PUBLIC CONTRACTING INSTITUTE

Protection of CUI and Related Cybersecurity Issues for Federal Contractors

June 20, 2023

Meghan Doherty
Dinesh Dharmadasa

PUBLIC CONTRACTING INSTITUTE

pillsbury

Outline

- Defining, Identifying, and Protecting Controlled Unclassified Information
- Cybersecurity Contract Clauses
- Cybersecurity Maturity Model Certification Basics and Update
- Risk Landscape

Controlled Unclassified Information

What is CUI?

- At a high level, CUI is information that is sensitive but unclassified.
- Defined by E.O. 13556 as information that requires safeguarding or dissemination controls pursuant to applicable law, regulations, and government-wide policies but is not classified.
- CUI is not:
  - Classified information
  - Corporate intellectual property unless created for or included in requirements related to a government contract
    - *See CUI Registry category "Procurement and Acquisition"*

What is CUI?

- Executive Order 13556, *Controlled Unclassified Information*, required the Executive Branch to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and Government-wide policies."
- The National Archives and Records Administration (NARA) was named the Executive Agent responsible for overseeing the CUI program.

What is CUI?

- CUI is intended to replace the "alphabet soup" that agencies previously used to identify sensitive information. For example:
  - For Official Use Only/FOUO
  - Sensitive But Unclassified/SBU
  - Proprietary Business Information/PBI
  - Confidential Business Information/CBI
  - Controlled Technical Information/CTI
  - Law Enforcement Sensitive/LES
- *Note: These legacy markings still appear on many government documents*
- CUI also encompasses specific categories of data. For example:
  - Export Controlled Data
  - Personally Identifiable Information
- Focus on protecting information that historically has not been consistently and sufficiently protected.

What is CUI?

- Extremely broad definition
  - CUI includes marked information from the government (marked either as CUI or with a legacy marking) BUT ALSO
  - Information that *should have been marked* and
  - Information that a private party (contractor) provides to the government (in performance of a government contract).
- Simple, right?
  - Wrong! The CUI program has been widely criticized, by government and industry, for being complex, confusing, costly to implement and applied inconsistently across agencies.

What is CUI?

- As a practical matter, entities often struggle to figure out what CUI they possess.
- It is helpful to begin this analysis by considering what the government has an interest in protecting.
  - Crown jewels
  - What data could cause harm to the government or the public if it got into the wrong hands?
  - Helpful to think about systems/networks that contain CUI
- Entities should then review documents for CUI markings and review contracts for descriptions of CUI.
- It is also helpful to consider the CUI Registries.

CUI Registries

- Two CUI registry resources that provide government approved CUI categories and subcategories.
  - NARA CUI Registry
  - DoD CUI Registry
- These registries identify 23 categories and 84 sub-categories of CUI, along with examples and citations to relevant legal authorities.
  - Critical infrastructure physical security;
  - Water assessments;
  - Bank secrecy;
  - ***Controlled Technical Information***
- The DoD Registry contains the same categories as the NARA Registry, but contains some additional DoD-specific information.

What is CUI?

- Forthcoming Update to CUI Definition
  - FY2022 National Defense Authorization Act required clarification of CUI definition
  - Congress required DoD to develop framework to identify whether information is Controlled Unclassified Information and under what circumstances commercial information is considered CUI
  - Proposed definition/rule is forthcoming
  - May be reason for delay in CMMC 2.0

NIST SP 800-171 Rev. 2

- How must CUI be protected?
- The National Institute of Standards and Technology ("NIST") has established a set of controls for protecting CUI on non-Federal systems:
  - NIST Special Publication ("SP") 800-171 Rev. 2 "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*"
    - 110 controls, 14 control families (in Rev. 2)
    - Based on standards set forth in Federal Information Processing Standards ("FIPS") 199, FIPS 200, and NIST SP 800-52.

NIST SP 800-171 Rev. 3

- On May 10, 2023, NIST released an Initial Public Draft of Revision 3.
- Revision 3 aims to:
  - Streamline requirements by removing redundant and unclear requirements
    - Note: Rev. 3 includes 17 control families as opposed to 14 under Rev. 2
  - Clarify ambiguous or confusing requirements, making compliance more straightforward
  - Update the requirements to bring them inline with updates made to NIST SP 800-53 and 53B, "*Control Baselines for Information Systems and Organizations*"
  - Introduce the concept of organization-defined parameters ("ODP"), which would allow federal agencies to customize certain requirements by setting values for defined parameters

NIST SP 800-171 Rev. 3

- Timeline
  - Initial Public Draft released May 10, 2023
  - Public comment due July 14, 2023
  - Under DFARS 252.204-7012 (discussed below), contractors are subject to the version of NIST SP 800-171 that is in effect as of the time that the solicitation is issued.
  - In addition, agencies may modify existing contracts to include the revised requirements.

Cybersecurity Contract Clauses

CUI Contractual Obligations

- In the above slides, we discussed how contractors can identify CUI and the standards by which contractors need to protect CUI.
- Another key part of this conversation is how the government incorporates these requirements into its contracts.

DFARS 252.204-7012

- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting): currently required in all DOD contracts except COTS
- Mandatory flow-down for subcontracts involving *covered defense information* or operationally critical support (in Armed Forces contingency operations)
- DFARS 252.204-7012 requires contractors/subcontractors to:
  - Safeguard *covered defense information*
  - Report cyber incidents and preserve evidence and images

Self-Attestation of Compliance

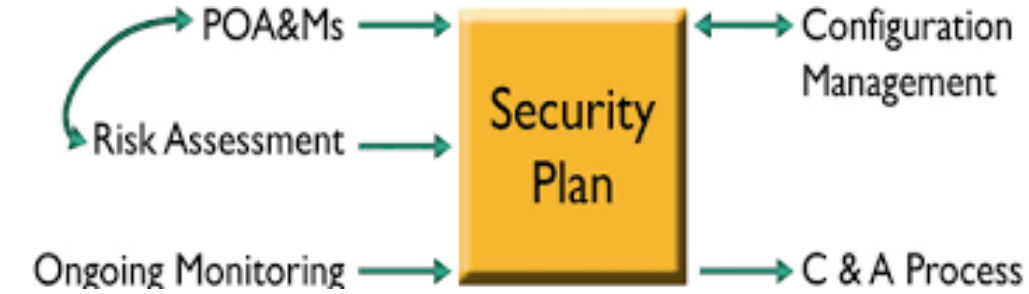
- DFARS 252.204-7008 “Compliance With Safeguarding Covered Defense Information Controls” is required in every solicitation, except for those solely for the acquisition of commercially available off-the-shelf (COTS) items
- The offeror represents that:
  - By submission of this offer, the offeror represents that it will implement the security requirements specified by [NIST SP 800-171] that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.
- DOD has interpreted “implementation” of NIST SP 800-171 as having a completed SSP and a POA&M for the relevant covered contractor information systems.

System Security Plans (SSP)

- SSP - The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system.
  - As noted in NIST SP 800-171 Rev 1
    - "There is no prescribed format or specified level of detail for system security plans"
  - The NIST SP 800-171 does require a description of the
    - "system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems"

Plan of Action & Milestones (POA&M)

- Plan of Action & Milestones (POA&M) - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones



Reporting Requirements

- Conduct a review for evidence of compromise of covered defense information
- “Rapidly report”- 72 hours of discovery to DOD Cyber Crime Center (“DC3”)
- Medium Assurance Certificate required
  - Get this in advance!
- Submit malicious software to DC3
- Preserve and protect images of all known affected information systems identified in paragraph

Information Sharing Update

- Proposed Rule: DoD Defense Industrial Base Cybersecurity (DIB CS) Activities
  - DoD currently runs a cyber-incident information sharing program that is limited to classified programs
  - On May 3, 2023, DoD issued a proposed rule to expand the scope of the program to contractors that "process, store, develop, or transit" CUI from DoD
  - Would allow contractors dealing with CUI access to critical cyber threat information
    - Even if the contractor does not have an existing active facility clearance at the Secret level
  - "All defense contractors who are subject to mandatory cyber incident reporting will be able to participate"

DFARS 252.204-7012 Flowdown Requirements

- The prime contractor is required to:
  - Include this clause in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items without alteration
  - Determine if the information required for subcontractor performance retains its identity as CDI and will require protection under this clause

DFARS 252.204-7012 Flowdown Requirements

- Subcontractors are required to:
  - Notify the prime contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST cybersecurity requirement to the contracting officer
  - Provide the incident report number, automatically assigned by DOD, to the prime contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD

Interim DFARS Rule

DFARS Case D041

- Issued September 29, 2020; effective November 30, 2020
- Three new DFARS clauses: DFARS 252.204-7019, 7020, and 7021
- Interim rules implement two assessment components:
  - NIST SP 800-171 DOD self-assessment and requirement for contractors to upload assessment to Supplier Performance Risk System ("SPRS") database, and
  - The CMMC framework DOD will establish over the next five years
- Self-assessments to NIST SP 800-171 standards required as of November 30, 2020

"Interim" DFARS Clauses

- DFARS 252.204-7019, Notice of NIST SP 800-171 DOD Assessment Requirements
  - Amends -7012 clause by requiring Contracting Officers ("COs") to verify offeror has current NIST 800-171 self-assessment on record
  - Contractors must post scores on SPRS
  - Assessments may not be more than three years old
- DFARS 252.204-7020, NIST SP 800-171, DOD Assessment Requirements
  - Provides DOD NIST SP 800-171 Assessment Methodology based on NIST 800-171 controls and a scoring
  - Basic, Medium, High level assessments

"Interim" DFARS Clauses

- DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification (CMMC) Level Requirements
  - Cybersecurity Maturity Model Certification Requirements
  - Prescribed for use in solicitations and contracts, including FAR part 12 procedures for the acquisition of commercial items (excluding COTS)
- Expect changes to this clause as CMMC 2.0 is rolled out

New*est* DFARS Clause Issued

- DFARS 252.204-7024, Notice on the Use of the Supplier Performance Risk System
  - Issued March 22, 2023
  - Allows COs to consider the information in SPRS, including supply chain risk information, when making an award decision.
  - "Contracting officers shall consider the supplier risk assessment available in the Supplier Performance Risk System"
    - Weight to give assessment?
  - Compliance with DFARS 252.204-7012, -7019, or -7020 is **not** currently used to generate supplier risk assessments
    - Only a matter of time - DFARS 7019 and 7020 currently require submission of self assessment to SPRS
  - Precursor to CMMC 2.0 becoming part of acquisition process

Scoring for NIST 800-171 Assessments

- To be eligible for awards on or after November 30, a contractor must complete the first level called a *Basic Assessment*.
- If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements.
- For each security requirement not met, the associated value is ***subtracted*** from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.

Scoring for NIST 800-171 Assessments

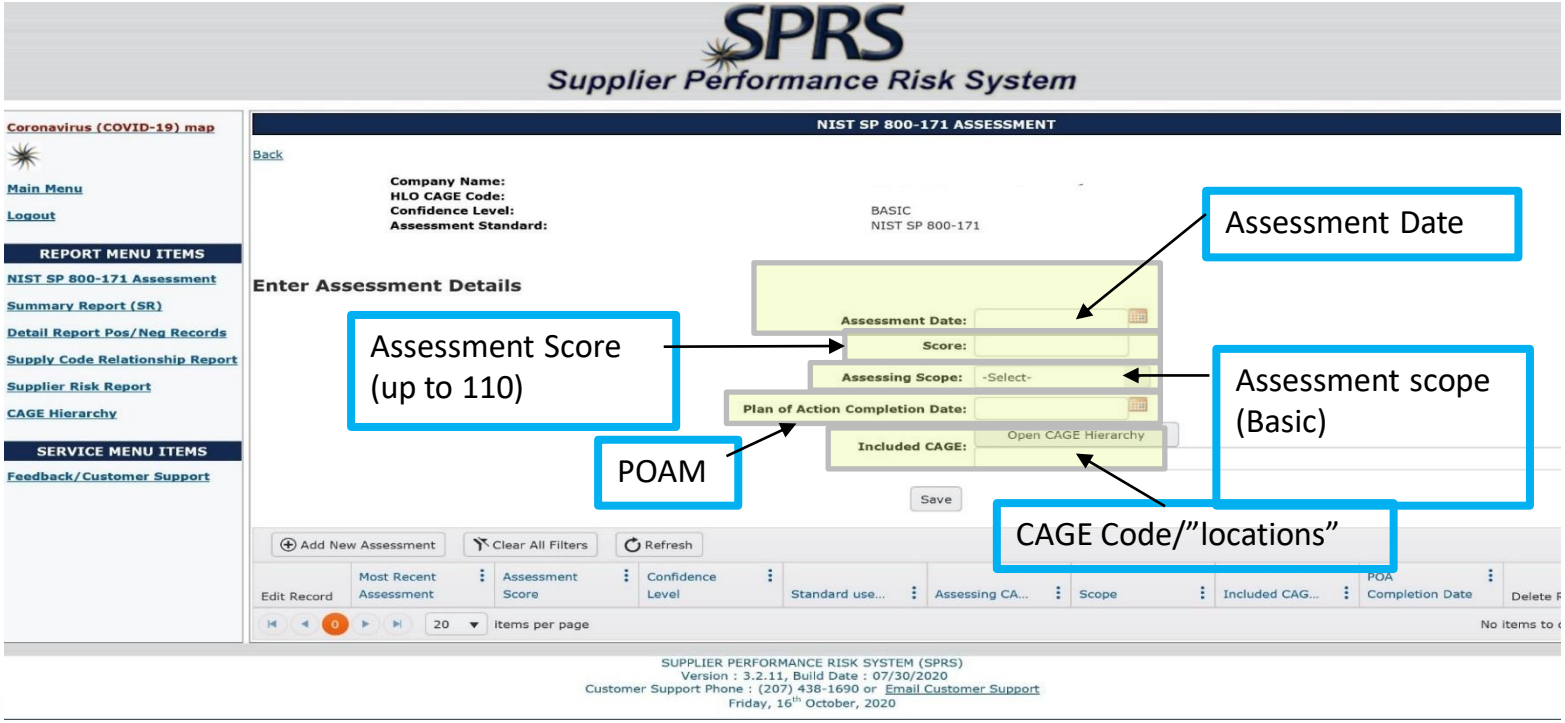
- Certain requirements have more impact on the security of the network and its data than others.
- This scoring methodology incorporates this concept by weighting each security requirement based on the impact to the information system and the DOD CUI created on or transiting through that system, when that requirement is not implemented.

SPRS: Weighted Security Controls

The cost of Security controls not implemented are weighted by vulnerability:

- +1 point per control for each security control, if fully implemented for a maximum of 110.
- 3 points of 5 points will be subtracted from the score of 110 for certain controls that are deemed to have a higher impact.
- 1 point is subtracted from the score of 110 for all remaining unimplemented Derived Security Requirements that have a limited or indirect effect on the security of the network and its data.

SPRS Assessment Entry Screen



PUBLIC CONTRACTING INSTITUTE

pillsbury

Cybersecurity Maturity Model Certification

What is CMMC?

- CMMC builds upon existing cybersecurity regulations by adding a self-assessment/verification component
- CMMC 1.0 was issued in 2020. In November 2021, DOD announced that it would be revamping CMMC and issuing CMMC 2.0.
- CMMC 2.0 is expected to contain significant changes.
- DOD estimates that the new rule will be issued around ~~March 2023~~ Fall 2023.

How Will CMMC Work?

- Upon release, government requests for proposals ("RFP") will specify the CMMC level required for that procurement
- Contractors must meet the RFP certification level by the time of award
- If not, contractor is not eligible to submit a proposal (and if it does, the proposal will be disregarded)
- Prime contractors must flow down the CMMC level to subcontractors
- Unless a higher level is specified, all contractors and subcontractors must meet CMMC Level 1

CMMC-Accreditation Body and Assessors

CMMC-AB

- 501(c)(3) non-profit formed in January 2020

C3PAO - Certified Third-Party Assessment Organizations

- Certified independent third-party organizations authorized to perform audits
  - Professional assessors to audit the more than 350,000 DOD vendors
  - Assessors do not work for the CMMC-AB; they work for a C3PAO
  - Licenses will match the assessment levels assessors permitted to conduct

Key Differences in CMMC 2.0

- On November 4, 2021 DoD announced major changes to the CMMC program, including:
  - Decreased number of assessment levels from 5 to 3
  - **Self-assessments** at Level 1 and Level 2
    - unless handling "critical national security information"
  - Reduces the total number of practices requires and aligns the required practices with standards issued by the National Institute of Standards and Technology (NIST);
  - Allows Plans of Action & Milestones (POA&Ms)
  - Allows for waivers to CMMC requirements under certain, limited circumstances
  - Rulemaking is estimated to be complete in 9-24 months (latest estimate Fall 2023)

Levels of Cybersecurity Maturity

- **Level 1 – Foundational:** will require 10 mandatory cybersecurity practices and require annual self-assessments
- **Level 2 – Advanced:** will require compliance with the 110 NIST Special Publication 800-171 controls, as set forth in DFARS 252.204-7012
  - Nonprioritized acquisitions: Annual self-assessments
  - Prioritized acquisitions: "Critical national security information;" triennial third-party assessments
- **Level 3 - Expert:** will require cyber hygiene that goes beyond the 110 NIST standard practices and require triennial *government-led* assessments

DOD Projections

- Costs are expected to be significantly lower than projected for CMMC 1.0, according to the DOD
- DOD to publish a “comprehensive cost analysis” of what contractors likely will spend to achieve each level of CMMC 2.0 compliance
- DOD estimates that the CMMC regulations will be promulgated in Fall 2023

Initial CMMC Challenges

- What data is considered CUI?
  - CMMC assessments must be scoped to cover all networks that contain CUI.
  - CUI is defined very broadly and likely covers data including engineering specifications; statements of work; pipeline control systems and design, construction and maintenance, maps, specifications and drawings received from the government.
- Scoping CMMC assessments
  - In order to save resources and expense, contractors will want to limit the scope of their CMMC assessments. To the extent that any system or application handles CUI, such a system will be included within the CMMC assessment.
- Supply chain/subcontractor compliance

Additional Steps Contractors Can Take Now

- Perform a self-assessment to consider current compliance
- Begin communications with supply chain to ensure that subcontractors are in compliance
- Consider representations and certifications to add to subcontracts
- Consider conversations with prime contractors to gauge expectations regarding upcoming CMMC requirements

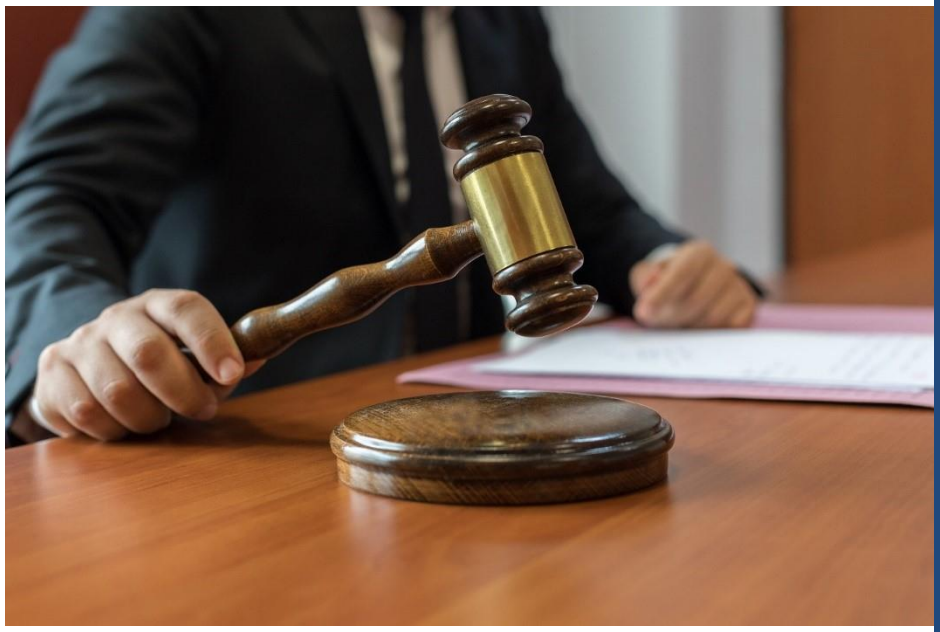
CMMC 2.0- Outstanding Questions

- How, when, and by whom will CMMC levels be determined for a multi-tiered supply chain working on separate, discrete aspects of a program?
- Who is considered a subcontractor for purposes of CMMC?
- Will certification levels of individual companies be public?
- Will contractors be able to challenge the CMMC assessments of competitors in bid protests?

CMMC 2.0- Outstanding Questions

- Will a certified contractor run the risk of de-certification while performing a contract?
  - Will there be periodic audits to determine if a contractor remains at a certification Level?
  - What happens if a contractor loses its certification during the performance period of a contract?
- What direction will third-party assessors be given regarding prioritizing which companies to assess first?

The Risk Landscape



Cybersecurity Update: DoD Memo on Ensuring Compliance with Cyber Clauses

- **DoD Memorandum, Contractual Remedies to Ensure Contractor Compliance with Cybersecurity Clauses**
  - Issued June 16, 2022
  - Memo reminds COs that:
    - Failure to make progress towards implementing NIST 800-171 per DFARS 252.204-7012 may be in material breach of contract;
    - Government's remedies include: "withholding progress payments; foregoing remaining contract options; and potentially terminating the contract in part or in whole;" and
    - They should, verify, prior to award, that the contractor has posted its DoD Assessment score in SPRS

The Civil False Claims Act

- Civil False Claims Act ("FCA") is used to recover damages where:
  - (1) "persons" (which includes individuals or entities);
  - (2) knowingly or with reckless disregard;
  - (3) submit false claims for payment;
  - (4) or who knowingly make or use false records or statements material to false claims.
- Persons that violate the FCA are liable for treble damages (three times the actual damages) plus civil penalties that range from $11,665 to $23,331 per false claim

The Civil False Claims Act – DOJ's Civil Cyber-Fraud Initiative

- DOJ recently announced the Civil Cyber-Fraud Initiative (the "Initiative") that will target contractors who knowingly fail to comply with cybersecurity protocols
- The Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients
- The Initiative aims to hold accountable those who put federal agency information or systems at risk by, among other things, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches
- Use of the FCA to address cybersecurity fraud is not a new development . . .

The Civil False Claims Act – DOJ's Civil Cyber-Fraud Initiative

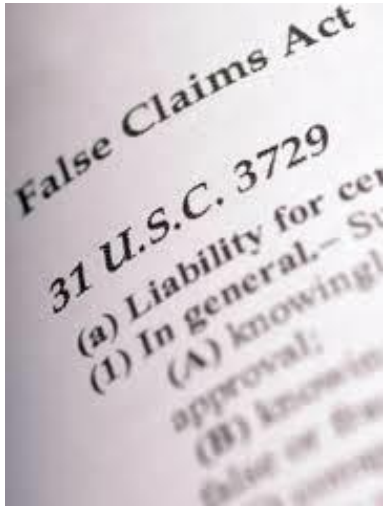
- **March 8, 2022 – DOJ's Cyber-Fraud Initiative's First Settlement**
  - Comprehensive Health Services LLC ("CHS") provided medical support services at U.S. government facilities in Iraq and Afghanistan
  - CHS submitted claims for the cost of a secure electronic medical record (EMR) system to store patients' medical records, including the identifying information of U.S. service members and diplomats
  - DOJ alleged that CHS failed to consistently store information on the EMR system and left records on an unsecure network (even after CHS personnel raised concerns)
  - CMS agreed to pay $930,000 to settle allegations (including other alleged violations)
  - DOJ press release noted that it "will continue to ensure that those who do business with the government comply with their contractual obligations, including those requiring the protection of sensitive government information."

The Civil False Claims Act – DOJ's Civil Cyber-Fraud Initiative

- **March 2023 – DOJ's Cyber-Fraud Initiative's Second Settlement**
  - Jelly Bean Communications Design LLC ("JB") maintained a federally funded website for the Florida Health Kids Corporation (FHKC)
  - JB invoiced for services that included a line item for "HIPAA-compliant" web hosting
  - Website suffered 3rd party hack and exposed patient information
  - Contrary to its representations, DOJ alleged JB's website was running outdated and vulnerable software
  - JB settled FCA allegations for $300,000

FCA Liability for Failure to Comply with -7012 Clause

- ***Markus v. Aerojet Rocketdyne Holdings, Inc.*, 2:15-cv-2245 WBS AC**
- U.S. District Court for Eastern District of California issued first decision regarding the FCA and the DFARS -7012 clause
  - Court held that *qui tam* relator plead sufficient facts to establish that the contractor misrepresented its compliance with the cybersecurity requirements to fraudulently obtain contracts with NASA and DoD

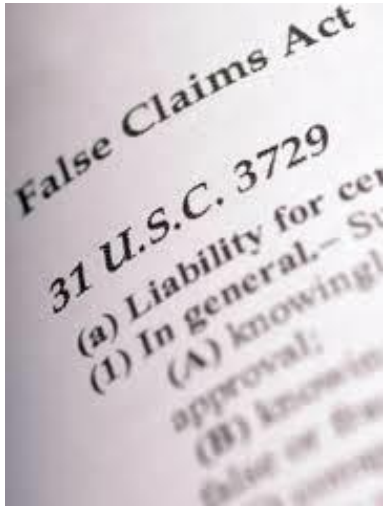


FCA Liability for Failure to Comply with -7012 Clause

- Qui tam relator worked at Aerojet Rocketdyne (AR) as the senior director of Cyber Security, Compliance, and Controls
- AR submitted SSP and POA&M stating they were not in full compliance with the -7012 requirements
- The FCA Claim survives motion to dismiss because Relator has plausibly pled that defendants' alleged failure to disclose fully its noncompliance was material to the government's decision to enter into and pay on the relevant contracts
- Jury trial is set to start on April 26, 2022

FCA Liability for Cybersecurity Flaws

- ***U.S. ex rel. Glenn v. Cisco Systems, Inc.*,**
  No. 1:11-cv-00400-RJA (W.D.N.Y.)
  - Cisco settled a multistate settlement over security surveillance
    system software sold to a collection of states, and various
    government agencies
  - Cisco will pay $2.6 million to the federal government and as
    much as $6 million to 15 states pursuant to two separate but
    related settlement agreements

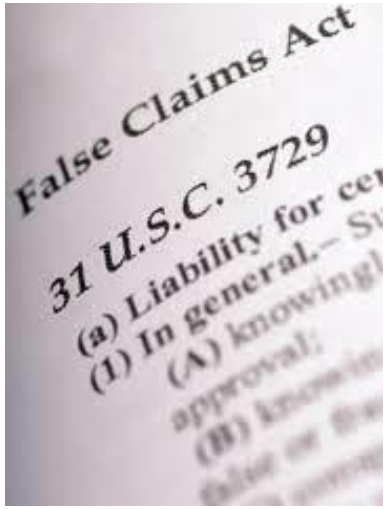


FCA Liability for Cybersecurity Flaws

- The whistleblower alleged that in 2009, Cisco had discovered security flaws in its software designed to control security camera systems. The flaws would permit unauthorized access to the system, with the potential to control and otherwise manipulate security cameras and the recorded footage
- Cisco failed to report or remedy these flaws until 2013 after the investigation had begun. The joint investigation uncovered no evidence that a hack or any unauthorized access of security surveillance systems ever took place, and the software has been discontinued

FCA Liability for Cybersecurity Flaws

- ***U.S. ex rel. Adams v. Dell Computer Corp.*, No. 15-cv-608 (D.C.C.)**
  - Qui tam relator alleged there was a hardware cybersecurity vulnerability in system control chips included in hundreds of millions of dollars' worth of computer systems Dell sold to the government
  - Relator argued that Dell had falsely certified that its systems were free from defects and in compliance with the DoD counterfeit prevention regulations



FCA Liability for Cybersecurity Flaws

- Qui tam relator had been a technology supplier to Dell and previously sued Dell over alleged patent violations
- The court noted that the government's cybersecurity policies do not specifically require defect-free products, but only computer systems with limited vulnerabilities and the means to remediate and mitigate any vulnerabilities that might appear
- The court held that relator failed to plead sufficient facts to establish that Dell's certification – despite the alleged vulnerability – was material to the government's decision to pay

Presenters

Meghan D. Doherty | Counsel
Northern Virginia
+1.703.770.7519
meghan.doherty@pillsburylaw.com

Dinesh Dharmadasa | Associate
Los Angeles
+1.213.488.7225
dinesh.dharmadasa@pillsburylaw.com