NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

CYBERSECURITY: COMPLIANCE & ENFORCEMENT

Presented by Jonathan DeMella
Partner, Davis Wright Tremaine
Government Contracts Counseling & Litigation

Notable Quotable

"Cybersecurity is the three-ton, rainbow colored elephant sitting atop every federal contractor's dining room table on Thanksgiving Day."

Alexander Major & Franklin Turner, *Guerrillas Of the NIST: DOD Re-attacks Supply Chain and Contractor Cybersecurity (Part 1),*" The Government Contractor, Vol. 61., No. 29, August 7, 2019.

NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

Recent Cases and Enforcement Activity

May 8, 2019: United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc. (E.D. Ca.)

- Aerojet's Senior Director of Cybersecurity alleges that company falsely certified compliance with DoD cybersecurity rules, that company did not:
  - satisfy NIST security controls as required by contracts, DFARS, NASA FAR Supplement;
  - disclose full extent of its noncompliance.
- Aerojet moves to dismiss, argues that "the DoD never expected full technical compliance because it constantly amended its acquisition regulations and promugulated guidances that attempted to ease the burdens on the industry." Court denies:
  - concludes nondisclosures are material under FCA because Government might not have awarded contract if it had known of noncompliance;
  - Rejects Aerojet's argument that it was sufficient to notify Government of some, but not all areas of noncompliance.

Note: Court (9th Circuit) remains unfavorable circuit for FCA defendants.

- Court relied on the fact that the alleged noncompliance "could" have affected the Government's decisions, despite evidence that it *actually did not.*
- Case highlights why contractors should be transparent about extent to which cybersecurity program does (and does not) meet applicable standards.
- DoD Cybersecurity clauses are not self-deleting!

July 31, 2019: First FCA Settlement based on Failure to Comply with Cybersecurity Requirements

- Qui Tam Relator asserts Government contractor sold video surveillance management software ("VSM") to Government agencies when it knew software allowed unauthorized access to Government information.
- Security flaws would have allowed access to passwords and stored data. Unauthorized user could:
  - "effectively shut down an entire airport by taking control of all security cameras and shutting them off," or
  - "access video archives of a large entity to obscure or eliminate video evidence of theft or espionage."
- Relator, Glenn, was terminated after reporting flaws to company.
- Glenn files qui tam action in 2011.
- Cisco defenses:
  - Cisco notified users in 2009 that additional security features necessary;
  - Cisco provided patch in 2013 advising customers to upgrade.
- After several years of litigation, Cisco pays $8.6 million to feds,18 states, D.C.
- **Takeaway**: DOJ, state attorneys general, qui tam bar perceive case as shift in FCA landscape. Cybersecurity noncompliance can be basis for significant FCA liability.

NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

DoD IG Audit of Protection of CUI on Contractor-Owned Networks and Systems, July 23, 2019

Summary Findings

- 2015-2018: **126 contractors reported 248 security incidents** to DoD Cyber crime center, including:
  - unauthorized access to networks by malicious actors;
  - stolen equipment (laptops, cell phones);
  - inadvertent disclosure of information;
  - data exfiltration;
  - exploitation of network vulnerabilities by malicious actors.
- IG identified multiple deficiencies among nine contractors assessed, including failure to:
  - identify and mitigate network and system vulnerabilities;
  - document and track cybersecurity incidents.
- DoD did not implement processes and procedures to track which contractors maintain CUI, placing DoD at greater risk of being compromised by cyberattacks.
- DoD contracting office did not take appropriate action to address "spillage of classified information to unclassified cloud, internal contractor network, and webmail environments."
  - DTRA, Contractor failed to report "spillage."
  - Classified information on unclassified cloud for almost 2 years.
- **Compromises constitute threats to national security**.

Failures by DoD Component Contracting Offices

DoD did not establish processes to:

- verify that contractors' networks and systems met NIST security requirements before contract award;
- notify contractors of the specific CUI category related to the contract requirements;
- determine whether contractors access, maintain, or develop CUI to meet contractual requirements;
- mark documents that contained CUI and notify contractors when CUI was exchanged between DoD agencies and the contractor; and
- verify that contractors implemented minimum security controls for protecting CUI.

Note: These are DoD failures, but will result in heightened scrutiny of contractor compliance.

Recommendations

- DTRA should revise agency's process for monitoring security incidents "to **verify that contractors took appropriate steps** to identify, respond to, and report security incidents."
- Director of DTRA should review performance of CO responsible for monitoring the security incident and consider administrative action for "**not ensuring that a contractor took actions** to remove classified information from its corporate network and cloud environment."
- Director should assess and document risk of leaving classified information unprotected in unclassified environments, develop new controls and policies.
- DoD CIO:
  - Use stronger passwords;
  - Lock accounts after 15 minutes of inactivity.
- Principal Director of Defense Pricing and Contracting:
  - Require pre award and post award (annually) validation of compliance for protecting CUI;
  - Track contractors that access, maintain or develop CUI as part of contractual obligations;
  - Revise policy so that DoD must validate compliance with minimum security requirements.

NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

Recent Changes in Cybersecurity Requirements for Federal Contractors

Key Developments 2018-2019

- Dec. 31, 2017: Last day to comply with **DFARS 252.204-7012**, control requirements of **NIST SP 800-171**.
- June 13, 2018: NIST issues **SP 800-171A**, to clarify security requirements through an assessment methodology to evaluate compliance with requirements.
- Sept. 28, 2018: Navy issues "**Guerts Memo**" calling for enhanced cybersecurity requirements on "critical" Navy programs.
- Oct. 28, 2018: SoD Mattis establishes the **Protecting Critical Technology Task Force**, to protect classified information, controlled unclassified information, and key data.
- Nov. 6, 2018: DoD issues **guidance** to facilitate consistent review of how SSPs, POAMs address NIST security requirements, and to assess impact of requirements "not yet implemented."
- Dec. 17, 2018: "**Fahey Memo**," recommends contract language not in DFARS re access to and delivery of contractors' SSPs, and flowdown of CDI to subcontractors.
- Jan. 21, 2019: "**Lord Memo**," empowers auditors to assess compliance with DFARS cyber clause via audits of a contractor purchasing systems.
- May 8, 2019: ***Aerojet Rocketdyne*** decision.
- June 11, 2019: **Armed Services Committee Report**: SoD to develop a "consistent, comprehensive framework to enhance the cybersecurity of the U.S. defense industrial base and to provide the congressional defense committees a briefing on the framework not later than March 11, 2020."
- June 19, 2019: NIST releases **SP 800-171 rev.2**:
  - Minor editorial changes, notes substantive updates to security requirements are coming in Revision 3;
  - Publishes new document, draft **SP 800-171B**, focusing on enhanced security requirements for "critical programs and high value assets" as a result of "ongoing barrage of cyber attacks" resulting in release of CUI.
- July 23, 2019: **DoD IG Audit**.
- July 31, 2019: ***Cisco*** case settles.
- Sept. 6, 2019: **Navy memo** extends "Guerts Memo" to NMCARS. Navy also amends NMCARS to instruct COs to seek equitable reductions, suspend progress payments for cybersecurity noncompliance.
- Oct. 3, 2019: **OUSD(A&S) issues RFI** for establishment of accreditation body for **CMMC program**. Responses were due Oct. 21, 2019.

Cybersecurity Maturity Model Certification

- Goal is to create a single unified standard for cybersecurity. Specific intentions:
  - "review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels";
  - "build[ ] upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements";
  - "be cost-effective and affordable for small businesses"; and
  - certify "independent 3rd party organizations to conduct audits and inform risk."

- Once implemented, offerors will be required to hold a CMMC certificate at a specified level or higher to be eligible for award on DoD solicitations.
- CMMC Certification will require assessment by Third Party Assessment Organization.
- The working estimate for the number of organizations requiring CMMC certifications is 300,000, with a very high percentage of those companies in the micro-, small-, and mid-size range.

See www.acq.osd.mil/cmmc

Summary of Current Initiatives

- **SP 800-171 rulebook is changing**.
- **Greater DCMA involvement** means that Contractors will be subject to heightened audit requirements, investigation, enforcement.
- **A Uniform System of Certification** under CMMC.

NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

What Are the Rules We Need to Know?

False Claims Act - Intent

- Ordinary contract breach, honest mistake does not typically give rise to FCA liability.
- Government/relator must prove contractor acted "**knowingly**," i.e., contractor:
  - had actual knowledge of the information;
  - acted in deliberate ignorance of the truth or falsity of the information, or;
  - acted in reckless disregard of the truth or falsity of the information.
- Proof of **specific intent** to defraud is not required.
- **Implied False Certification Liability**:
  - *"at least in certain circumstances, implied false certification theory can be a basis for liability"*
  - *"False Claims Act liability for failing to disclose violations of legal requirements does not turn on whether those requirements were expressly designated as conditions of payment. . . . What matters is not the label the Government attaches to a requirement, but whether the defendant knowingly violated a requirement that the defendant knows is **material** to the Government's payment decision"*

***Universal Health Serv., Inc. v. United States ex rel. Escobar*, 136 S. Ct. 1989, 1997 (2016).**

“Materiality” in Practice – Proving that Violation Was Not Material to the Government’s Payment

Questions to consider:

- Was Government first aware of the alleged violations prior to the submission of the claim?
- Did Government approve, explicitly or implicitly, a modification to the contractor’s obligation?
- Did Government take no action in response to the allegations of fraud or misrepresentation?
- Did Government not impose an administrative or payment sanction?
- Did Government renew any existing contract?
- Did Government enter into new contracts that omit the provisions that gave rise to potential liability?
- Did agency head publish favorable statements about the materiality of any similar cases?
- Does legislative history show little significance placed on the requirements in the statute or regulation at issue?
- Did government or qui tam plaintiff have other motives to pursue the action besides the materiality of the requirements?

Supreme Court’s view of materiality:

- Materiality looks to effect on the likely or actual behavior of the recipient of the alleged misrepresentation.
- Materiality standard is demanding.
- Government’s payment despite actual knowledge is “strong evidence” that requirements not material.

FAR: Compliance & Mandatory Disclosure

- Contractors should have a **written code of business ethics and conduct**. To promote compliance with such code of business ethics and conduct, contractors should have an employee business ethics and compliance **training program** and an **internal control system**.
- Contractor must timely disclose, in writing, to OIG, credible evidence that Contractor has committed:
  - "A violation of Federal criminal law involving fraud . . . or"
  - A violation of the civil False Claims Act.

FAR 3.1002 – Policy; FAR 52.203-13.

Note:

- Preponderance of evidence is standard.
- This requires a culture of compliance and disclosure.

Sidebar:

- April 2019, DOJ updated its guidance regarding corporate compliance enforcement; 3 questions a prosecutor should ask:
  - Is the corporation's compliance program well designed?
  - Is the program being implemented effectively?
  - Does the corporation's compliance program work in practice?

Cybersecurity Clause – Civilian Agencies FAR 52.204-21

- FAR clause applies when contractor's information system may contain "Federal contract information."
- "Federal contract information" – information **not intended for public release** that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government.
- "Covered contractor information system" – system that is owned or operated by contractor that **processes, stores, or transmits** Federal contract information.
- Applies to **all acquisitions**, including for commercial items, **except COTS items**.
- Clause flows down to subcontractors of all tiers in which sub has Federal contract information on system.

- Requires contractor to apply to apply **15** "**basic safeguarding requirements and procedures**" to protect covered contractor information systems.
- Contractor must also comply with other specific safeguarding requirements specified by federal agencies relating to covered contracting information systems generally or requirements for controlled unclassified information.

Note:

- FAR Council in process of amending regulation to make FAR compliant with SP 800-171. *See* FAR Case 2017-016.os`

Cybersecurity Clause – Civilian Agencies FAR 52.204-21

At a minimum, Contractor shall implement the following security controls:

- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Cybersecurity Clause – Department of Defense DFARS 252.204-7012

DFARS clause requires contractors and subcontractors to:

- **Provide "adequate security" to safeguard "covered defense information"** that resides on or is transiting through a contractor's internal information system or network;
- **Report cyber incidents** that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support;
  - *Cyber incident*: "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein."
  - *Compromise*: disclosure of information to "unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred."
- **Submit malicious software** discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center;
- If requested, **submit media** and additional information to support damage assessment;
- **Flow down** the clause in subcontracts for **operationally critical support**, **or** for which subcontract performance will involve covered defense information**.**

“Covered Defense Information” – What Does it Mean?

Term used to identify information that requires protection under DFARS Clause 252.204-7012. It means:

- Unclassified **controlled technical information** (“CTI”) **or other information** as described in the CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies **and** is −
- **Marked** or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of DoD in support of the performance of the contract; **OR**
- Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor **in support of the performance of the contract**.

Note:

- “In support of the performance of the contract” is ***not*** meant to include the **contractor’s internal information** (e.g., human resource or financial) that is **incidental** to contract performance.

“Controlled Technical Information” – What Does it Mean?

- CTI is a category of CUI specified on the CUI Registry.
- CTI means **technical information** with military or space application **that is subject to controls** on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Examples include: Research and engineering data;
  - Engineering drawings and associated lists;
  - Specifications;
  - Standards;
  - Process sheets;
  - Manuals;
  - Technical reports;
  - Technical orders;
  - Catalog-item identifications;
  - Data sets;
  - Studies and analyses and related information;
  - Computer software executable code and source code.

Marking and Identification of Covered Defense Information

DoD policy/regulations require DoD to:

- **Identify** covered defense information and **mark** information in accordance with DoD procedures for controlled unclassified information (CUI). *See* DoD Manual No. 5200.01, Vol 4, DoD Information Security Program: CUI (February 24, 2012).
- **Document in the contract** (*e.g.*, Statement of Work, CDRLs) information, including covered defense information, that is required to be developed for performance of the contract;
- **Specify requirements for the contractor to mark**, as appropriate, **information to be delivered to DoD**.

Contractor is responsible for

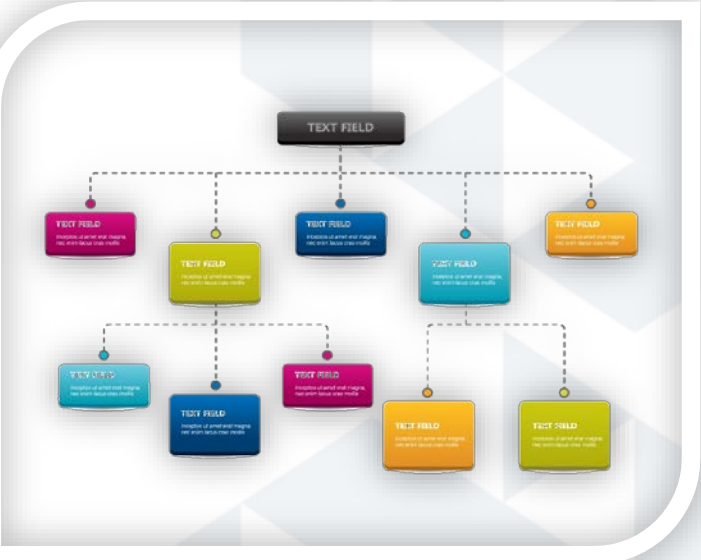
- Following the terms of the contract, which includes the requirements in the Statement of Work.

Subcontractor Flowdown

When should DFARS Clause 252.204-7012 flow down to subcontractors?

- The clause is required to flow down to subcontractors only when performance will involve operationally critical support or covered defense information.
- The contractor shall determine if the information required for subcontractor performance is, or retains its identify as, covered defense information and requires safeguarding.
- Flowdown is a requirement of the terms of the contract with the Government; enforcement is the responsibility of prime contractor.

- If a subcontractor does not agree to or cannot to comply with DFARS 252.204–7012, contractor cannot share covered defense information with the subcontractor.



Implementation: What Does "Adequate Security" Mean?

- Implementation of NIST SP 800-171's "fourteen families" of security requirements. Most requirements are about policy, process, and configuring IT securely.
- Implementation of additional security controls specified by evolving Defense Department requirements or as required by contract.
- Variance from NIST SP 800-171 requires submission to Contracting Officer, with a written explanation of:
  - why security requirement is not applicable; or
  - how an alternative but equally effective security measure is used to achieve equivalent protection.
- If contractor uses an external cloud service provider to store, process, or transmit CDI on contractor's behalf, contractor must ensure that CSP:
  - Meets requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline;
  - Complies with requirements for cyber incident reporting and damage assessment.

Note: CSPs processing data on DoD's behalf shall comply with DFARS 252.239-7010.

The “Fourteen Families”

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Configuration Management
5. Identification and Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Personnel Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System and Communication Protection
14. System and Information Integrity

Note:

- Requirements in each family divided among “basic” (fundamental) and “derived” security requirements.
- System Security Plan, Plan of Action addressed in section Chapter 3.12.

Cyber Incident Reporting

- If a contractor discovers a cyber incident that affects (1) an information system, or (2) CDI, or (3) the contractor's ability to perform requirements designated as operationally critical support, then contractor must:
  - Conduct a **review** of the evidence of compromise of CDI, including identification of compromised computers and analysis of compromised systems and networks, and;
  - Report cyber incident to DoD within 72 hours.
- **Cyber incident** means actions taken through the use of computer networks that result in a compromise or an **actual** or **potentially adverse effect** on an information system and/or the information residing therein.
- Contractor must protect, preserve all affected media and information for at least 90 days from submission of cyber incident report.
- Contractor will provide DoD access to perform **forensic analysis**.
- If DoD elects to conduct **cyber incident damage assessment**, contractor will provide DoD all information on request.

Contractor Representations & Certifications

- Submission of the proposal without qualification constitutes the contractor's representation of compliance with FAR, DFARS Cybersecurity clauses.
- Execution of the constitutes contractor's certification of compliance.
- Clauses place responsibility upon contractor to comply with security requirements, including NIST SP 800-171 and related requirements necessary to protect CDI.
- NIST SP 800-171 enables contractors to demonstrate implementation or planned implementation of security requirements through "System Security Plan" ("SSP") and "Plans of Actions & Milestones" ("POAM").
  - Security requirement 3.12.4 (System Security Plan) requires the contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
  - Security Requirement 3.12.2 (Plans of Action) requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems.

NEXT LEVEL LEADERSHIP

SOARING TO NEW HEIGHTS

And Finally...

Best Practices

- **Know your contracts' requirements**. Before entering into a contract, scrutinize and document contract and subcontract cybersecurity requirements, assess your ability to comply with requirements.
- **Document, document, document**. Document operational assessments, steps taken to comply with cybersecurity controls and requirements, and analyses regarding whether the company possesses information that requires protection. Document correspondence with Government of exceptions, waivers, applicability.
- **Work together**. Cybersecurity compliance requires a multi-disciplinary team with clearly defined roles and responsibilities. At a minimum, this team should include personnel from IT, Legal, Contracts, and Operations.
- **Conduct periodic assessments**. One time assessments are insufficient, particularly in view of recent guidance. Stay current on standards.
- **Be precise and transparent** when communicating extent of compliance to Government.
- **Remember that compliance is company's affirmative obligation**. Tacit acceptance by CO of contractor's representations does not relieve company of compliance obligations.

Thank you!

Jonathan A. DeMella

Davis Wright Tremaine
Government Contracts Counseling & Litigation
tel: 206.757.8338
jonathandemella@dwt.com

Please visit our Government contracts law blog:
https://www.dwt.com/blogs/government-contracts-insider