Cybersecurity Assessment/Cybersecurity Maturity Model Certification

The New DFARS Interim Rule

Akin Gump
STRAUSS HAUER & FELD LLP

November 30, 2020

Angela B. Styles
Partner

Robert K. Huffman
Partner

Agenda

- "Basic Assessment" Rubric
  - CUI Determination
  - Pre-Existing SSP and POAM
  - Systems that Transmit, Store, or Process CUI
  - Enterprise, Enclave or Contract Determination
  - Application of DOD NIST SP 800-171 Assessment Methodology
  - Input Basic Assessment.
- Subcontracts – Flow-down and Verification
- DOD Assessment and Use of Basic Assessment
- Medium/High Assessments
- Cybersecurity Maturity Model Certification
- Potential False Claims Act Liability.

Basic Assessment - CUI Determination

- Do you receive Controlled Unclassified Information (CUI) from DOD?
- ***May*** you receive CUI from DOD in the future under current contract?

  CUI Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is:

  > (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; or
  >
  > (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. 252.204-7012(a)

  - ITAR Controlled (but also additional requirements)
  - Specifications/Drawings
  - For Official Use Only (FOUO)
  - Basic Score, SSP, POAM?
  - When in doubt – ask the contracting officer.

Pre-Existing SSP and POAM

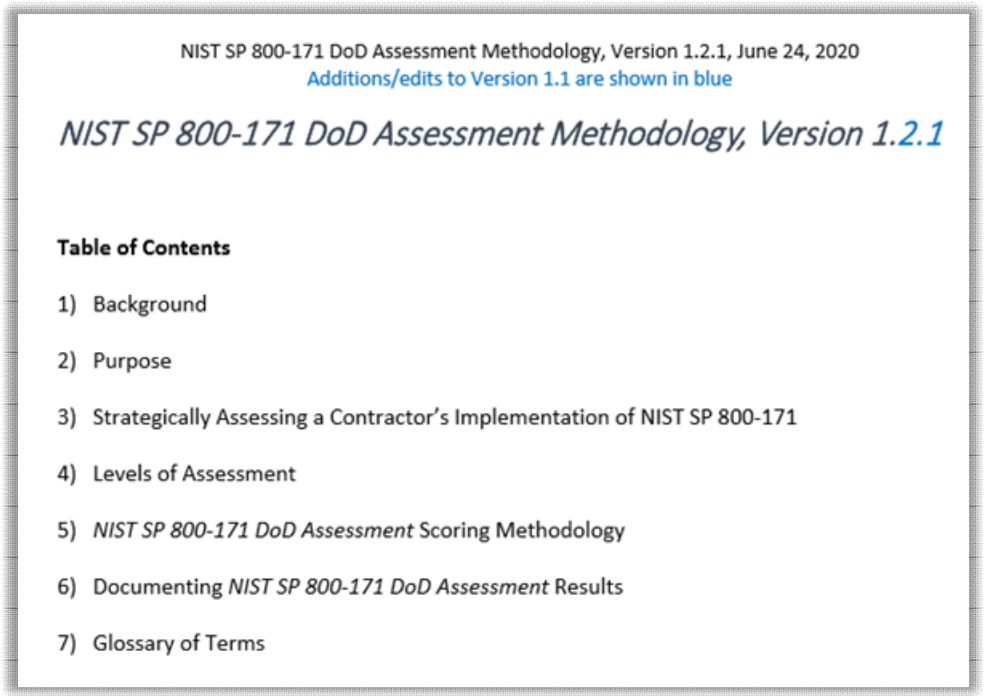
- If you have 252.204-7012 in a contract *and* you receive CUI, you have been required to apply the security requirements of NIST SP 800– 171 to systems transmitting, storing or processing CUI.
- NIST SP 800-171
  - 110 security requirements
  - Must create System Security Plan (SSP) and a Plan of Action and Milestones (POA&M).
- SPP and POAM – know which requirements you meet and when you meet others.
  - Likely will require updated to complete basic assessment.

Basic Assessment - Systems

- What systems transmit, store, process CUI?
- Follow the CUI.
  - How do you receive CUI? What is your email system? Do you have more than one system?
  - Where do you store CUI? Specific servers, server farm, cloud?
  - How do you “use” CUI? Does it make its way to the manufacturing floor?
  - You can and often will have multiple “systems” receiving, storing or processing CUI.
- Enterprise, Enclave or Contract
  - Your “basic assessment” will be of the systems where CUI is transmitted, store or processed
  - Enterprise - Some companies will assess the entire enterprise – developing a System Security Plan for entire organization.
  - Enclave - Many companies create an “enclave” and will have a System Security Plan (SSP) for the enclave or specific systems within the enclave. (If company can effectively isolate CUI, enclave may be most cost-effective approach – particularly for commercial companies).

Apply DOD NIST Methodology to Systems

- DOD NIST Methodology – “Basic Assessment” Score
- Take 110 requirements and score them based upon DOD template.
  - Not all NIST requirements are equal.
  - For each NIST requirement met, you receive one point.
  - For certain NIST requirements not met, you will have a deduction of three or five points.
  - Many companies will have negative scores.



NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020
Additions/edits to Version 1.1 are shown in blue

NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1

Table of Contents

1) Background
2) Purpose
3) Strategically Assessing a Contractor’s Implementation of NIST SP 800-171
4) Levels of Assessment
5) *NIST SP 800-171 DoD Assessment* Scoring Methodology
6) Documenting *NIST SP 800-171 DoD Assessment* Results
7) Glossary of Terms

Input/Send Basic Assessment to DOD

- Encrypted Email: webptsmh@navy.mil

System security plan	CAGE codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total score	Date score of 110 will achieved

- Supplier Performance Risk System
  - https://www.sprs.csd.disa.mil/ - to register and enter data.
  - Slightly different questions than encrypted email option.
    - No field for “Brief description of plan architecture.”
    - Self populates Cage Codes from www.SAM.gov (but they can be individually deleted).
    - Assessment Scope allows you to select: Enterprise, Enclave or Contract.
  - No fields for comments or to qualify answers.
  - Only DOD has access to information.

Subcontracts – Flowdown & Verification

- Flowdown - DFARs 252.204-7012(m)

  "[S]ubcontracts, 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, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause."

- Flowdown - DFARs 252.204-7020 (g)

  All subcontracts and other contractual instruments except COTS.

- Subcontractor Verification

  "The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800–171 security requirements, in accordance with DFARS clause 252.204– 7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800–171 DOD Assessment."

  Prime is not required to ask for score, SSP, or POAM.

DOD Use of Information - Unclear

- Basic Assessment Scores available to DOD contracting officers.
- No guidance to COs or contractors on use of information for awards.
- No guidance on evaluation criteria.
- Not expected to impact contract awards immediately.
- Caution from Cost/Benefit Analysis in preamble to Interim Rule:

  “Given that proper calculation of the score and its submission may well determine whether or not the company is awarded the contract.”

DOD Medium/High Assessment

- DOD will decide if you need a Medium or High Assessment before award.
- Medium Assessment
  - Conducted primarily by phone.
  - Expected to take less than three hours of contractor time.
  - DOD plans to conduct 200/year.
- High Assessment
  - Will be conducted by Government personnel using NIST SP 800–171A, ‘‘Assessing Security Requirements for Controlled Unclassified Information.’’
  - Expect to take 116 hours of contractor time.
  - DOD plans to conduct 110/year.
- Assessments Can be Disputed.

Legal Issues and Questions Concerning CMMC

- Can I dispute a CMMC level assessment by a C3PAO? How do I do that?
- Can I dispute a CMMC level certification by a C3PAO, the CMMC-AB or DOD? How do I do that?
- How do I know what CMMC level my subcontractors and their subcontractors must be certified to for a particular solicitation? Who makes that decision?
- What role, if any, can I play in making that decision if I am the prime contractor? Subcontractor?
- Is there any way I can challenge a requirement that a prime have a particular CMMC level? A requirement that my sub have a particular CMMC level?
- How can I find out my potential subs' certified CMMC levels?

Risk of Self Attestation, Self-Assessment and CMMC for Contractors – Potential False Claims Act Liability

- Inaccurate representations or assessment can potentially subject the contractor to liability for treble damages and civil penalties under the civil False Claims Act (FCA).
- FCA allows a private individual or "whistleblower" (aka the "relator") to file suit on behalf of the government (aka a "*qui tam*" action). Relator shares in up to 30 percent of any treble damages and penalties recovered in the suit.
- *Qui tam* suits are initially filed under seal for 60 days so that the government may investigate the allegations.
- The government may choose to intervene and prosecute the action.
- If the government declines to intervene, the relator may still pursue the action.
- Either way, the relator may be entitled to a bounty:
  - 15-25 percent of the recovery for intervened cases.
  - 25-30 percent of the recovery for non-intervened cases.

Elements of False Claims Act Liability

- Claim (Request for payment; failure to pay an obligation to the government – includes requests from subcontractor and suppliers).
- Falsity (false express certifications; false implied certifications (“misleading half-truths” resulting from undisclosed noncompliances); fraudulent inducement of contract.
- Materiality (Escobar’s “demanding” materiality standard).
- Knowledge (Actual knowledge of the falsity of the claim or statement; reckless disregard or deliberate indifference regarding the truth or falsity of the claim or statement; no showing of specific intent to defraud necessary).

FCA Liability Based on Representations of DFARS Cybersecurity Compliance—Case Study

- *U.S. ex rel Markus v. Aerojet Rocketdyne Holdings, Inc*., 381 F. Supp. 3d 1240 (E.D. Cal. 2019) (May 8, 2019)
  - *Qui tam* relator was Senior Director of Cybersecurity Compliance and Controls for Aerojet before his employment was terminated in 2015 after filing an internal ethics complaint. Relator alleged that Aerojet violated the FCA by making false representations of compliance with the DFARS and FAR security controls and fraudulently inducing DOD and NASA to award it contracts in reliance on such representations.
    - Specifically, the relator alleged that Aerojet "fraudulently entered into contracts with the federal government despite knowing that [it] did not meet the minimum cybersecurity requirements to be awarded contracts funded by DOD or NASA." Relator "avers that {Aerojet] repeatedly misrepresented its compliance with these technical standards in communications with government officials."
  - Aerojet moved to dismiss relator's complaint on the grounds that relator had failed to allege facts sufficient to demonstrate the materiality of the alleged noncompliances under the standard for materiality established by the Supreme Court's decision in Universal Health Servs., Inc. v. Escobar, 136 S. Ct. 1989 (2016).

FCA Liability Based on Representations of Compliance with DFARS Cybersecurity Controls—Case Study (cont'd)

- The district court **rejected** Aerojet's materiality arguments:
  - First, the court rejected Aerojet's argument that it had disclosed to the government noncompliances with the NIST 800-171 cybersecurity standards. The court found that "while it may be true that [Aerojet] disclosed some of its noncompliances, a partial disclosure would not relieve [Aerojet] of liability where [it] failed disclose noncompliance with material statutory, regulatory, of contractual requirements", citing *Escobar*.
  - Second, the court rejected Aerojet's argument that the Government's awarding it new contracts and DOJ's decision not to intervene in the qui tam suit demonstrated that the Government did not regard noncompliances as material.
  - Third, the court rejected Aerojet's argument that cybersecurity did not go to the central purpose of the contracts, which were for missile defense and rocket engine technology.
  - Finally, the court rejected Aerojet's argument that DOD never expected full compliance with the NIST 800-171 standards because it constantly amended the -7012 clause and promulgated guidances that attempted to ease the burden on industry, including allowing industry to use SSPs and POAMs to demonstrated compliance with the standards. The court found that even if DOD never expected full compliance, the degree to which the company was or was not compliant could still matter to the Government's decision to enter into the contracts in question. "Accepting relator's allegations as true, the government may not have awarded these contracts if it knew the full extent of the company's compliance, because how close [the company] was to full compliance was a factor in the government's decision to enter into some contracts."

When Can Ambiguous Laws Result in An FCA Violation?

- Several circuits have ruled that if an FCA defendant has a reasonable interpretation of ambiguous rules that FCA scienter cannot be demonstrated unless the Government has issued official guidance to warn defendant away from its reasonable interpretation.
- See, e.g., *United States v. Allergen, Inc*., 746 F. App'x 101, 109-10 (3d Cir. 2018) (although the court was not prepared to find that the defendants had the best interpretation of the statute, it found that the plaintiff had failed to plead an FCA cause of action because the defendants had a reasonable interpretation of an ambiguous statute, and the relator did not plead that the Government had published any official guidance that would "warn" defendants away from their reasonable interpretation).
- *U.S. ex rel. Purcell v. MWI Corp*., 807 F.3d 281, 289 (D.C. Cir. 2015) (defendant did not knowingly submit false claims when there was no "'guidance from the courts of appeals' or relevant agency 'that might have warned [the defendant] away from the view it took'") (citation omitted).

When Can Ambiguous Laws Result in An FCA Violation? (cont.)

- Given this precedent:
  - Does the entity have to have actually relied on the interpretation that it is advocating?
  - Is a good faith belief evidenced by an internal analysis plausibly arriving at a conclusion that there is compliance?
  - Does the entity have to inquire of counsel to arrive at a good faith belief?
  - Does the entity have to inquire of the Government – regarding every ambiguity – to form a good faith belief? And, if so, does it have to be through an advisory opinion? How formal does it have to be?
  - What does it take for the Government to "warn away" an entity from a particular interpretation?
  - Is there a difference between a complex regulation and an ambiguous regulation? Can a regulation be considered ambiguous simply because it is complicated or complex?
  - Are DOD Assessments or CMMC level certifications "opinions"? What are the standards used to determine whether opinions are "false" under the FCA?

Contact Information

Angela Styles
atyles@akingump.com
+1 202.887.4050

Robert Huffman
rhuffman@akingump.com
+1 202.887.4530