Morgan Lewis

TECHNOLOGY MARATHON

Government Contractor Considerations and Risks in Technology Transactions

Presenters: Sheila A. Armstrong, Barron W. Avery, Carl A. Valenstein, Casey Weaver

Date | 3:00-4:00 pm ET

Before we begin

Tech Support

If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.

Q&A

The Q&A tab is located near the bottom right hand side of your screen; choose "All Panelists" before clicking "Send."

CLE

We will mention a code at some point during the presentation for attendees who requested CLE. Please make note of that code, and insert it in the pop-up survey that will appear in a new browser tab after you exit out of this webinar. You will receive a Certificate of Attendance from our CLE team in approximately 30 to 45 days.

Audio

The audio will remain quiet until we begin at 3:00 ET.

You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.

To access the audio for by telephone, please click the "phone" icon below your name on the Participants Panel for teleconference information.

Presenters

Sheila A. Armstrong

W. Barron A. Avery

Carl A. Valenstein

Casey Weaver

Morgan Lewis

Agenda

- General Landscape
- Particular Risks and Considerations
  - Specialized Due Diligence
  - Small Business Considerations
  - Organizational Conflicts of Interest
  - Cybersecurity Obligations
  - Protecting Intellectual Property Rights
  - Additional Concerns
- Diligence Identified an Issue. Now What?
  - Mitigation of Risk
  - False Claims Act Liability
- Structuring the Deal
  - Novation, Assignment, and Consent
  - Security Clearance, FOCI, and Export Controls
  - Deal Considerations

General Landscape

Morgan Lewis

Increased Transactions Involving the Government

- Many technology companies don't think of themselves as government contractors, but they often have material amounts of government contracting exposure, and these issues are germane to many tech businesses.
- M&A activity remains strong, including among government contractors, driven by both strategic buyers and private equity and venture capital. These transactions often involve government funding or contracts.
- Government budgets are growing, and the current administration has been more favorable to Defense and Intelligence spending than originally predicted. Increased government funding of emerging and foundational technologies as well as domestic infrastructure. Novel use of the Defense Production Act.
- Prioritization of spending has been on RDT&E, cyber, space, data, and IT to improve US defensive posture.
- NextGen IT, cybersecurity, cloud computing, digital transformation and modernization, DevSecOps, and data analytics are all high-end value-add capabilities that drive enhanced valuation.

Increased Transactions Involving the Government

- Private equity groups and venture capital investments remain active in the technology/government contracting sector.
- Buyers pursue targets with key contract vehicles to overcome a powerful barrier to entry (which also comes with premium value).
- Small businesses that may outgrow their status often seek a buyer.
- Government contractors may spin-off business units or companies to mitigate the risks of organizational conflicts of interest.
- While the macro environment is favorable for deals, some headwinds are mounting in the form of sustained inflation, tightened monetary policy, credit conditions, and general economic slowdown.

Operational Risks and Hidden Liabilities

- Potential civil and criminal penalties for non-compliance with contractual, statutory, and regulatory requirements.
- Long-term revenue and valuation projections are challenging given the Government's termination rights, short-term contract structure, and funding profiles.
- Government audit rights allow for retroactive cost or pricing adjustments.
- Mandatory reporting obligations and whistleblower rights amplify the need to proactively address potential compliance problems.
- It is thus important to have specialized government contracts counsel involved in the diligence and in the transaction.

Particular Risks and Considerations

Morgan Lewis

Specialized Due Diligence

Morgan Lewis

Specialized Due Diligence

- Government contracting is a highly regulated environment with compliance and business risks that differ from purely commercial transactions.
- Diligence involves requesting and reviewing detailed information about the seller's government work, which may feel burdensome.
- Thorough diligence is crucial because a failure to comply with the terms of a government contract can result in treble actual damages and statutory penalties under the civil False Claims Act and potentially lead to suspension and debarment, which may be the death knell of the company.
- Threshold issues can affect the structure of the transaction and planning such as (1) whether any foreign ownership or control is contemplated; (2) whether the target has security clearances; (3) whether the target is subject to export controls; (4) whether the target benefits from special preferences or set aside programs.

Typical Diligence Topics

- Contractor Responsibility
- Outstanding Proposals
- Past and Ongoing Performance
- History of Claims or Requests for Equitable Adjustment
- Historic, Pending, and Potential disputes
- Small Business Considerations
- GSA/VA MAS Contract Compliance
- Industrial Security Compliance
- Cost Accounting and Pricing Compliance
- Organizational and Personal Conflicts of Interest
- Internal compliance policies, procedures, and training programs
- Internal Investigations and Disclosures
- Compliance with Ethics Rules

Specialized Considerations

- Materiality Threshold
  - Does the materiality threshold established for the deal make sense for the target's government contracts?
  - Consider lower or no materiality threshold for government contracts due to greater risks.
- Lookback Period
  - Is the lookback period for the deal sufficient?
  - Government audit rights generally extend for 3 years after final payment
  - FCA considerations, SOL is 3/6/10 years
  - May consider looking at certain contracts performed prior to the lookback period.
- Escrow Period or R&W Insurance
  - Is the escrow period long enough to protect from issues arising from its government contracts?
  - Consider holding a portion of the escrow for a longer period if concerns involving the target's government contracts arise during due diligence.
  - If using R&W insurance, ensure that the R&W apply to all government contracts, including any classified contracts, and that they adequately address the risk of suspension and debarment and contract termination regarding past and present compliance obligations, as well as the risk of termination or exclusion from future contracts related to compliance with socio-economic obligations.

Effect on Target Business Prospects

- Loss of eligibility for contracts set aside for small businesses, veteran-owned businesses, 8(a) companies, woman-owned, and HUBzone companies.
- Service Disabled Veteran status is usually lost.
- Contracts set aside under the 8(a) program may be terminated for convenience.
- Small business size recertification is generally required under IDIQ and long-term contracts.
- Organizational conflicts of interest ("OCI") concerns may arise due to the acquisition that can preclude a company from bidding on certain programs.

Small Business Considerations

Morgan Lewis

Small Business Preference

- Some government contracts are set aside for small businesses, and in other cases, small businesses may receive preferential treatment in the evaluation and source selection process.
- SBA regulations provide that a company qualifies as a small business concern by meeting requirements for either number of employees or annual average gross revenue, including all affiliates, for preceding five fiscal years based on applicable NAICS codes.
- The primary obstacle to investing in small businesses, from a government contracts perspective, is that small businesses generally lose their small business size status as the result of a corporate transaction because of the doctrine of "affiliation."

Small Business Affiliation

- Affiliation rules can be tricky and generally apply very broadly.
  - A person is an affiliate if it owns or controls or has the power to control 50% or more of a company's voting stock. Actual control is irrelevant if the power to control exists.
  - Companies are also affiliates of each other if a third company controls or has the power to control (directly or indirectly) both companies.
- Factors including ownership, management, previous relationships with or ties to another business, and contractual relationships are all relevant in analyzing the issue of control.
- The government treats the contractor and its affiliates as a single entity by aggregating their employees and gross receipts when determining size status.

What if the transaction results in a size change?

- If a transaction results in a change in size status, the small business contractor must notify relevant contracting officers and update its SAM registration within 30 days.
- Buyers should identify any contracts that are small business set-aside awards and determine whether the target will continue to qualify after the transaction.
- If the target will not qualify, the buyer should consider:
  - The risk that the Government might terminate existing contracts for convenience or decline to exercise options;
  - Whether there are opportunities for large businesses to perform similar work or whether such contracts are typically set aside for small businesses;
  - The likelihood that the target, as a large business, will be able to compete against small businesses in that space; and
  - The fact that the business could be exposed to requirements from which a small business is exempt, e.g., cost accounting standards, business ethics program, and robust control systems.

Cybersecurity Obligations

Morgan Lewis

Technology and Cybersecurity

- The Government has increasingly focused on cybersecurity obligations for federal contractors, which creates an increased risk of related FCA liability.
- DOJ Civil Cyber-Fraud Initiative places cybersecurity non-compliance at heighted risk of FCA allegations.
- Key contract provisions include –
  - FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
  - DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
  - DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements
  - DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements

20

President Biden's Cybersecurity Executive Order

- Organizations must define "critical" software in their products and provide a software BOM to include all components—libraries, drivers, firmware, licenses, and operating systems.
- Seeks to remove obstacles to sharing threat information between federal agencies and the private sector.
- Mandates software purchased by the federal Government meet new cybersecurity standards.
- Emphasizes zero-trust architecture and secure cloud systems.
- Applies throughout the federal supply chain, not only to prime contractors.
- Assess whether the target has adequate safeguards in place and appropriate policies and procedures for providing required information.

Cybersecurity Maturity Model Certification

- CMMC is still evolving and is currently applicable only to select pilot contracts.
- CMMC will ensure that defense contractors are all meeting a basic level of cybersecurity hygiene for protecting sensitive unclassified defense information.
- Consists of five cumulative levels practices ranging from basic to advanced cybersecurity and processes ranging from performed to optimizing.
- It is designed to subject all DoD contractors to cybersecurity assessments
  - Companies that process, store, or handle Federal Contract Information (FCI) but not CUI and are associated with CMMC Levels 1 or 2 may complete a **self assessment**.
  - Contractors managing information critical to national security must undergo **third-party assessments**.
  - The highest priority, most critical defense programs will require **government-led assessments**.

FedRAMP Compliance

- FedRAMP requires that covered companies implement a set of security controls to ensure that all federal data is secure in cloud environments.
- All cloud service providers (including IaaS, PaaS, SaaS applications) that are used by federal agencies or want to pursue these types of business partnerships in the future must demonstrate FedRAMP compliance.
- At a high level, FedRAMP requires covered companies to implement a set of security controls, parameters, and requirements within their cloud computing environment, document how those controls are implemented in a System Security Plan, go through an independent assessment, and submit a set of documents to authorizing officials for review.
- FedRAMP also requires covered entities to implement a continuous monitoring program to ensure their cloud system maintains an acceptable risk posture.

Cybersecurity Diligence

- Determine whether seller is subject to specific cybersecurity obligations and, if so, whether it has taken steps necessary to implement required security protocols or has obtained waivers from the contracting officer.
- Review whether seller's contracts include other cybersecurity requirements and assess system compliance, identifying any gaps in capabilities.
- Identify any non-standard or burdensome default, indemnification, or liquidated damages provisions related to cybersecurity breaches.
- Assess IT compliance training materials, basic security protocols, and any known cyber incidents or breaches and accompanying governmental disclosures.
- Buyer may include representations and warranties regarding seller's cybersecurity compliance and risk of cyber incidents.

Protection of Intellectual Property Rights

Morgan Lewis

Protection of Intellectual Property Rights

- Protection of Intellectual Property Rights is uniquely challenging in government contracts.
- Under the Bayh-Dole Act, the Government generally obtains very broad license rights in software and technical data pertaining to items, components, or processes developed under a government contract.
- These rights can be limited, but the Government is entitled to a royalty-free license in perpetuity, which includes the right to sublicense to a competitor and certain march-in rights.
- The Government obtains "unlimited rights" in technical data and software where the Government paid all or part of the development costs, which include the right to disclose the data to the originating contractor's competitors.

Protection of Intellectual Property Rights

- The Government obtains only "limited rights" in technical data where item was developed exclusively at private expense, which include the right to disclose the data for maintenance or emergency repair of the item. Any third party to whom a disclosure is made must agree to protect the contractor's limited rights.
- Contractors can limit the Government's rights in technical data and computer software pertaining to privately developed technologies, but this requires planning and discipline, including, for example, use of prescribed restrictive legends and maintaining adequate records to establish development at private expense.
- The Government obtains "restricted rights" in software developed at private expense. The Government can disclose the software to a support services contractor that agrees to the restrictive rights.
- Generally, in a commercial item procurement, the Government obtains only the same data and data rights provided to commercial customers.

Protecting Intellectual Property Rights

- Regarding patents, the Government generally obtains broad license rights in, and the contractor generally retains ownership of, inventions conceived or first actually reduced to practice under a government contract (i.e., "subject inventions").
- The contractor can lose its rights in a subject invention, however, if it does not timely disclose that invention to the Government.
- Most government contracts data and patent rights clauses must be flowed down to subcontractors, so a buyer should analyze the clauses included in a material government contract, identify what intellectual property was developed at private expense, and determine whether the target has complied with the administrative burdens necessary to protect its intellectual property rights, including obligations related to disclosure, marking, and recordkeeping.
- Some buyers also seek robust representations and warranties, particularly where intellectual property is an important aspect of the target's business.

Organizational Conflicts of Interest

Morgan Lewis

Categories of OCI

- An **unequal access to information** OCI arises where a contractor has access to nonpublic information that would give it an advantage in a later competition for a government contract. Such non-public information may include proprietary or source selection information, as well as other information beyond that available to a typical incumbent contractor.
- An **impaired objectivity** OCI typically occurs when a contractor's work under one government creates a situation that benefits other government contracts.
- A **biased ground rules** OCI typically occurs where a contractor, as part of its performance of a government contract, has set the ground rules for another procurement, e.g., by drafting specifications or the statement of work.

Impacts of Possible OCI

- The Government cannot award a contract to a contractor that has an OCI unless the conflict has been mitigated or waived.
- Many government contracts include clauses that require contractors to avoid potential OCIs, to notify the Government of any OCIs that arise after award, and to work with the Government to mitigate any such OCIs. OCIs are often mitigated by some agreed upon preclusion on future work.
- A contractor and its affiliates are generally treated as a single entity for purposes of biased ground rules and impaired objectivity OCIs. Purchasing a target that advises the Government on acquisitions or evaluates products or services for the Government, for example, could preclude the buyer – not just the target – from competing to supply those same products or services to the Government under other contracts.

Due Diligence on OCI

- Understand the target's business in relation to the buyer's business.
- Review the terms and conditions and statements of work for the target's significant government contracts, paying special attention to contracts that include express OCI clauses or preclusions of future work.
- Review the target's OCI mitigation plans.
- Analyzing OCI implications may also require internal diligence for the buyer to determine potential impact of the transaction.

Additional Concerns

Cost and Accounting Concerns

- Contracts for commercial items and services, e.g., those of a type generally available to the public and used for non-government purposes, present a lower compliance risk than contracts for non-commercial items and services.
- At the opposite end of the spectrum, cost-reimbursement contracts and contracts awarded on a non-competitive basis impose a higher level of risk.
- Depending on the value of the relevant contract, the contractor may be required to certify that it has disclosed to the Government all facts that would reasonably affect price negotiations or that it has complied with Cost Accounting Standards.
- Cost reimbursement contracts are subject to the Cost Principles, which address the types of costs for which the Government will and will not reimburse.
- Failure to comply can result in liability, including cost disallowance and FCA violations.

Socio-Economic Requirements

- Government contractors must comply with a host of socio-economic requirements, including for example those related to equal opportunity, affirmative action, prevailing wage rates, and employee eligibility verification.
- In addition to impose substantive obligations, these clauses include extensive recordkeeping and reporting requirements.
- Noncompliance can result in consequences ranging from the assessment of liquidated damages to contract termination and, potentially, suspension or debarment from government contracting.
- A buyer should determine whether the target has adequate policies and procedures to ensure compliance, and should review the target's standard form subcontracts to ensure that all mandatory clauses are being flowed down.

Past Performance and Responsibility

- Agencies use records from the CPARs database in evaluating a contractor's past performance, and anything lower than "Satisfactory" can negatively impact a contractor's ability to obtain future work.
- Buyers should request CPARs for material contracts and consider representations and warranties regarding adverse past performance.
- It is also advisable to identify any contracts that have been terminated, to request any "cure" or "show cause" notices that have been received, and to analyze those records to determine the level of risk they present to the business, in terms of both any immediate financial impact and the long-term ability to secure future work.

GSA/VA Multiple Award Scheule Contracts

- GSA and VA award MAS contracts for commercial items
- The MAS program is one of largest federal programs, GFY 2021 reported sales:
  - GSA $39.6B
  - VA $16.3B
- Most contracts include MFC pricing provision and pre-award pricing disclosure requirements
- Many FCA settlements over the past two decades were based on allegations of non-compliance with MAS contract requirements


Diligence Identified
an Issue. Now What?
Morgan Lewis

Mitigation of Risk

Importance of Specialized Reps and Warranties

- Typical commercial representations and warranties are insufficient to identify and address the particular risks encountered by a federal contractor.
- Specialized representations and warranties are necessary to force disclosure of government contract issues and set up appropriate indemnities.
- The buyer should ensure the purchase agreement addresses concerns specific to government contracting, including:
  - The contractor's responsibility and performance;
  - The contractor's knowledge of facts or circumstances that would result in a mandatory disclosure obligation;
  - Potential civil or criminal liability; and
  - The contractor's compliance with statutory, regulatory, and contractual obligations.

Indemnification

- The buyer often will seek indemnification for the target's noncompliance with government contracting obligations identified during diligence or disclosed in the purchase agreement disclosure schedules.
- Indemnification can help to mitigate the risks associated with:
  - Significant civil or criminal liability
  - Termination of existing federal contracts
  - Foreclosure of future federal contracts
  - Suspension or debarment

Audits and Investigations

- Government audit reports, correspondence with government auditors and investigators, and mandatory disclosures are valuable tools for identifying and quantifying the regulatory compliance and liability risks associated with the acquisition of a government contractor.
- The target may also have conducted internal audits of government contracting compliance, which can provide valuable insight to potential concerns.
- Sophisticated buyers typically request copies of these documents as well as representations and warranties regarding the target's knowledge of any pending audits and investigations. The definition of "knowledge" often becomes a point of contention.

Mandatory Disclosures

- FAR 52.203-13 applies to contracts valued at over $6M with a performance period over 120 days.
- Requires the contractor to:
  - Have a written code of conduct that is available to all employees.
  - Exercise due diligence to prevent and detect criminal conduct and promote an ethical culture committed to compliance.
  - ***Timely*** disclose in writing to the contracting officer and agency inspector general ***credible evidence*** that a principal, employee, agent, or subcontractor has committed a criminal violation or violation of the FCA ***in connection with the award, performance, or closeout of a contract.***
- FAR 9.4 extends this obligation to ***significant overpayments***, which are reason for most of mandatory disclosures we file.

Mandatory Disclosure

- Under the "look back" provision, the rule requires disclosure of covered misconduct "until 3 years after final payment" under the contract.
- The terms "timely disclosure" and "credible evidence" are intentionally undefined and confirm that the contractor has some time for a preliminary investigation before a disclosure is mandatory.
- Contractors must document investigations of misconduct and promptly reach conclusions regarding the existence of credible evidence.
- Buyers must include diligence request and insist on representations that will facilitate disclosure of internal investigations and violations of procurement statutes, regulations, and contract terms so that these risks can be fully evaluated and, if necessary, disclosed.

Debarment and Suspension

- Suspension and debarment are administrative actions to protect the Government from contractors that are not ***presently*** "responsible" by excluding the contractor from government contracts, grants, and other programs.
- Debarment from contracting with the Government typically last 3 years and ***can be the death knell*** of a contractor.
- Individuals can be debarred for ethical reasons, and certain "Principals" can be debarred for not reporting violations of law involving fraud and other issues to the IG and CO.
- Debarments for 2021 totaled 884 firms, individuals, and special entities.
- During due diligence, the acquirer should use representations and diligence to uncover and assess any matters or investigations that could potentially lead to suspension or debarment.

Your CLE Credit Information

For ALL attorneys seeking CLE credit for attending this webinar, please write down the alphanumeric code on the right >>

Kindly insert this code in the **pop-up survey** that will appear in a new browser tab after you exit out of this webinar.

False Claims Act

Morgan Lewis

False Claims Act

- Primary enforcement tool used by DOJ to combat federal program fraud
- Cases can be brought by the government or *qui tam* relators who receive 15-30% of proceeds
- In FY2021: DOJ recovered $5.69 billion under the FCA
  - Nearly $1.6 billion of this in 598 *qui tam* cases
  - Whistleblowers recovered $237 million
- Matters historically settled as breach of contract actions are now frequently alleged to violate the FCA

False Claims Act

- In general, the FCA provides for civil liability for: (1) knowingly presenting, or causing to be presented, a false claim for payment or approval to the Government; (2) knowingly presenting, or causing to be presented, a false record or statement material to a false claim; and (3) a conspiring to commit a violation of (1) or (2) above.
- Specific intent is not required.
  - "Knowingly" means that a person, with respect to information, has (1) actual knowledge of the information; (2) acts in deliberate ignorance of the truth or falsity of the information; or (3) acts in reckless disregard of the truth or falsity of the information.
  - **Recklessness standard implicates adequacy of contractor systems**
- A "claim" is any request or demand for money or property, and it is "false" if it is factually false or includes an express or implied false certification.

Liability Under the FCA

- Treble damages are automatically imposed, and many courts believe they lack discretion to reduce the award of damages absent a voluntary disclosure by the violator.
- In addition to treble damages, a minimum statutory penalty is imposed of $12,537 to $25,076 per false claim as of May 9, 2022.
- The successful relator (whistleblower) can share in 15% to 30% of the government's recovery. Relators are protected.
- Government audit rights extend many years after final payment and the FCA statute of limitations is 6 years.
- During due diligence, any actual or threatened investigations or issues that could lead to FCA liability must be identified and assessed.

Structuring the Deal

Morgan Lewis

Novation, Assignment, and Consent

Morgan Lewis

Novation

- An agency may approve the assignment of a Government contract through a **novation**, which is a three-party agreement among the Government, the prime contractor (transferor), and the successor-in-interest (transferee).
- The agency typically seeks assurance that the transferee is responsible and has the financial and technical ability to perform the contracts.
- A novation may take place only **post-closing**, and the original contractor remains responsible until the novation agreement is fully executed, and potentially thereafter by a guarantee of future performance in the novation agreement.
- If the transaction is structured as a stock purchase or reverse triangular merger, then the novation processes generally can be avoided.
- Consider novation when structuring the deal as pursuing novation takes time and effort, the relationship between transferor and transferee must continue post-closing, and novation is subject to the Government's discretion.

Novation Agreements

- Restrictions on assignment may be included in subcontracts for competitive reasons. During diligence, identify all subcontracts that limit assignments or require approval of a change of control.
- If a novation is required, identify appropriate lead contracting officer and address when to begin discussions
- The standard novation agreement provides that: (1) the transferor guarantees performance of the contract by the transferee; (2) the transferee assumes all of the transferor's obligations; (3) and the transferor waives all rights and remedies under the contract against the Government.

Novation Deal Terms

- Novation cannot be a condition to closing.
- Consider a subcontract for performance from close until novation is complete as the transferor remains responsible for performance.
- Recognize that it can take months for contracting officer to process novation.
- Address in the purchase agreement what happens if the Government denies a novation request.

Security Clearances, FOCI, and Export Controls

Morgan Lewis

Security Clearances

- A U.S. company must obtain a facility security clearance ("FCL") to access classified materials.
- Personal security clearances are required for key management personnel and the Facility Security Officer ("FSO") and persons who need access.
- Cleared U.S. companies must submit an SF-328 disclosing any foreign ownership, control or influence ("FOCI") (5% ownership may be significant).
- An acquiring company should review the results of the annual inspections by DSS for each facility, the SF-328, and any FOCI mitigation measures in place.
- A company under FOCI cannot hold an FCL unless the FOCI is negated or mitigated to the satisfaction of the Government.
- Asset sales raise issues because FCLs do not transfer with assets. The acquiring company will need an FCL to accept the assets.
- Approach DSS early in the process to address any questions/concerns.

Mitigation of FOCI

- A foreign interest that owns or controls a cleared U.S. company may take steps to mitigate the FOCI and maintain the company's FCL.
- FOCI issues and mitigation plans must be considered in structuring the transaction and in the contemplated board membership.
- When a contractor with an FCL enters into negotiations that could result in takeover by a foreign interest, DSS must be notified at the "commencement of such negotiations." NISPOM 2-302(g).
- FOCI mitigation plans may include: board resolutions, a Security Control Agreement, Voting Trust, Special Security Agreement and other measures.
- A notice of change of control and a revised SF-328 normally must be submitted when the merger or acquisition of a cleared company is completed, or when there have been changes to the answers on the SF-328.
- Access to Top Secret, SCI, COMSEC and other types of information by a company subject to FOCI may require other approvals such as National Interest Determination.
- Mitigation of FOCI is separate from the Exon Florio/CFIUS process.

Export Controls and National Security

- If the target has export control licenses under either the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR), the target must notify the government of the impending change and coordinate with the government post-closing to transfer registrations and licenses.
- The Committee on Foreign Investment in the United States (CFIUS) is authorized to review transactions that could result in foreign control of US businesses to determine the effect on national security.
- CFIUS review is effectively mandated for acquisitions involving contractors with:
  - Security clearances;
  - Exports of certain controlled items; or
  - Significant defense, national security, or homeland security contracts.

Deal Considerations

Morgan Lewis

Post-Closing Obligations

- Notification to the Government
  - Change in ownership, with size re-representation if the company is a small business
    - Within 30 days of the change in ownership, if no novation is required; or
    - Within 30 days of the execution of the novation agreement.
  - Transfer of security clearances
  - Notice to DDTC for ITAR registrants is required within **5 days of the event** if there is a material change in its Statement of Registration and **at least 60 days in advance** of a sale or transfer to a foreign person.
- Update the entity's SAM Registration to confirm accuracy
- Promptly address any noncompliance identified during due diligence

Sell-Side Considerations

- Sellers should review their Code of Conduct and compliance programs for FCA violations, FCPA, ITAR, and other areas as these will be scrutinized, especially by a strategic buyer. Consider cleaning house and making voluntary disclosures of past non-compliance.
- If transaction will result in foreign ownership or control, consider need for Exon-Florio/CFIUS review and mitigation of FOCI. If clearances are required, need to assess how easily the Buyer can qualify. These issues may increase deal completion risk.
- Sellers may prefer a stock transaction or reverse triangular merger to avoid a novation agreement which provides for Seller's continued liability to the government for contract performance.

Buy-Side Considerations

- Buyers should conduct specialized due diligence and include specialized representations and warranties.
- Buyers should consider special indemnities and escrows to cover potential government contract liabilities.
- If buyer is a foreign person, then clearance under Exon-Florio/CFIUS and mitigation of FOCI need to be addressed and associated deal completion risk.
- Consider restructuring the transaction as a stock purchase or reverse triangular merger to avoid the need for novation of government contracts.
- Develop plan for maintenance of required security clearances and export control licenses.

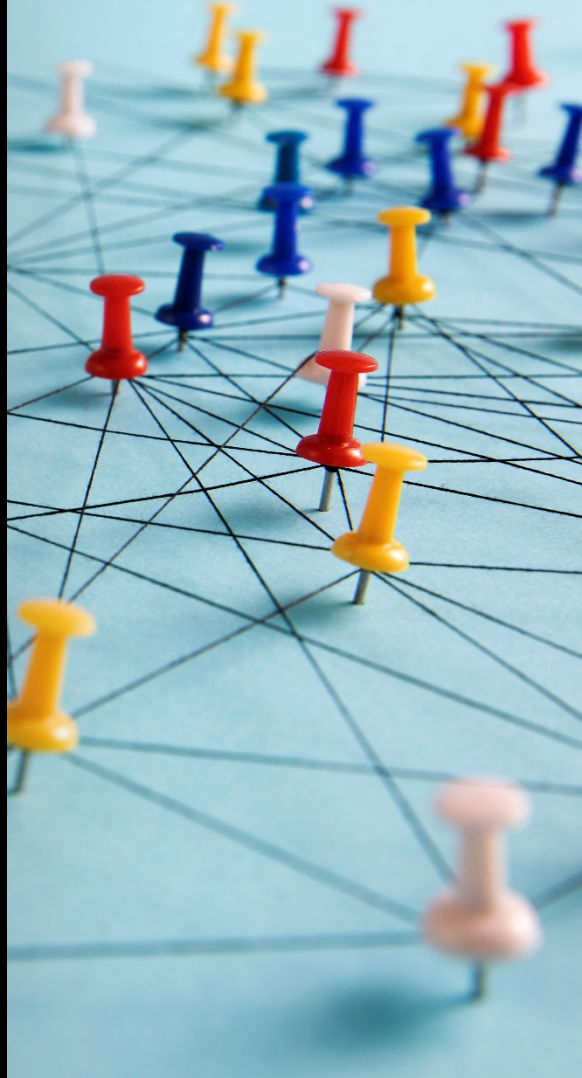
Ukraine Conflict Resources

Our lawyers have long been trusted advisers to clients navigating the complex and quickly changing global framework of international sanctions. Because companies must closely monitor evolving government guidance to understand what changes need to be made to their global operations to maintain business continuity, we offer a centralized portal to share our insights and analyses.

Morgan Lewis

To help keep you on top of developments as they unfold, visit the website at **www.morganlewis.com/topics/ukraine-conflict**

To receive a daily digest of all updates, please visit the resource page to **subscribe** using the "Stay Up to Date" button.



Biography

Sheila A. Armstrong
Dallas, TX
+1.214.466.4175
Sheila.armstrong@morganlewis.com

Sheila Armstrong represents a broad range companies in all aspects of government contracting including FAR-based contracts, grants and other financial assistance agreements and Other Transaction Agreements (OTAs). She routinely counsels both prime and subcontractors in a variety of contractual and civil settings. Sheila's experience includes proposal preparation, contract negotiation, subcontracting, teaming arrangements, intellectual property rights in government contracts, contract compliance, audits, investigations, mandatory disclosures, and procurement fraud. She also routinely provides support to clients on novation and due diligence issues. Sheila frequently advises clients with respect to General Services Administration (GSA) and Veterans Affairs (VA) Federal Supply Schedule contracts.

Biography

W. Barron A. Avery
Washington, D.C.
+1.202.739.5790
Barron.avery@morganlewis.com

Barron Avery, who leads the firm's government contracts practice, advises and represents government contractors and subcontractors in a wide range of matters involving all aspects of federal government contracting. With substantial knowledge of the rules and regulations that drive the government contracts industry, Barron provides knowledgeable day-to-day advice and counseling to government contractors.

Biography

Carl A. Valenstein
Boston, MA
+1.617.341.7501
Carl.valenstein@morganlewis.com

Carl Valenstein focuses his practice on domestic and international corporate and securities matters, mergers and acquisitions, project development, and transactional finance. He counsels extensively in the life science, telecom/electronics, and maritime industries, and has worked broadly in Latin America, the Caribbean, Europe, Africa, Asia, and the Middle East. He previously served as co-chair of the International Section of the Boston Bar Association and co-chairs the firm's environmental, social, and governance (ESG) and sustainable business and Cuba initiatives. Carl is the leader of the Boston office corporate and business transactions practice.

Biography

Casey Weaver
Houston, TX
+1.713.890.5409
Casey.weaver@morganlewis.com

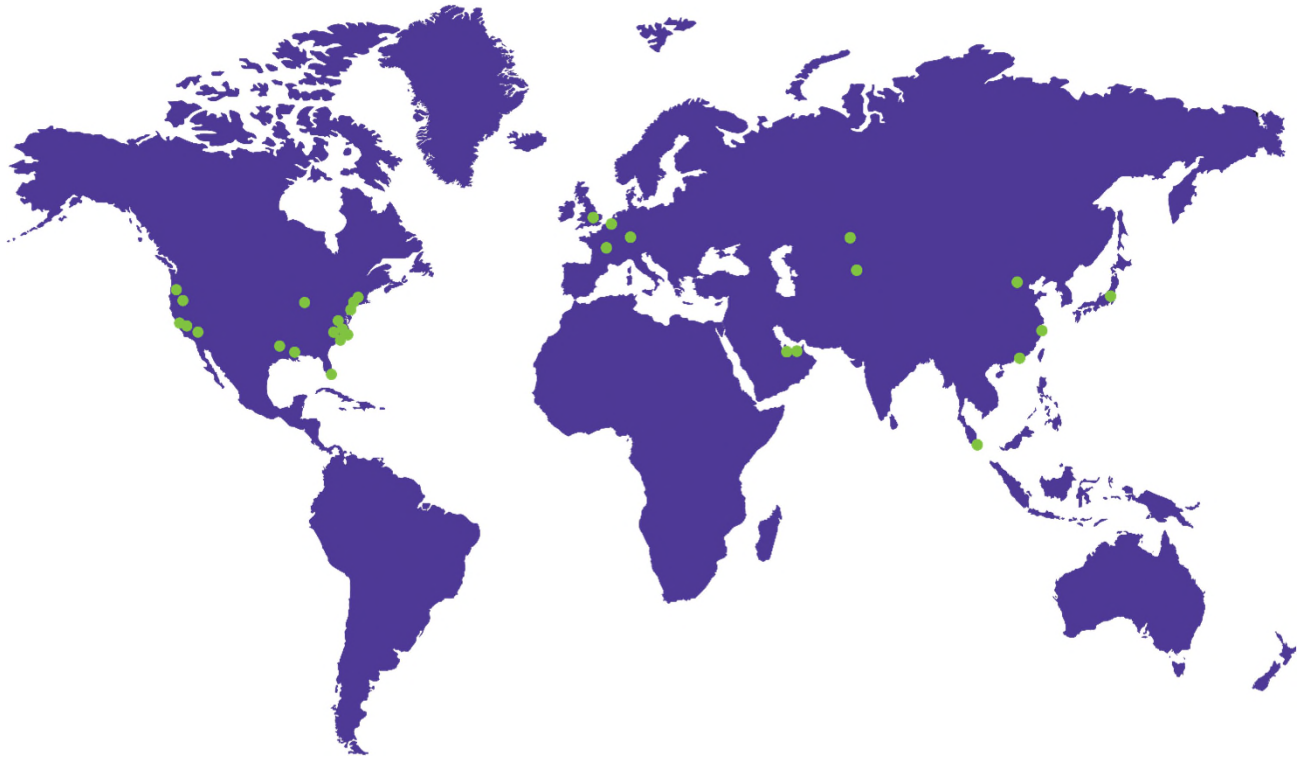
Casey Weaver focuses her practice on regulatory compliance matters, government and internal investigations, and government contracts. Her regulatory practice involves US laws and regulations affecting international trade, including import and export controls, economic and trade sanctions, and anti-corruption. Casey counsels clients regarding compliance with federal, state, and local government contracting, including domestic preference obligations. Her experience and knowledge of a breadth of compliance obligations allow her to help clients efficiently navigate a complex regulatory landscape.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU