risks, especially in lead system integrator roles, SETA, and major defense acquisition programs. The DFARS provisions reflect DoD's heightened concern with lifecycle conflicts and contractor roles that can influence requirements, architecture, technical direction, or future competition.

²⁷See Weapon Systems Acquisition Reform Act of 2009, Pub. L. No. 111-23, § 207, 123 Stat. 1704, 1726–27; Defense Federal Acquisition Regulation Supplement; Organizational Conflicts of Interest in Major Defense Acquisition Programs, 75 Fed. Reg. 81,908, 81,908 (Dec. 29, 2010). Section 207 directed DoD to revise the DFARS to provide uniform guidance and tighten existing OCI requirements for major defense acquisition programs. The 2010 DFARS final rule implemented that direction and is a key point in the movement from broad FAR principles toward more structured DoD-specific OCI disclosure, mitigation, and compliance requirements.

²⁸DFARS 209.570-2(a).

²⁹DFARS 252.209-7008(c).

³⁰DFARS 252.209-7009(c),(d).

³¹DFARS 209.505-4.

³²DFARS 209.503-70(a), (b).

³³DFARS 252.209-7008.

³⁴DFARS 252.209-7009.

³⁵DFARS 209.503-70.

³⁶DFARS 209.571-2(b).

³⁷DFARS 209.571-2(b).

³⁸Executive Order No. 14275, Restoring Common Sense to Federal Procurement (Apr. 15, 2025), 90 Fed. Reg. 16,447 (Apr. 18, 2025).

³⁹<https://www.acquisition.gov/far-overhaul>.

⁴⁰See Federal Acquisition Regulation; Organizational Conflicts of Interest, 76 Fed. Reg. 23,236 (Apr. 26, 2011); Federal Acquisition Regulation; Organizational Conflicts of Interest, 76 Fed. Reg. 38,089 (June 29, 2011) (reopening comment period); Federal Acquisition Regulation; Organizational Conflicts of Interest, 86 Fed. Reg. 14,863 (Mar. 19, 2021) (withdrawing proposed rule); Federal Acquisition Regulation: Preventing Organizational Conflicts of Interest in Federal Acquisition, 90 Fed. Reg. 4,376 (Jan. 15, 2025). The 2011 FAR proposal attempted to revise government-wide OCI coverage, including treatment of contractor access to nonpublic information, but was later withdrawn without a final comprehensive FAR rewrite. The 2025 proposal reflects renewed congressional and regulatory attention to OCI prevention and signals potential movement toward more formal disclosure and mitigation expectations.

⁴¹Federal Acquisition Regulation: Revolutionary Federal Acquisition Regulation Overhaul Parts 3 and 49, 91 Fed. Reg. 37,698 (June 23, 2026) (proposed rule to be codified at 48 C.F.R. pts. 3, 49, 52). The June 23, 2026, proposed rules implementing the RFO address OCI. Under FAR Case 2026-007, the OCI rules are being moved to FAR Part 3, the ethical and integrity-focused section of the FAR, from the former FAR Subpart 9.5.

⁴²See 91 Fed. Reg. 37,698. Published on June 23, 2026, under FAR Case 2026-005 (Document Number 2026-12562), this proposed rule is part of a regulatory rollout implementing Executive Order No. 14275, Restoring Common Sense to Federal Procurement (Apr. 15, 2025), 90 Fed. Reg. 16,447 (Apr. 18, 2025). Because the RFO restructures the layout of procurement ethics, the rules governing business ethics, conduct, and OCI fall under the Parts 3 and 49 rewrite.

⁴³See DFARS 209.571-7(b)(2); Weapon Systems Acquisition Reform Act of 2009, Pub. L. No. 111-23, § 207, 123 Stat. 1704, 1726–27.

⁴⁴See generally FAR 9.506; FAR 9.507-1 to -2; FAR 9.508. These provisions address solicitation-stage procedures, solicitation provisions, contract clauses, and examples. They matter because OCI disputes often turn on what the solicitation required offerors to disclose, how the agency evaluated disclosures and mitigation plans, and whether the resulting procurement record shows a reasoned CO judgment.

⁴⁵See NASA Guide, ch. 3.

⁴⁶Aetna Gov't Health Plans, Inc., B-254397.15 et al., 95-2 CPD ¶ 129, 1995 WL 449806 (Comp. Gen. July 27, 1995). GAO sustained protests where an affiliate of one offeror's major subcontractor assisted the agency in evaluating proposals. The decision is important for its treatment of affiliate relationships, agency independence in OCI analysis, and the insufficiency of mitigation measures that do not address the practical significance of the conflict.

⁴⁷Lucent Techs. World Servs., Inc., B-295462, 2005 CPD ¶ 55, 2005 WL 525448 (Comp. Gen. Mar. 2, 2005). GAO denied a protest challenging exclusion where the agency reasonably determined that the protester had a biased ground rules OCI arising from its preparation of technical specifications used in the solicitation. The decision illustrates the risk that a contractor helping define requirements may later be unable to compete for the resulting work.

⁴⁸Alion Sci. & Tech. Corp., B-297022.3, 2006 CPD ¶ 2, 2006 WL 59564 (Comp. Gen. Jan. 9, 2006).

⁴⁹Alion Sci. & Tech. Corp., B-297022.4, B-297022.5, 2006 CPD ¶ 146, 2006 WL 2820168 (Comp. Gen. Sept. 26, 2006). GAO first sustained a protest where the record did not support the agency's assessment of impaired objectivity OCI risk involving contractor judgments that could affect the awardee's products, competitors, and customers. After corrective action, GAO denied a later protest where the agency documented its review and reasonably relied on fire-walled subcontractor mitigation.

⁵⁰Dell Servs. Fed. Gov't, Inc., B-414461, B-414461.2, 2017 CPD ¶ 192, 2017 WL 2831080 (Comp. Gen. June 21, 2017); Dell Servs. Fed. Gov't, Inc., B-414461.3, B-414461.4, B-414461.5, 2018 CPD ¶ 213, 2018 WL 3135121 (Comp. Gen. June 19, 2018); Dell Servs. Fed. Gov't, Inc., B-414461.6, 2018 CPD ¶ 374, 2018 WL 5994106 (Comp. Gen. Oct. 12, 2018). GAO sustained protests addressing unequal access and biased ground rules OCI concerns where the agency record did not adequately show meaningful analysis or mitigation of competitively useful nonpublic information. GAO later denied a challenge to the agency's waiver where the waiver was written, described the conflict, and was signed by an authorized official. The decisions underscore the importance of information access controls, meaningful agency analysis, and

properly executed waivers.

⁵¹Dell Servs. Fed. Gov't, Inc., B-414461, B-414461.2, 2017 CPD ¶ 192, 2017 WL 2831080 (Comp. Gen. June 21, 2017).

⁵²Dell Servs. Fed. Gov't, Inc., B-414461.3, B-414461.4, B-414461.5, 2018 CPD ¶ 213, 2018 WL 3135121 (Comp. Gen. June 19, 2018).

⁵³Dell Servs. Fed. Gov't, Inc., B-414461.6, 2018 CPD ¶ 374, 2018 WL 5994106 (Comp. Gen. Oct. 12, 2018).

⁵⁴See Axiom Res. Mgmt., Inc. v. United States, 564 F.3d 1374, 1380–81 (Fed. Cir. 2009), rev'g Axiom Res. Mgmt., Inc. v. United States, 78 Fed. Cl. 576 (2007). The Federal Circuit reversed an injunction that had set aside an Army TRICARE support services award based on alleged impaired objectivity and unequal access OCIs. The decision emphasizes record-based review under the arbitrary-and-capricious standard and limits supplementation of the administrative record to circumstances necessary for meaningful judicial review.

⁵⁵See Weapon Systems Acquisition Reform Act of 2009, Pub. L. No. 111-23, § 207, 123 Stat. 1704, 1726–27.

⁵⁶See Federal Acquisition Regulation: Preventing Organizational Conflicts of Interest in Federal Acquisition, 90 Fed. Reg. 4,376 (proposed Jan. 15, 2025) (proposed rule amending the FAR to implement Preventing Organizational Conflicts of Interest in Federal Acquisition Act, Pub. L. No. 117-324, 136 Stat. 4459 (2022)). Its primary goal is to tighten rules and prevent corporate contractors from advising federal agencies while simultaneously working for private entities with opposing interests.

⁵⁷U.S. Gov't Accountability Off., GAO-07-380, "Defense Acquisitions: Role of Lead Systems Integrator on Future Combat Systems Program Poses Oversight Challenges" (June 6, 2007). For OCI purposes, this report shows Congress became concerned about contractors occupying positions normally associated with governmental oversight and acquisition management.

⁵⁸See Squeo, "Boeing's Role in Defense Project Worries Pentagon, Competitors," Wall St. J., June 16, 2003.

⁵⁹See generally FAR 9.506; FAR 9.507-1, -2; FAR 9.508. These provisions address solicitation-stage procedures, solicitation provisions, and contract clauses.

⁶⁰An example of an OCI article from a teaming agreement:

Article 12. Organizational Conflict of Interest (OCI)

12.1 Party Disclosure and Assessment by Team Mem-

bers. The Team Members understand that [the buying agency] is concerned about Organizational Conflict of Interest (OCI) and will enforce OCI regulations under the Federal Acquisition Regulation (FAR). Each Team Member hereby represents that, to the best of its knowledge and belief, that no OCI exists regarding its participation in this Program or the resulting Contract. If a Team Member identifies an actual or potential (whether Unequal Access to Information, Biased Ground Rules, or Impaired Objectivity) at any time during this Agreement, it shall immediately notify the other Team Members in writing within one working day.

⁶¹For example, such a provision in a teaming agreement could state that: “If the Prime Contractor concludes that an OCI cannot be mitigated, and such OCI would disqualify the entire Team from competing for or receiving the award, the Prime Contractor shall have the right to immediately terminate this Teaming Agreement with respect to the Subcontractor without liability. In such an event, the Prime Contractor may proceed with the solicitation independently or with a replacement teammate, and the Subcontractor shall be released to pursue other opportunities, provided all proprietary information is returned or destroyed.”

⁶²See FAR 505-1; FAR 9.508(a); DFARS 209.571-7.

⁶³“Incumbent advantage” is generally considered a legitimate byproduct of contract performance, whereas an unequal access to information OCI arises when the advantage comes from access to competitively useful, nonpublic information that other offerors cannot obtain. FAR OCI rules are aimed at the latter, not the former. If all such knowledge created an OCI, agencies would constantly have to exclude incumbents from recompetes.

⁶⁴See Lukos-VATC JV III, LLC, B-418427.9, B-418427.11, 2021 CPD ¶ 43, 2020 WL 8665285 (Comp. Gen. Dec. 22, 2020).

⁶⁵See FAR 9.505-3.

⁶⁶Aetna Gov’t Health Plans, Inc., B-254397.15 et al., 95-2 CPD ¶ 129, 1995 WL 449806 (Comp. Gen. July 27, 1995).

⁶⁷See DFARS 209.571-4.

⁶⁸ <https://govtribe.com/file/government-file/fa880625rb003-attachment-5-dot-organizational-conflict-of-interest-checklist-dot-pdf>.

⁶⁹The simple firewall plan provided as Exhibit 1 to this Briefing Paper is an example. It provides the basic framework often utilized by contractors.

⁷⁰The additional clauses seen in Exhibit 2 to this Briefing Paper provide some clauses that may be useful for impaired objectivity OCI situations.

⁷¹See Leidos, Inc., B-417994, 2019 CPD ¶ 425,

2019 WL 7019036 (Comp. Gen. Dec. 17, 2019).

⁷²See DirectViz Sols., LLC, B-423366, B-423366.3, B-423366.4, 2025 CPD ¶ 137, 2025 WL 1745028 (Comp. Gen. June 11, 2025). (GAO sustained the protest, explicitly ruling that an agency cannot rely on “after-the-fact assumptions” or treat a broad internal corporate firewall as a catch-all solution without conducting a specific, fact-based structural inquiry.)

⁷³See A Square Grp., LLC, B-421792.2, B-421792.3, 2024 CPD ¶ 139, 2024 WL 3103880 (Comp. Gen. June 13, 2024). (GAO determined that despite the agency documenting that the awardee’s OCI had been mitigated, the actual risk of an impaired objectivity conflict remained entirely unaddressed by the plan’s concrete mechanics.)

⁷⁴See Steel Point Sols., LLC, B-419709, B-419709.2, 2021 CPD ¶ 254, 2021 WL 3172103 (July 7, 2021). (GAO sustained the protest because the CO did not perform a rigorous, fact-specific investigation into the overlapping contract duties, proving general oversight or generic mitigation statements are insufficient.)

⁷⁵See 9-505 (“Each individual contracting situation should be examined on the basis of its particular facts and the nature of the proposed contract.”).

⁷⁶See FAR 9.504.

⁷⁷Although not specifically designated as an OCI review, defense and technology mergers reviewed by the Department of Justice (DOJ) or the Federal Trade Commission (FTC) often receive scrutiny regarding vertical integration, access to competitively sensitive information, and the ability to influence procurements. These facts overlap with OCI analysis. Examples include:

- Northrop Grumman/Orbital ATK (2018)—FTC required behavioral remedies because Orbital supplied critical components used by competing missile manufacturers. The concern mirrored OCI concepts involving access to competitively sensitive information and the ability to disadvantage competitors.
- L3 Technologies/Harris Corporation (2019)—regulators reviewed how the merged company would interact with competing contractors and programs across multiple defense portfolios.
- Lockheed Martin/Aerojet Rocketdyne (2020–2022)—FTC reviewed whether a merchant supplier would work with multiple primes competing for the same award and whether the firewalls

and other components of the mitigation plan would be sufficient.

Martin/Aerojet Rocketdyne merger reviews mentioned in endnote 77, above.

⁷⁸This is the situation reviewed by the FTC in the Northrop Grumman/Orbital ATK and the Lockheed