September 27, 2023

# False Claims Act Hot Topics: Cybersecurity, Government Contracting, and Technology Companies

Winston Y. Chan
Dhananjay S. Manthripragada
Lindsay M. Paulin
Eric D. Vandevelde

GIBSON DUNN

# MCLE CERTIFICATE INFORMATION

**Approved for 1.0 hours General PP credit**

- CLE credit form must be submitted by **Wednesday, October 4th**
- Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_8HWYLoT4u243oTI

**Please direct all questions regarding MCLE to** CLE@gibsondunn.com

# OUR SPEAKERS

## Winston Y. Chan

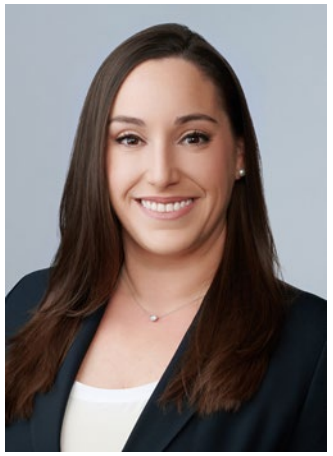
Partner / San Francisco

Winston Chan is a partner in the San Francisco office and Co-Chair of the firm's White Collar Defense and Investigations practice group, and also its False Claims Act/Qui Tam Defense practice group. He leads matters involving government enforcement defense, internal investigations and compliance counseling, and regularly represents clients before and in litigation against federal, state and local agencies, including the U.S. Department of Justice, Securities and Exchange Commission and State Attorneys General. Prior to joining the firm, Mr. Chan served as an Assistant United States Attorney in the Eastern District of New York, where he held a number of supervisory roles and investigated a wide range of corporate and financial criminal matters.

## Dhananjay S. Manthripragada

Partner / Los Angeles; Washington, D.C.

Dhananjay (DJ) Manthripragada is a partner in the Los Angeles and Washington, D.C. offices. He is Co-Chair of the firm's Government Contracts practice group, and also a member of the Litigation, Class Actions, Labor & Employment, and Aerospace and Related Technologies practice groups. Mr. Manthripragada has a broad complex litigation practice, and has served as lead counsel in precedent setting litigation before several United States Courts of Appeals, District Courts in jurisdictions across the country, California state courts, the Court of Federal Claims, and the Federal Government Boards of Contract Appeals.



## Lindsay M. Paulin

Partner / Washington, D.C.

Lindsay Paulin is a partner in the Washington, D.C. office and Co-Chair of the firm's Government Contracts practice group. Her practice focuses on a wide range of government contracts issues, including internal investigations, claims preparation and litigation, bid protests, government investigations under the False Claims Act, cost allowability, suspension and debarment proceedings, mergers and acquisitions involving government contracts, and compliance counseling. Ms. Paulin's clients include contractors and their subcontractors, vendors, and suppliers across a range of industries including aerospace and defense, information technology, professional services, private equity, and healthcare.

## Eric D. Vandevelde

Partner / Los Angeles

Eric Vandevelde is a partner in the Los Angeles office and Co-Chair of the firm's Artificial Intelligence practice group. As a former Assistant US Attorney, he brings extensive government experience to his role. With a background in white-collar crime, litigation, and crisis management, Mr. Vandevelde's expertise includes handling complex fraud and cybercrime investigations. He is a thought leader on emerging legal issues surrounding AI and algorithmic decision-making, having been recognized as one of California's leading AI lawyers in 2018. Mr. Vandevelde's computer science degree from Stanford and experience in AI software development contribute to his technical fluency in areas such as machine learning, deep learning, and natural language processing.

# AGENDA

## The False Claims Act

- FCA Basics
- Recent Legal Developments
- Enforcement Priorities and Trends
- Recent Enforcement Actions

## Government Contracting

- Contractor Cybersecurity: Overview & Cyber Incident Reporting
- Mandatory Disclosure Rule
- Overview of Suspension & Debarment System
- Recent Updates on Suspension & Debarment

## Comparison: SEC Focus on Cybersecurity

- Recent Rulemaking
- Recent Enforcement Action
- Issue in Focus: Vulnerabilities

# THE FALSE CLAIMS ACT

# FCA BASICS

# FCA BASICS

## The False Claims Act (FCA)

- The FCA, 31 U.S.C. §§ 3729–3733, is the federal government's primary tool for combating fraud against government agencies and programs.
- The FCA provides for recovery from any person who knowingly submits or causes the submission of false or fraudulent claims to the United States for money or property.
- The Attorney General, through prosecutors at Main DOJ and U.S. Attorney's Offices, investigates and pursues FCA cases—working in close coordination with federal agencies, including the Department of Health and Human Services—Office of Inspector General.
- DOJ has devoted substantial resources to pursuing FCA cases—and to considering whether civil FCA matters merit parallel criminal investigation.


"It seems quite clear that the objective of Congress was broadly ***to protect the funds and property of the Government from fraudulent claims*** …."

*Rainwater v. United States*, 356 U.S. 590 (1958)

# FCA BASICS

## The False Claims Act (FCA)

*Elements of an FCA case:*

- Falsity: A request for payment (claim) that is false or fraudulent.
  - Factual falsity: Billing for goods or services that were not correctly described or not provided at all.
  - Legal falsity: When a claim is based on a false representation of compliance, express or implied, with statutory, regulatory, or contractual requirements.
- Materiality: The falsity of the claim was material to the Government's payment of the claim.
- Scienter: The false claim was submitted "knowingly," which consists of "actual knowledge" of the falsity of the claim; "deliberate ignorance" of the truth or falsity of the claim; or "reckless disregard" of the truth or falsity of the claim.
- Causation: The false claim caused the Government to pay money.

To succeed, the plaintiff—either the Government or a whistleblower—must prove each of the above elements by a ***preponderance of evidence***.

# FCA BASICS

## Key FCA Theories of Liability

### Factual Falsity

- False billing (e.g., goods or services not provided)
- Overbilling (e.g., upcoding)

### Legal Falsity

- Express certification of compliance with legal requirements
- Submission of claim with representations rendered misleading as to goods / services provided

### Promissory Fraud / Fraud in the Inducement

- Obtaining a contract through false statements or fraudulent conduct
- *United States ex rel. Marcus v. Hess*, 317 U.S. 537 (1943) (claims by contractors who colluded on bids)

### Reverse False Claims

- Improper avoidance of obligation to pay money to the government
- Retention of government overpayment

# FCA BASICS

## *Qui Tam* Provisions

- The law's qui tam provisions enable so-called "relators" to bring cases in the government's name and receive as much as 30% of recovery or judgment.
- The Government is allowed to intervene, but an increasing number of cases are pursued without government intervention (but often with a government statement of interest).
- DOJ has broad authority to dismiss qui tam suits.
- Whistleblower protections, 31 U.S.C. § 3730(h), protect employees and others (e.g., contract workers) who report fraud.
- Relief under whistleblower protections may include double back pay and interest on back pay; reinstatement (at same level); and costs and attorneys' fees.
- Case law continues to develop, e.g., around meaning of the anti-retaliation provision's causation language ("because of").

"In short, sir, I have based the [*qui tam* provision] upon the old-fashioned idea of holding out a temptation and '***setting a rogue to catch a rogue***,' which is the safest and most expeditious way I have ever discovered of bringing rogues to justice."

Statement of Senator Howard, Cong. Globe, 37th Cong. 955-56 (1863)

# FCA BASICS

## Damages and Civil Penalties

- Simple Damages Calculation: Treble damages are traditionally calculated by multiplying the government's loss by three (e.g., if the government charged $100 for goods not received, damages would be $300).

- But, the damages calculation can get much more complicated (and less certain) when the government receives goods or services it considers deficient or when there is a "false certification" or "promissory fraud."

- In addition to damages, there is a per-claim civil penalty:
  - Previously $5,500 to $11,000.
  - Increased by interim rule in 2016, with later adjustments for inflation; current range, per final rule issued in January 2023, is **$13,508 to $27,018**.
  - Lower penalty range still in effect for violations occurring on or before November 2, 2015 ($5,500 to $11,000 per violation).

# THE FALSE CLAIMS ACT
# RECENT LEGAL DEVELOPMENTS

# RECENT LEGAL DEVELOPMENTS

## Proposed FCA Amendments

*False Claims Act Amendments of 2023*

- On July 25, 2023, a bipartisan group of senators, spearheaded by Senator Chuck Grassley, introduced proposed amendments to the FCA that would present difficulty for FCA defendants.
- If passed, the amendments would essentially eliminate the argument that alleged fraud was not material if the government continued payment.
- The bill purportedly aims to close "loopholes" left opened by the 2016 Supreme Court case *Universal Health Services, Inc. v. United States ex rel. Escobar*, 579 U.S. 176 ("*Escobar*")
- *Escobar* laid out a holistic analysis for materiality under the FCA.
- The amendments would rectify *Escobar*'s "flawed ruling" and make "clear that the government's continued payment on a fraudulent claim is not dispositive evidence that the fraud was not material if the government shows other reasons exist for the payment," according to Senator Grassley's press release on the proposed amendments.
- The amendments would also clarify that the FCA's whistleblower anti-retaliation provision applies to post-employment retaliation and requires a GAO study on the benefits and challenges of enforcement efforts and amounts recovered under the FCA.
- According to the press release, the bill ensures that entities "cannot escape liability in cases where the government has made recurring payments on a fraudulent claim."

# RECENT LEGAL DEVELOPMENTS

## Case Law

*SCOTUS Cases on Scienter Element*

- *United States ex rel. Schutte v. SuperValu Inc.*
- *United States ex rel. Proctor v. Safeway, Inc.*
- Facts:
  - Pharmacies seeking reimbursement for prescription drugs under Medicare and Medicaid generally must charge and disclose their "usual and customary" price for the drugs.
  - Relators alleged that, for generic drugs, discounted prices offered by the pharmacies to customers enrolled in membership programs were the "usual and customary" prices for the drugs, but pharmacies instead reported and charged their higher, non-discounted prices to Medicare and Medicaid.
  - Relators alleged that defendants knew the discounted prices were their "usual and customary prices," but submitted inaccurate claims to the Government anyways.
- Issue: Given that "usual and customary" is open to interpretation, could defendants have the scienter required by the FCA if they correctly understood what their "usual and customary" drug prices were, and submitted inaccurate claims anyways?

# RECENT LEGAL DEVELOPMENTS

## Case Law

*SCOTUS Cases on Scienter Element (cont'd)*

- Procedural history:
  - District court granted summary judgment to defendant on FCA's scienter element, holding that defendants could not have acted "knowingly."
  - Seventh Circuit affirmed, relying on *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47 (2007), where SCOTUS interpreted the term "willfully" in the context of the Fair Credit Reporting Act (FCRA).
    - Read *Safeco* to require that a claim must be objectively unreasonable, as a legal matter, before a defendant can be held liable for "knowingly" submitting a false claim.
    - Since "usual and customary" could have been reasonably understood as referring to the pharmacies retail prices, not their discounted prices, it did not matter whether defendants subjectively thought the discounted prices were the "usual and customary" prices.
- Holding (9-0): FCA's scienter element refers to defendants' knowledge and subjective beliefs, not what an objectively reasonable person may have known or believed.
  - This interpretation of "knowingly" is consistent with the common-law scienter requirement for claims of fraud.
  - Both text of the FCA and common law point to what the defendant thought when submitting the false claim, not what defendant may have thought *after* submitting it.
  - Facial ambiguity of "usual and customary" alone is not sufficient to preclude a finding that defendants knowingly submitted false claims.

# THE FALSE CLAIMS ACT ENFORCEMENT PRIORITIES & TRENDS

# ENFORCEMENT PRIORITIES & TRENDS

## Overview

- FY 2022: More new FCA cases (948) than in any prior year.
  - Government initiated 296 cases outside *qui tam* setting (also a record). FCA recoveries tend to be higher in these cases.
- In first half of 2023, DOJ announced 36 FCA resolutions totaling more than $485 million.
  - 2023 appears to be off to a slower start.
  - By comparison, in the first half of 2022, the DOJ had 29 resolutions totaling over $500 million However, the DOJ collected $2.2 billion by the end of FY22.
- As usual, FCA recoveries in the health care and life sciences industries have continued to dominate enforcement activity.
- There was also a federal jury trial under the FCA during the first half of the year, a relative rarity.
- In line with the Justice Department tamping down on unwarranted False Claims cases, the Supreme Court confirmed in June in *United States, ex rel. Polansky v. Executive Health Resources, Inc.* that the Justice Department can move to dismiss FCA suits despite whistleblower protest as long as the government intervenes in the case.

# ENFORCEMENT PRIORITIES & TRENDS

## DOJ's Civil Cyber-Fraud Initiative

On October 6, 2021, Deputy Attorney General Lisa O. Monaco announced the launch of DOJ's Civil Cyber-Fraud Initiative, combining DOJ's civil fraud enforcement, government procurement and cybersecurity expertise "to combat new and emerging cyber threats to the security of sensitive information and critical systems."

**"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward to report it."**

The Civil Cyber-Fraud initiative will use the FCA to pursue cybersecurity-related fraud by government contractors and grant recipients that are "knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."

Whereas earlier cybersecurity FCA actions were initiated primarily by *qui tam* relators, the announcement reflects the Biden Administration's increasing emphasis on affirmatively policing cybersecurity requirements for government contractors and their suppliers.

# ENFORCEMENT PRIORITIES & TRENDS

## DOJ's Civil Cyber-Fraud Initiative

On October 13, 2021, the Acting Assistant Attorney General for DOJ's Civil Division, Brian Boynton, delivered remarks on this new initiative, noting the Civil Cyber Fraud Initiative "will use the [FCA] to identify, pursue and deter cyber vulnerabilities and incidents that arise with government contracts and grants and that put sensitive information and critical government systems at risk."

In his speech, calling the FCA "a natural fit to pursue knowing failures" to comply with contracting requirements, Acting AAG Boynton identified "three common cybersecurity failures" that would be "prime candidates" for potential FCA enforcement by DOJ:

- (1) "knowing failures to comply with cybersecurity standards" in government contracts;
- (2) "knowing misrepresentation of security controls and practices"; and
- (3) "knowing failure to timely report suspected breaches."

# ENFORCEMENT PRIORITIES & TRENDS

## DOJ's Civil Cyber-Fraud Initiative

In a November 2021 ABA event, various DOJ speakers further emphasized that the Initiative will focus on the following scenarios:

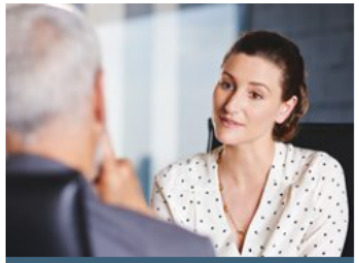
- "The government purchases hardware or software with cyber requirements, and the requirements are not met."
- "A contractor implements IT systems for the government and does not comply with contract requirements, including U.S. citizenship requirements."
- "A contract has an IT system that houses government data, and cyber requirements applicable to that system or data are not met."
- "A contractor is providing cloud services, i.e., through FedRAMP, and requirements are not met."
- "A contractor fails to comply with regulatory/contractual/statutory requirements to monitor and report cyber incidents and breaches."

# ENFORCEMENT PRIORITIES & TRENDS

## Plaintiffs' Firms Are Interested

Cybersecurity Fraud

- Tips for Potential Cybersecurity Whistleblowers
- Generally Applicable Cybersecurity Requirements
- Department of Defense Contractor Cybersecurity Requirements
- GSA Public Buildings Service Contractor Cybersecurity Requirements
- NASA Contractor Cybersecurity Requirements



How can we

### Do You Need a Whistleblower Lawyer for Cybersecurity Fraud?

#### What is cybersecurity fraud?

Cybersecurity fraud is when a government contractor or subcontractor knowingly violates key government requirements to:

i) incorporate specified cybersecurity features when providing goods or services;

ii) take specified measures to protect electronic documents or data; or,

iii) promptly report cybersecurity breaches.

If you know of cybersecurity violations that expose the Government to undue security risk, your information may form the basis for a strong qui tam action.

In 2020, the digital systems of about a dozen federal agencies and one hundred companies were breached by suspected agents of the Russian government. The hackers exploited weaknesses in software provided by a federal contractor: Solar Winds. In the wake of this attack, the federal government has made addressing the nation's cybersecurity a priority and is calling on whistleblowers to help. In October 2021, the Department of Justice unveiled the Civil Cyber-Fraud Initiative which will be empowered to use the False Claims Act and assist whistleblowers in pursuing cases against government contractors who have failed to follow required cybersecurity standards or report hacks of their systems.

This is a pressing area of fraud, and cybersecurity whistleblowers who have valuable information may see the federal government dedicate generous resources and attention to investigating their complaints. If you know of cybersecurity violations that meet the above criteria and are looking for an experienced whistleblower

# RECENT ENFORCEMENT ACTION

# CONTRACTORS

## Focus on Cybersecurity

- In FY 2022, DOJ was focused on the application of the FCA to misrepresentations of compliance with cybersecurity requirements.
  - Comprehensive Health Services, Inc.: In March 2022, a Florida-based medical provider paid $930,000 to resolve allegations that it misrepresented its compliance with State Department contract requirements to store medical records in a secure EMR system.
  - Aerojet Rocketdyne, Inc.: In July 2022, defense- and space-sector contractor Aerojet paid $9 million to resolve allegations that it misrepresented its compliance with DoD regulations to safeguard controlled unclassified information (CUI) and with a NASA rule for protecting sensitive information.
    - In May 2019, a U.S. District Judge in E.D. Cal. denied Aerojet's motion to dismiss the case, holding that Aerojet's compliance with cybersecurity clauses in its contracts could be deemed material to the Government's decision to award Aerojet contracts and pay Aerojet's invoices.
- This trend has carried over into 2023.
  - Jelly Bean Communications Designs LLC (Jelly Bean): In March 2023, Jelly Bean agreed to pay approximately $300,000 to resolve allegations that it violated the FCA by failing to secure personal information on a federally funded Florida children's health insurance website, which Jelly Bean created, hosted, and maintained. DOJ claimed that, contrary to its representations in agreements and invoices, Jelly Bean knowingly failed to maintain, patch, and update the website's software systems, leaving the site vulnerable to attack.

# RECENT ENFORCEMENT ACTION

# CONTRACTORS

## Verizon Business Network Services LLC

- September 5, 2023: Verizon settled allegations that it failed to completely satisfy certain cybersecurity controls in connection with an information technology service provided to federal agencies.
  - The settlement arose following a self-initiated compliance review by Verizon.
- Key findings:
  - Managed Trusted Internet Protocol Services (MTIPS) are designed to provide federal agencies with secure connections to the public internet and other external networks. Verizon was awarded contracts by the U.S. GSA from 2017 – 2021 to provide MTIPS to federal agencies, which required compliance with Trusted Internet Connection Standards.
  - After initiating a review and finding deficiencies with MTIPS, Verizon promptly reported issues it discovered to the GSA's Office of Inspector General.
  - Under the settlement agreement, Verizon did not admit liability and, for its cooperation, paid a 1.5 multiplier, less than its maximum potential exposure under the FCA.
  - DOJ touted the settlement as evidence of its commitment to pursue "knowing cybersecurity related violations under the Department's Civil Cyber-Fraud Initiative" while providing "credit in settlements to government contractors that disclose misconduct, cooperate with pending investigations and take remedial measures."
- Verizon agreed to pay **$4,091,317** to resolve the dispute.

# RECENT ENFORCEMENT ACTION

# CONTRACTORS

## Penn State University

- September 1, 2023: The U.S. District Court for the Eastern District of Pennsylvania unsealed a qui tam lawsuit, originally filed October 5, 2022, alleging Penn State University misrepresented its adherence to cybersecurity protocols and failed to provide adequate security for Controlled Unclassified Information (CUI).
  - The suit is being brought by Matthew Decker, former Chief Information Officer and Director of Information Technology Services at Penn State's Applied Research Lab (ARL).
- Allegations:
  - The lawsuit alleges that the university has been falsely attesting to compliance since January 1, 2018.
  - The suit alleges that "the organization can neither identify where CUI is nor where it should be, nor validate existing CUI, [so] there is no chance that comprehensive protection or compliance can be truthfully attested."

# GOVERNMENT CONTRACTING

# CONTRACTOR CYBERSECURITY: OVERVIEW & CYBER INCIDENT REPORTING

# CONTRACTOR CYBERSECURITY: OVERVIEW

## Overview – "Safeguarding" Clauses

- Backbone requirements for contractor (i.e., non-Federal) information systems:
  - NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
  - Applies to every federal contract, except for acquisitions of commercially available off-the-shelf (COTS) items, "when a contractor's information system may contain Federal contract information" (FCI) – FAR 4.1902
- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
  - Applies to all DoD "solicitations and contracts," except for COTS items – DFARS 204.7304
- VAAR 852.204-71, Information and Information Systems Security
  - Directs "[c]ontractors, subcontractors, their employees, third-parties, and business associates with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services" to adhere to VA Directive 6500, VA Cybersecurity Program – VAAR 852.204-71(b)
- NFS 1852.204-76, Security Requirements for Unclassified Information Technology Resources
  - Mandates that "[t]he contractor shall protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources and protect NASA Electronic Information from unauthorized disclosure." – NFS 1852.204-76(a)

# CONTRACTOR CYBERSECURITY: OVERVIEW

## Overview – DoD's NIST SP 800-171 Assessment Methodology

- DoD NIST SP 800-171 Assessment Methodology
  - Basic (Self Assessment)
  - Medium (DoD Assessment)
  - High (DoD Assessment)

- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirement
  - Requires contractor to provide access to facilities, systems, and personnel for DoD to conduct Medium or High assessment, if necessary – DFARS 252.204-7020(c)
  - Provides that "[s]ummary level scores for all assessments will posted in the Supplier Performance Risk System (SPRS)" – DFARS 252.204-7020(d)

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
  - Eligibility for contract award requires current assessment for each covered contractor information system relevant to offer – DFARS 252.204-7019(b)
  - Similarly, prime contractor may not award a subcontract unless the subcontractor has completed an assessment within the last 3 years – DFARS 252.204-7020(g)(2)

# CONTRACTOR CYBERSECURITY: OVERVIEW

## Overview – NIST SP 800-171, Revision 3

- May 10, 2023: NIST released its first public draft of Revision 3 of NIST SP 800-171.
  - These controls underpin federal cybersecurity standards – e.g., FAR 52.204-21, DFARS 252.204-7012, upcoming CMMC program.

"*Many of the newly added requirements specifically address threats to CUI, which recently has been a target of state-level espionage. We want to implement and maintain state-of-the-practice defenses because the threat space is changing constantly. We tried to express those requirements in a way that shows contractors what we do and why in federal cybersecurity. There's more useful detail now with less ambiguity. . . . Protecting CUI, including intellectual property, is critical to the nation's ability to innovate – with far-reaching implications for our national and economic security. We need to have safeguards that are sufficiently strong to do the job.*" – Ron Ross, NIST Fellow

- Changes include:
  - Creation of three new "families" of controls – planning (Section 3.15), system and services acquisition (Section 3.16), and supply chain risk management (Section 3.17);
  - Updated guidance on tailoring the security controls to better fit a contractor's certain system or environment; and
  - Closer ties/references to SP 800-53, the set of cybersecurity controls and standards that federal agencies use to maintain confidentiality, integrity, and availability of their data.
- NIST anticipates publishing one more draft of Rev. 3 before publishing the final version in early 2024.

# CONTRACTOR CYBERSECURITY: OVERVIEW

## Overview – Cybersecurity Maturity Model Certification (CMMC)

- DoD's cybersecurity framework of the future: Cybersecurity Maturity Model Certification (CMMC)
- CMMC 1.0 (January 2020)
  - Tiered framework identifying cybersecurity requirements for members of Defense Industrial Base (DIB) and associated third-party assessment/verification process
- CMMC 2.0 (November 2021) – simplified framework following industry feedback
  - 3 maturity levels: Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert)
- DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements:
  - In some contracts and will eventually require certification, but rulemaking ongoing

# CONTRACTOR CYBERSECURITY: OVERVIEW

## Overview – FedRAMP/Cloud Computing

- Federal Risk and Authorization Management Program (FedRAMP): “a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.” – FedRAMP.gov FAQs
- FedRAMP created by 2011 OMB Memo; now codified into law
- Builds off NIST SP 800-53 controls
- Cloud computing products and services must be FedRAMP-authorized to be used by Government
- DFARS 252.239-7010, Cloud Computing Services

# CYBER INCIDENT REPORTING

## Cyber Incident Reporting – DFARS -7012

- Contractors may be subject to contractual requirements that they report breaches of contractor information systems to the Government or to prime contractors (or higher-tier subcontractors).
- Cyber incident clauses may be tailored to individual contracts/agreements.
  - E.g., a contract with DoD made pursuant to the agency's Other Transaction Authority, which will not incorporate clauses from the FAR or DFARS.
- Most well-known provision is found in DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, which is incorporated into all DoD solicitations and contracts (except for COTS).
  - "When the contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall-- . . . (ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil." – DFARS 252.204-7012(c)(1)(i)
  - "Rapidly report" = "within **72 hours** of discovery of any cyber incident" – DFARS 252.204-7012(a)
- Under the DFARS -7012 clause, contractor must also:
  - Submit any malicious software it discovers in connection with the incident to DoD.
  - Preserve and protect images of all known affected information systems for at least 90 days after submission of the cyber incident report.
- Clause must be flowed-down to subcontracts, requiring subcontractors to report cyber incidents to prime contractors and to DoD via DIBNet.

# CYBER INCIDENT REPORTING

## Cyber Incident Reporting – VAAR

- The new Veterans Affairs cybersecurity/privacy clause also includes provisions addressing cyber incident reporting:
  - "The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify VA immediately via the Contracting Officer and the COR within ***one (1) hour*** of an incident which is an occurrence (including the discovery or disclosure of successful exploits of system vulnerability) that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or the availability of its data and operations, or of its information or information system(s); or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. *The initial notification may first be made verbally but must be followed up in writing within* ***one (1) hour****.*" – VAAR 852.204-71(g)
  - Contract will further stipulate the timeline for remediating the vulnerability, but in any event, it must be within 60 days of discovery or disclosure. – *Id.*
  - Clause further specifies content of notice – "To the extent known," it shall "identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant." – VAAR 852.204-71(h)
  - If incident involves "theft or break-in or other criminal activity," it must be concurrently reported "to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and the VA Office of Security and Law Enforcement." – *Id*.
  - Clause must be flowed-down to subcontracts. – VAAR 852.204-71(k)

# CYBER INCIDENT REPORTING

## Cyber Incident Reporting – HSAR

- The new Department of Homeland Security (DHS) rule amended the Homeland Security Acquisition Regulation (HSAR), amends cybersecurity/privacy clauses also include provisions addressing cyber incident reporting:
  - "All known or suspected incidents involving personally identifiable information (PII) or sensitive personally identifiable information (SPII) shall be reported ***within one (1) hour*** of discovery. All other incidents shall be reported ***within eight (8) hours*** of discovery." -- HSAR 3052.204-72(c)(2)
  - If an incident involves PII or SPII, in addition to reporting the incident, contractors and subcontractors must report ***additional information within 24 hours*** of submission of the initial incident report, which shall include, inter alia:
    - The contract clearance level;
    - The government programs, platforms, or systems involved;
    - The date and time the incident was discovered; and
    - The description of the government PII or SPII contained within the system.
  - Contractors must notify any individual whose PII or SPII was impacted by an incident ***within five (5) business days*** of being directly contacted by the Contracting Officer. The Contracting Officer may also require the Contractor to provide credit monitoring services to individuals whose PII or SPII was impacted by an incident for at least 18 months. -- HSAR 3052.204-73(c)(2).

# CYBER INCIDENT REPORTING

## Cyber Incident Reporting – CIRCIA

- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") also includes incident reporting provisions that could apply to Government contractors.
  - President Biden signed CIRCIA into law on March 15, 2022; the Cybersecurity & Infrastructure Security Agency ("CISA") is responsible for implementing the reporting requirements.
  - Amended the Homeland Security Act of 2002 to include cyber incident reporting requirements for "covered entities":
    - Covered entity: "[A]n entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b)." - § 103(a)(2)
    - In Presidential Policy Directive 21, the Defense Industrial Base is a "critical infrastructure sector."
    - While the exact definition of "covered entity" is subject to CISA's pending rulemaking, it is clear that at least some defense contractors will be swept into the definition.
- Act requires CISA to propose implementing regulations within 24 months (by March 2024), and to promulgate final regulations within 18 months thereafter (by September 2025).
  - "Covered cyber incidents" will also be further defined in rulemaking, but shall include, e.g., a cyber incident "that leads to substantial loss of confidentiality, integrity, or availability of such information or system or network, or a serious impact on the safety and resiliency of operational systems and processes."

# CYBER INCIDENT REPORTING

## Cyber Incident Reporting – CIRCIA (cont'd)

- CIRCIA includes two cyber incident reporting requirements:
  - Cyber Incident Reporting Requirement: Covered entities must report any "covered cyber incident" to CISA within 72 hours "after the covered entity reasonably believes that the covered cyber incident has occurred."
  - Ransomware Payment Reporting Requirement: Covered entities that make payments as "the result of a ransomware attack" must report the payments to CISA within 24 hours of the payment.
- Helpfully, CIRCIA creates an exception to the reporting requirements for covered entities that, "by law, regulation, or contract," are already required to report "substantially similar information to another Federal Agency within a substantially similar timeframe."
  - But, for this exception to apply, there must be "an agency agreement and sharing mechanism" in place between CISA and the other agency.
  - Exact overlap of CIRCIA reporting requirements with, e.g., DFARS -7012, has yet to be determined.
- Status: Rulemaking to implement CIRCIA's requirements is underway at CISA; next step is a proposed rule.
  - CISA requested comments from the public in September 2022.
  - CISA held public listening sessions across the country from September-November 2022.

# CYBER INCIDENT REPORTING

## State Data Privacy Laws

- Several states (California, Colorado, Connecticut, and Virginia) have active consumer data privacy laws that impose obligations on certain businesses. California's is arguably the most rigorous.
- Compromised businesses must disclose data breaches in the most expedient time possible and without unreasonable delay. California residents can sue for damages up to $750 per incident that meets certain criteria.
- The California Privacy Protection Agency released draft of proposed rules for privacy risk assessments and cybersecurity audits for the privacy law on August 28, 2023. Under draft regulations, a company must conduct a risk assessment if they process consumers' personal information in such a way that it presents "significant risk" to privacy or security. The criteria for 'significant risk' has not been finalized.
- The CPPA's cybersecurity audit draft, if pursued, would effectively impose major cybersecurity requirements on covered businesses by requiring the annual audit to assess, document and summarize each applicable component of an entity's cybersecurity program, specifically identify any gaps or weaknesses in that program, and address the status of gaps or weaknesses identified in any prior audit.
- Seven states (Indiana, Iowa, Montana, Oregon, Tennessee, Texas, and Utah) all have enacted consumer privacy laws that will come into effect, most between 2024 and 2026.
- Although California's data privacy law arguably continues to be the most stringent of any U.S. data privacy laws, many of the individual state privacy laws have nuances and they are not uniform. These nuances continue to make it difficult for national companies to comply with the patchwork and require a close eye on them.

# GOVERNMENT CONTRACTING
# MANDATORY DISCLOSURE RULE

# MANDATORY DISCLOSURE RULE

## FAR Contract Clause

- The Mandatory Disclosure Rule ("MDR") requires Government contractors to disclose to the Government actual or potential violations of criminal and civil law as well as instances of significant overpayment.
  - *See* Contractor Business Ethics Compliance and Disclosure Requirements, 73 Fed. Reg. 67064 (Nov. 12, 2008)
- FAR contract clause implementing the MDR requires contractor to:
  - "timely disclose, in writing, to the agency Office of Inspector General (OIG), with a copy to the Contractor Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed-

    (A) A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or

    (B) A violation of the civil False Claims Act (31 U.S.C. 3729-3733)."

    – FAR 52.203-13(b)(3)(i)(B)
- Clause is included in all solicitations and contracts "if the value of the contract is expected to exceed **$6 million** and the performance period is 120 days or more." – FAR 3.1004(a)

# MANDATORY DISCLOSURE RULE

## Parallel Basis for Suspension or Debarment

- MDR also created a parallel basis for suspension or debarment in FAR Subpart 9.4, linked to contractor disclosure requirement.
- For example, FAR 9.406-2, Causes for debarment, provides that a debarring official may debar a contractor based upon a preponderance of the evidence for-

. . . .

(vi) Knowing failure by a principal, until **3 years** after final payment on any Government contract awarded to the contractor, to timely disclose to the Government, in connection with the award, performance, or closeout of the contractor or a subcontract thereunder, credible evidence of-

(A) Violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code;

(B) Violation of the civil False Claims Act (31 U.S.C. 3729-3733); or

(C) Significant overpayment(s) on the contract, other than overpayments resulting from contract financing payments as defined in 32.001.

# GOVERNMENT CONTRACTING
# OVERVIEW OF SUSPENSION & DEBARMENT SYSTEM

# OVERVIEW OF SUSPENSION & DEBARMENT SYSTEM

## Suspension & Debarment in the United States

"The S&D process protects the federal government from fraud, waste and abuse by using a number of tools to avoid doing business with non-responsible contractors." - GSA

The FAR provides that contracting officers may award contracts to "responsible prospective contractors only." FAR 9.103

Suspension and debarment are discretionary actions taken by the Government to effectuate the policy of doing business "with responsible contractors only." FAR 9.402(a)

Differences:

- Suspension – based on an immediate need; usually greater than 12 months; usually used pending completion of investigation/legal proceedings; based upon "*adequate evidence*," e.g., an indictment where "immediate action" is necessary to protect the Government's interest
- Debarment – longer-term (usually three years in length); based upon a "*preponderance of evidence*," e.g., a conviction

- Effects
  - Contractor's name published on SAM.gov as ineligible
  - Offers not solicited from contractor
  - Contracts not awarded to contractor
  - Existing contracts will not be renewed or extended
  - Contractor also barred from entering into subcontracts with prime government contractors
  - Reputational and commercial harm

# OVERVIEW OF SUSPENSION & DEBARMENT SYSTEM

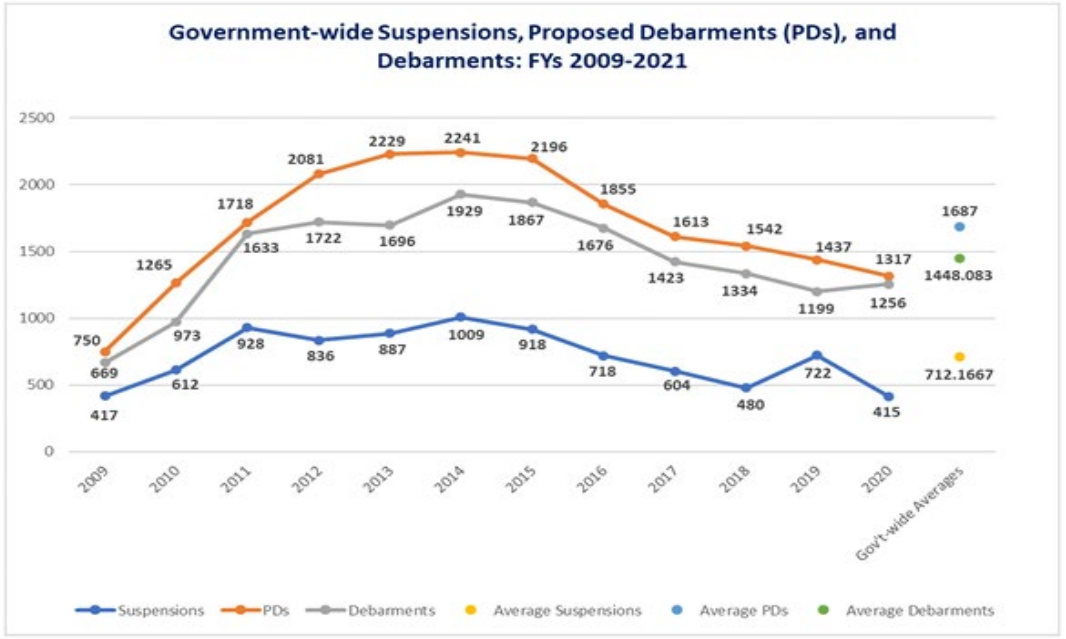
## Suspension & Debarment in the United States (cont'd)

- Causes for suspension/debarment include:
  - Knowing failure of principal to comply with the MDR (*see supra*)
  - Commission of fraud, embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal laws, receiving stolen property, unfair trade practices
  - Violation of antitrust statutes
  - Willful, or a history of, failure to perform
  - Violation of Drug-Free Workplace Act
  - Delinquent Federal taxes (more than $3,000)
  - Knowing failure to disclose violation of criminal law
  - *Any other cause that affects present responsibility*

# OVERVIEW OF SUSPENSION & DEBARMENT SYSTEM

## Recent Exclusion Data

- As required by statute, the Interagency Suspension & Debarment Committee (ISDC) publishes data on exclusions in a report to Congress.
- ISDC published its report for FY 2020 in March 2022; as of now, the FY 2021 report has not been published.
- Government-wide, in FY 2020, there was a decrease in the number of suspensions (from 722 to 415), a decrease in the number of proposed debarments (1437 to 1317), and a slight increase in the number of debarments (1199 to 1256).
- For all three categories, the numbers are significantly lower than the middle of last decade.



# OVERVIEW OF SUSPENSION & DEBARMENT SYSTEM

## Legislation & Congressional Pressure

- Congressional Pressure for Increased DOJ Use of Suspension and Debarment
  - In an August 11, 2022 letter to DOJ, Senators Warren (D-Mass) and Lujan (D-N.M.) urged DOJ to boost its use of suspension/debarment in connection with its prosecution of criminal or fraud cases.
  - The letter urged DOJ "to pursue more robust use of its suspension and debarment authority," including against companies that are the subject of criminal and civil fraud probes but that it "does not directly do business with."
  - Troublingly, the letter failed to appreciate the *non-punitive* nature of exclusions—that is, the focus of the suspension & debarment regime on *present responsibility* rather than *past misconduct*.

# COMPARISON: SEC FOCUS ON CYBERSECURITY

# RECENT RULEMAKING

## Adopted SEC Final Rule

- September 5, 2023: SEC final rules requiring the disclosure of material cybersecurity incidents and cybersecurity risk management, strategy, and governance by public companies went into effect.
- Implementation Timeline:
  - Most public companies will be required to comply with the Form 8-K incident disclosure requirements beginning on the later of December 18, 2023 and 90 days after the final rule is published in the Federal Register.
  - Smaller reporting companies are eligible for an extension and have until the later of June 15, 2024 and 270 days after the date the final rule is published in the Federal Register.
  - *All public companies will be required to comply with the new annual disclosure requirements beginning with the annual report on Form 10-K or 20-F for the fiscal year ending on or after December 15, 2023.*
- Rule Requirements:
  - (i) Form 8-K disclosure of material cybersecurity incidents within four (4) business days of the company's determination that the cybersecurity incident is material.
  - (ii) New annual disclosures in Form 10-K regarding a company's cybersecurity risk management and strategy, including with respect to the company's processes for managing cybersecurity threats and whether risks from cybersecurity threats have materially affected the company.
  - (iii) New annual disclosures in Form 10-K regarding the company's cybersecurity governance, including with respect to oversight by the board and management.
    - Annual disclosures are also required in foreign private issuers' annual reports on Form 20-F, and material cybersecurity incident disclosure will be covered by Form 6-K."

# RECENT ENFORCEMENT ACTION

## Blackbaud

- March 9, 2023: SEC reached a settlement with Blackbaud, a client relationship management service provider for nonprofits.
  - SEC alleged Blackbaud (i) made materially misleading statements in its securities filings regarding a ransomware attack that it had suffered, and (ii) failed to maintain adequate disclosure controls designed to ensure it accurately and timely disclosed information related to the ransomware attack.
- Key findings:
  - Blackbaud detected unauthorized access to company's systems; the company ultimately coordinated payment of ransom in exchange for attacker's promise to delete any exfiltrated data.
  - Blackbaud disclosed incident on website and to customers, stating that the threat actor "did not access . . . bank account information, or social security numbers."
    - However, company personnel soon became aware that the threat actor had, in fact, accessed this information in unencrypted form. But, Blackbaud's management personnel were not informed of this update, and the company did not have policies and procedures in place to ensure this occurred.
  - Blackbaud also made several incomplete or incorrect statements regarding the incident in its Form 10-Q.
    - E.g., threat actor "removed a copy of a subset of data" – no reference to exfiltrated bank account information or social security numbers.
- Blackbaud paid **$3 million** in penalties to resolve the dispute.

# ISSUE IN FOCUS: VULNERABILITIES

## Other Developments

- The National Institute of Standards and Technology at the U.S. Department of Commerce (NIST) released a draft Cybersecurity Framework 2.0 on August 8, 2023.
  - In 2014, NIST published voluntary Cybersecurity Framework (CSF) 1.0.
  - These are a comprehensive set of guidelines for mitigating organizational cybersecurity risks, based on existing standards, guidelines, and practices.
  - NIST anticipates publishing the final CSF 2.0 in early 2024.

- On August 22, 2023, Representative Nancy Mace in the U.S. House of Representatives introduced a bill that would require federal contractors to adopt the kinds of vulnerability disclosure practices recommended in the NIST Framework.

- A proposed bill in California, AB581, would do the same as to state agencies.

# THANK YOU!

Please note that the enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.

**EDUCATION**

**Yale University**
Juris Doctor

**Yale University**
Bachelor of Arts, *magna cum laude*

**CLERKSHIPS**

**U.S. Court of Appeals, Second Circuit**

**U.S.D.C., Southern District of New York**

**RECOGNIZED**

**Litigation, White-Collar Crime & Government Investigations**
Chambers USA

**Litigation Star**
Benchmark Litigation

**Rising Star, White Collar Criminal Defense**
Law360

555 Mission Street, Suite 3000, San Francisco, CA 94105-0921 USA
T +1 415.393.8362
wchan@gibsondunn.com

# Winston Y. Chan

Partner / San Francisco

Winston Y. Chan is a litigation partner in Gibson, Dunn & Crutcher's San Francisco office, and serves as Co-Chair of the firm's global White Collar Defense and Investigations practice group, and also its False Claims Act/Qui Tam Defense practice group. He leads matters involving government enforcement defense, internal investigations, and compliance counseling, and regularly represents clients before and in litigation against federal, state and local agencies.

Mr. Chan is a Chambers-ranked attorney in the category of White Collar Crime and Government Investigations, and *Benchmark Litigation* recognizes him as a Litigation Star for being "recommended consistently as a reputable and effective litigator by clients and peers." He is regularly included in *Best Lawyers*, as well as *Who's Who Legal* for Investigations. *Global Investigations Review* ranks Mr. Chan in its annual Global Guide of Recommended Investigations Counsel, and he is a *LMG Life Sciences* "Star" in White Collar and Government Investigations.

Prior to joining the firm, Mr. Chan served as an Assistant United States Attorney in the Eastern District of New York, where he investigated a wide range of corporate and financial criminal matters as part of that office's Business and Securities Fraud Section. Mr. Chan additionally prosecuted cases in the Organized Crime and Racketeering Section, where he handled matters involving Italian, Eastern European and Asian criminal enterprises, for which the Attorney General awarded Mr. Chan one of the Department of Justice's highest awards for his "exemplary and historic work." As a senior prosecutor, he served in a number of supervisory roles, including as Deputy Chief of the General Crimes section, where he supervised and trained that office's line prosecutors, as well as Health Care Fraud Coordinator, where he oversaw criminal healthcare fraud and qui tam matters.

Mr. Chan earned his undergraduate degree, *magna cum laude*, from Yale University, and his Juris Doctor from Yale Law School, where he was on the *Yale Law Journal* and president of the Pacific Islander, Asian and Native American Law Students' Association. Following law school, Mr. Chan served as a law clerk for the Honorable Leonard B. Sand of the United States District Court for the Southern District of New York, and then for the Honorable Chester J. Straub of the United States Court of Appeals for the Second Circuit.

**EDUCATION**

**University of California – Los Angeles**
Juris Doctor

**Duke University**
Bachelor of Arts

**RECOGNIZED**

**One to Watch: Commercial Litigation**
Best Lawyers

333 South Grand Avenue, Los Angeles, CA 90071-3197 USA
Tel: +1 213.229.7366
dmanthriprigada@gibsondunn.com

# Dhananjay S. Manthriprigada

Partner / Los Angeles

Dhananjay (DJ) Manthripragada is a partner in the Los Angeles and Washington, D.C. offices of Gibson, Dunn & Crutcher. He is Chair of the firm's Government Contracts practice group, and also a member of the Litigation, Class Actions, and Labor & Employment practice groups. Mr. Manthripragada has served as lead counsel in precedent setting litigation before several United States Courts of Appeals, District Courts and state courts in jurisdictions across the country, the Court of Federal Claims, and the Federal Government Boards of Contract Appeals. He has first-chair trial experience and has successfully tried to verdict both jury and bench trials, and has served as lead counsel in arbitration and other alternative dispute resolution forums. His practice spans a wide range of industries, and he has represented some of the world's leading aerospace and defense, logistics/transportation, and high-technology companies in their most significant matters. Mr. Manthripragada is also highly regarded as a trusted advisor to clients regarding significant compliance/enforcement, contract, and dispute resolution issues. He was recognized in *The Best Lawyers in America*® Ones to Watch in Commercial Litigation in 2021 and 2022.

As Chair of the firm's Government Contracts practice, Mr. Manthripragada also has a breadth of experience in the field of government contracts. His government contracts practice focuses on civil and criminal fraud investigations and litigation, bid protests, complex claims preparation and litigation, qui tam suits under the False Claims Act, defective pricing, cost allowability, and the Cost Accounting Standards. He has represented government contractors and their subcontractors, vendors, and suppliers before the Armed Services Board of Contract Appeals, the United States Court of Federal Claims, the U.S. Government Accountability Office, and federal appellate and trial courts across the country, and has provided advice to clients on issues involving contract negotiations, claims analysis, and contract performance. Mr. Manthripragada maintains a robust compliance counseling practice, aimed at offering practical guidance on complex regulatory issues in line with clients' business goals. In addition, he is the Editor-in-Chief of the Government Contract Costs, Pricing and Accounting Report, and serves on The Government Contractor Advisory Board.

Mr. Manthripragada received a law degree in 2007 from the University of California, Los Angeles, where he served as Chief Comments Editor and Articles Editor of the *UCLA Journal of Environmental Law & Policy*. He also served as a judicial extern to Judge Kim McLane Wardlaw of the U.S. Court of Appeals for the Ninth Circuit.

**EDUCATION**

**The George Washington University**
Juris Doctor

**The George Washington University**
Bachelor of Arts

**RECOGNIZED**

**One to Watch, Administrative and Regulatory Law and Criminal Defense: White Collar**
Best Lawyers

**Rising Star (Washington D.C.)**
Super Lawyers

1050 Connecticut Avenue, N.W., Washington, DC 20036-5306 USA
T +1 202.887.3701
lpaulin@gibsondunn.com

# Lindsay M. Paulin

Partner / Washington, D.C.

Lindsay M. Paulin is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. She currently serves as co-chair of the Gibson Dunn's Government Contracts Practice Group.

Ms. Paulin's practice focuses on a wide range of government contracts issues, including internal investigations, claims preparation and litigation, bid protests, government investigations under the False Claims Act, cost allowability, suspension and debarment proceedings, mergers and acquisitions involving government contracts, and compliance counseling. She has represented clients in disputes before the United States Court of Federal Claims, the Armed Services Board of Contract Appeals, the United States Government Accountability Office, and administrative agencies. Ms. Paulin's clients include contractors and their subcontractors, vendors, and suppliers across a range of industries including aerospace and defense, information technology, professional services, private equity, and insurance. Ms. Paulin was named a DC "Rising Star" by *The National Law Journal* (2023), and has been recognized by *Best Lawyers* as "One to Watch" for Administrative and Regulatory Law (2022-2023) and Criminal Defense: White Collar (2023), as well as been featured in *Super Lawyers* Washington D.C. as a "Rising Star" (2019-2022).

Ms. Paulin received her law degree with high honors from the George Washington University Law School in 2012, where she was elected to the Order of the Coif and served as an Editor of the *George Washington Law Review*. While in law school, Ms. Paulin worked for a McLean, Virginia-based government contractor, providing support to the Department of Defense Office of the General Counsel, Deputy General Counsel for International Affairs. In 2009, she received her Bachelor of Arts in International Affairs *summa cum laude* from the George Washington University's Elliott School of International Affairs, where she was elected to Phi Beta Kappa.

Ms. Paulin is admitted to practice law in the Commonwealth of Virginia and the District of Columbia.

333 South Grand Avenue, Los Angeles, CA 90071-3197 USA
T +1 213.229.7186
evandevelde@gibsondunn.com

# Eric D. Vandevelde

Partner / Los Angeles

Eric Vandevelde is a partner in Gibson Dunn's Los Angeles office. He is co-chair of the Artificial Intelligence (AI) practice group and a member of the firm's White Collar, Privacy & Cybersecurity, and Intellectual Property practice groups. Mr. Vandevelde is a former federal prosecutor, supervised the Cyber & IP Crimes section of the U.S. Attorney's Office in the Central District of California, and has significant first-chair trial experience, both while at the DOJ and in the private sector. He has a deep technical background, with a degree in computer science from Stanford and having worked as a software engineer in Silicon Valley and Latin America. He repeatedly has been ranked by *Chambers* and recognized by *Super Lawyers* and the *Daily Journal*, including as one of the Top 20 Cyber/Artificial Intelligence lawyers in California.

Mr. Vandevelde has an extremely broad practice—handling criminal and civil trials, internal investigations, enforcement matters, advisory work for boards and management, and product counseling—but nearly all of his matters lie at the intersection of technology and the law, and involve cutting edge issues in AI, cryptocurrency, data privacy, cybersecurity, biotech, fintech, gaming, and software. Mr. Vandevelde has also represented clients in some of the highest profile, highest stakes cases in the country concerning government demands for personal data and technical assistance in connection with criminal and national security-related investigations.

From 2007 to 2014, Mr. Vandevelde served as an Assistant U.S. Attorney in the U.S. Attorney's Office for the Central District of California. He was Deputy Chief of the Cyber & IP Crimes unit, supervising one of the nation's largest teams of federal prosecutors dedicated to investigating and prosecuting computer hacking and intellectual property offenses. He was the lead prosecutor on numerous high-profile cyber-crime investigations, including cases involving corporate espionage, theft of trade secrets, APTs, botnets, distributed denial of service (DDoS) attacks, and other sophisticated cyberattacks by nation-state actors. Mr. Vandevelde handled the prosecution of several infamous hacking groups that infiltrated government and corporate servers around the world. He also successfully prosecuted numerous traditional white collar cases as part of the Major Frauds Section.

**EDUCATION**

**University of California**
Juris Doctor

**Stanford University**
Bachelor of Science

**CLERKSHIPS**

**U.S.D.C., Central District of California**

**RECOGNIZED**

**Litigation, White-Collar Crime & Government Investigations**
Chambers USA

**White Collar Crimes, Intellectual Property Litigation, General Litigation**
Super Lawyers

**Top 20 Cyber/Artificial Intelligence Lawyers in California**
Daily Journal


GIBSON DUNN