Software and Supply Chain Assurance Forum
June 1, 2023

Regulated Cybersecurity: Where We Are. The Consequences of Non-Compliance

Robert S. Metzger

This presentation reflects my personal views and should not be attributed to any client of my firm or organization with which I have been or am now involved or affiliated.

A Decade of Cyber Initiatives

February 2013:	Executive Order 13636: "Improving Critical Infrastructure Cybersecurity"
November 18, 2013:	Final Rule: "Safeguarding Unclassified Controlled Technical Information"
May 8, 2015:	NARA Proposed Rule: "Controlled Unclassified Information"
June 19, 2015:	NIST SP 800-171: (Final)
August 11, 2015:	OMB draft Guidance: "Improving Cybersecurity Protections in Federal Acquisitions"
August 26, 2015:	Interim Rule: DFARS "Network Penetration Reporting and Contracting for Cloud Services"
October 8, 2015:	DoD Class Deviation – Multifactor authentication (local/network access) – 9 mos.
December 30, 2015:	Am'd Interim Rule: "Network Penetration …" (defers cyber obligation to 12/31/2017)
September 14, 2016:	NARA Final Rule, "Controlled Unclassified Information"
June 2019:	CMMC (1.0) announced
February 2020:	CMMC (1.0) Model documents
September 2020:	CMMC Interim Final Rule (IFR) Published; Effective Nov. 30, 2020
November 2021:	CMMC 2.0 announced (5 levels compressed to 3; SP 800-171 baseline)
December 2021:	DoD publishes Level 1 and Level 2 Scoping Guidance & Assessment Guides
March 22, 2023:	Final Rule, Use of Supplier Performance Risk System (SPRS) Assessments
May 3, 2023:	Proposed Rule, Expanding Defense Industrial Base (DIB) Cybersecurity (CS) Activities
May 10, 2023:	NIST SP 800-171 Rev. 3 Initial Public Draft

Cyber Compliance Obligations
CMMC

Every Contractor With CUI and the DFARS 252.204-7012 Clause Is Now Required to Provide Adequate Security for CUI Using the 110 Safeguards of NIST SP 800-171

CMMC 2.0 Will Add Required Independent Assessments

Cyber DFARS Requirements: Summarized

1. The **-7012 DFARS** clause requires companies to implement NIST SP 800-171.
2. This requirement is to **protect** the **confidentiality** of **Controlled Unclassified Information** (CUI)
3. The **-7019 DFARS** clause requires a **current** SP 800-171 **self-assessment** to be considered for award. Companies are to **self assess** using the DoD Assessment Methodology.
4. Offerors must **post** their self-assessment **scores** on DoD's Supplier Performance Review System (**SPRS**).
5. Contracting Officers may consider scores SPRS scores as part of "supplier risk" under the DFARS -7024.
6. DFARS-**7020 DFARS** requires each contractor to **provide access to "facilities, systems and personnel"** for **DoD assessment**.
7. DoD has current methods for its DIBCAC unit to **assess contractor implementation** of cyber requirements.
8. DIBCAC **conducts random** "**Medium Assessments,**" reviewing System Security Plans vs. SPRS scores. "**High Assessments**" are on-site verification, examination and demonstration.

Rulemaking – Codifying CMMC 2.0

Changes will be released through a Proposed Rule. A public comment period of at least 60 days will follow publication of the Proposed Rule. DoD "adjudication" likely will take 12 – 15 months after the comments closing date. The 2.0 rules may not be effective until late Fall 2024.

- DoD has **mandatory rulemaking obligations**, under the OFPP Act, that must be addressed as part of the CMMC 2.0 implementation. The proposed rule package must be approved by OMB's OIRA unit.
- Rulemaking under 32 CFR is required to establish the CMMC program. **The Pt. 32 rules will be new.**
  - Rulemaking under 48 CFR is required to update the contractual requirements in the DFARS to implement the CMMC 2.0 program. **These will be both new regs and updates (revisions) of Pt. 48 present regs.**
  - The DoD has suspended mandatory CMMC certification until the effective date of the 2.0 rules.
  - DoD continues to encourage the DIB sector to enhance their cybersecurity posture during the interim period.
  - Until CMMC 2.0 regs are effective, DIB companies can seek a Joint Surveillance Assessment (JSV).
- **DoD (OCIO) leadership has recently affirmed their commitment to CMMC 2.0 and said they are targeting late Fall 2024 to for CMMC contract requirements.**
- The Department also is working on an overarching cybersecurity framework, apparently CSF-based, per NDAA FY 2020 § 1648 and NDAA FY 2024 § 1526. Reportedly, CMMC will be the "Protect" component.

Questions the 2.0 Regs May Answer

- What will be included in Part 32 CFR? Perhaps:
  - **Answers to the small business challenge.**
  - Rollout plan and priorities (rationale, programs, contracts…
  - Roles & Responsibilities within DoD and with The Cyber AB.
  - Guidelines regarding CSPs, MSPs, MSSPs, and other ESPs.
  - Document DCMA / DIBCAC roles and basis for "Joint Surveillance Assessment."
  - Formalize adoption and use of the Level 1 and Level 2 Scoping & Assessment Guides.
  - "Dispute" resolution as to C3PAO results & as to contract eligibility.
  - "Criticality" distinctions among CUI categories (?)
  - Purposes and limits of the CMMC Assessment Process (CAP).
  - How to handle PO&AMs and resolution of assessment gaps.
  - Clarification of assessments required for Level 1 (FCI, not CUI).
  - Explanation of Level 3 implementation.

Key Point:
CMMC 2.0 does not change the fundamental DFARS compliance requirements and it uses the same NIST -171 security baseline. CMMC 2.0 implements mandatory third-party assessment – for many.

EITR*: The Business Case for (Just) Compliance?

* Elephant In The Room

- DoD announced CMMC 2.0 in Nov. 2021:
  - "Simplifying the CMMC standard and providing additional clarity on cybersecurity regulatory, policy, and contracting requirements."
  - *Is this more aspiration than reality? Over time, the apparent requirements of the CMMC regime have become more complex, if not more confusing, despite no change in the core requirements of SP 800-171 which largely the same as in 2015.*

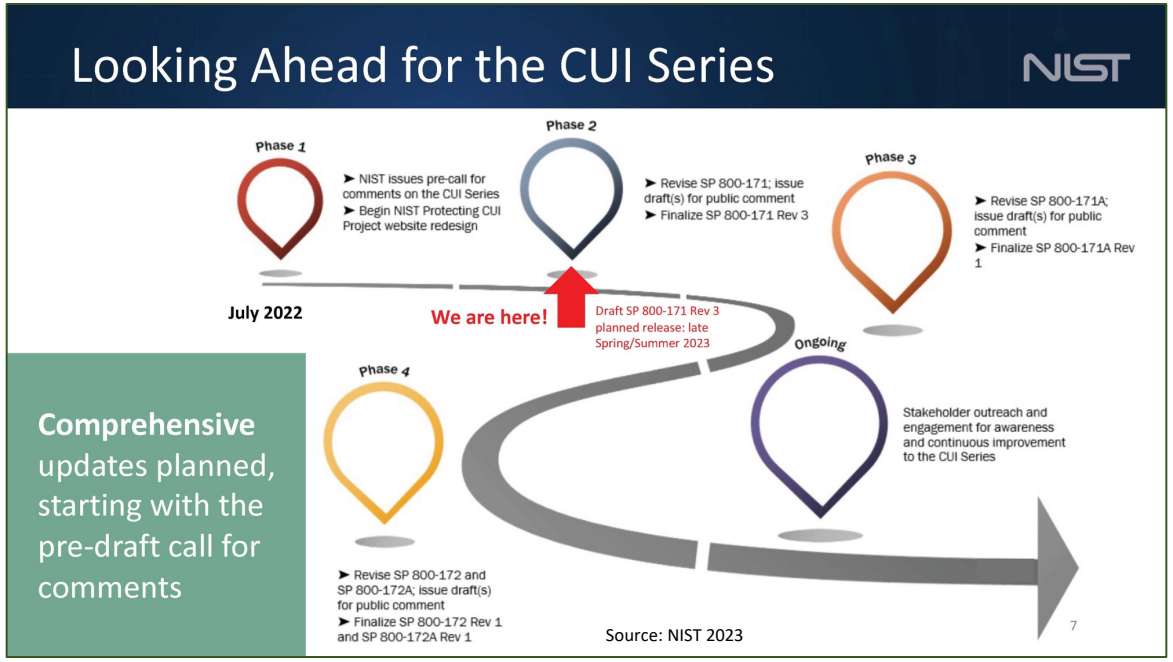
Affordability remains a fundamental challenge. If the business case is not present, companies will minimize, misrepresent, or exit.

- The cyber requirements cannot and should not be eased– the threat environment has worsened over time. SMEs are targets.
- *But* DoD must facilitate means by which more companies can achieve compliant security more affordably.

"Flash" Discussion of Key Issues

- Small Businesses: *Consider: deferred start of required SME assessments; extended period within which a required assessment must be satisfied; limiting assessments to CTI and export-controlled information; more time and latitude to address PO&AMs.*
- Lowering Costs: *Promote the availability of enclaves; clarify selection criteria and priority for required SME assessment; articulate "sufficiency" assessment objectives.*
- Cloud and MSPs: *Establish reasonable process and achievable ground rules to establish trusted MSPs, MSSPs and other ESPs; avoid requiring FedRAMP Moderate.*
- Industry Reaction to Proposed Rules: *Expect much study, considerable anxiety, some consternation, many Comments and … compliance actions by many companies!*
- Enterprise Actions: *More companies will seek to validate SPRS scores through DIBCAC, JSV or other trustworthy assessment. A high SPRS score provides a competitive advantage and reduces exposure to contractual actions or the FCA.*

SP 800-171 Rev. 3: What's ahead?



Revision 3 is better in explaining many individual requirements. However, the greater detail may make it more difficult for many businesses to satisfy 800- 171, when Rev. 3 is effective, and it could be extremely difficult for smaller enterprises. While easier to understand, the elaboration and detailing of controls may drive contractors toward a more rigid (and expensive) compliance approach. Independent third-party assessment would be required. A great concern is the prolific use of "Organizationally Defined" values." Who decides, when, according to what, and how is consistency achieved??

- NIST issued the Initial Public Draft (IPD) of Rev. 3 on May 10, 2023. Comments are due on July 14, 2023. NIST is hosting a public webinar on June 6, 2023, to discuss the draft. After receipt of comments, NIST will decide whether to issue another draft, and seek further public comments, or issue the final Rev 3. This cycle likely will take until early next year.
- Unsurprisingly, Rev. 3 aligns more closely with SP 800-53 Rev. 5, which NIST released on September 23, 2020. Not until May 30, 2023, did the FedRAMP PMO release the approved FedRAMP Rev. 5 baseline. It also provided a Transition Guide.
- It took 32 months for FedRAMP to release the new Rev. 5 baselines and describe what is expected during the transition. The transition is not immediate - nor could it be. This approach is only suggestive of what DoD will do to implement Rev. 3 to NIST SP 800-171, when it becomes final (likely in 2024).
- The present phrasing of DFARS -7012 requires contractors to employ the revision of SP 800-171 that is "in effect at the time the solicitation is issued or as authorized by the Contracting Officer." However, IMO, DoD will employ a Class Deviation to defer immediate implementation of Rev. 3. It did so, e.g., for MFA in 2015.
- DIBCAC and CMMC assessment methods are built upon 171 Rev. 2 and its companion, SP 800-171A. NIST will not start to revise 171A until after 171 Rev. 3 is done. It will take time. Consequential changes to CMMC Scoping and Assessment Guides can be completed only afterwards. The Cyber AB will need to change training and accreditation methods and refresh certifications already awarded.
- **It could take several years to complete necessary revisions to the assembly of existing process and documents that are built upon Rev. 2 and SP 800-171A.**

DoD's Present Tools & Remedies

Expect DoD to Increase Cyber Compliance Actions

DoD Has Many Contractual and Administrative Remedies Should Companies Fail to Comply with the Present DFARS Cyber Regime.

Continuing Obligations (-7019 and -7020); new -7024

- Self-assessment per -7019 is to use the NIST SP 800–171 DoD Assessment Methodology.
  - The Basic Assessment results in a "summary level score" of the contractor's compliance with NIST SP 800-171 (e.g., 95 out of 110). DoD's updated Cyber FAQs, at A122, states that the "Basic Assessment" is to be "conducted in accordance with NIST SP 800-171A."
  - DIBCAC may conduct a "Medium" or "High" assessment under DFARS 252.204-7020.
  - *DIBCAC has recently stated, publicly that is has or intends to hire nearly 100 GS-13 level assessors and that the rate of DIBCAC assessments will grow from 5/wk to 12/wk.*
- Contractors post their summary level scores in the Supplier Performance Risk System (SPRS), DoD's source for supplier and product performance information.
  - Contractors also post the "[d]ate that all requirements are expected to be implemented"
- The newly effective DFARS 252.204-7024 enables Contracting Officers to consider "supplier risk" during competitive evaluation; they *may* but are not required to consider SPRS scores as part of supplier risk. Low self-posted scores risk award; high validated scores may be a competitive advantage for USG and for primes and higher-tier buyers.

In the Interval: Increased Federal Oversight

- Between today and the eventual effective date of the final "CMMC 2.0" rules, we can expect DoD to increase its compliance oversight and enforcement. Poor "fidelity" to SPRS to actual is known.
- An official DoD (DPC) document of June 16, 2022, states:

> "Failure to have or to make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of contract requirements. Remedies for such a breach may include: withholding progress payments; foregoing remaining contract options; and potentially terminating the contract in part or in whole."

- After a cyber incident reported to Defense Cyber Crime Center (DC3), a DoD requiring activity can request an assessment of a contractor's compliance with DFARS 252.204-7014. Knowing failure to report increases exposure to allegations under the False Claims Act. (See below.)
- Beyond these contractual mechanisms, DoD itself can investigate allegations of non-compliance, and DCMA's DIBCAC unit can make "referrals" to prompt such investigations. A gross disparity between a claimed, posted SPRS score and DIBCAC assessment results may prompt investigation.
- Suspension or debarment is a risk if there is willful failure to perform cyber violations. In 2019, DHS suspended a supplier of license-plate scanners after it was hacked.

DoJ's Civil Cyber Fraud Initiative & The False Claims Act

Strong and Documented Cyber Measures Are the Best Way to Avoid FCA Exposure

"Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative"

Department of Justice, Oct. 6, 2021

- The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by 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. The benefits of the initiative will include:
- Building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners.
- Holding contractors and grantees to their commitments to protect government information and infrastructure.
- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.
- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.
- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.
- Improving overall cybersecurity practices that will benefit the government, private users and the American public.

"Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit"

Department of Justice, Oct. 13, 2021

"Three Common Cybersecurity Failures are prime candidates"

First, the False Claims Act is a natural fit to pursue knowing failures to comply with cybersecurity standards. When government agencies acquire cyber products and services, they often require contractors and grantees to meet specific contract terms, which are often based on uniform contracting language or agency-specific requirements.

Second, False Claims Act liability may be based on the knowing misrepresentation of security controls and practices. In seeking a government contract, or performing under it, companies often make representations to the government about their products, services, and cybersecurity practices.

Finally, the knowing failure to timely report suspected breaches is another way a company may run afoul of the Act. Government contracts for cyber products, as well as for other goods and services, often require the timely reporting of cyber incidents that could threaten the security of agency information and systems.

False Claims Act

- DOJ's Primary Civil Enforcement Tool
- The FCA is extremely broad and imposes liability on anyone who:
  - "knowingly presents, or causes to be presented, a **false or fraudulent claim** for payment or approval"; or
  - "knowingly makes, uses, or causes to be made or used, a **false record or statement** material to a false or fraudulent claim"
- FCA cases may be brought by the Government (DOJ) or whistleblowers ("*qui tam*" suits).
- Four essential elements required to prove FCA violation:

  (1) false statement or fraudulent course of conduct,

  (2) made with "scienter" (i.e. **knowledge**),

  (3) that was "**material**," causing

  (4) the Government to pay or forfeit money.

FCA Theories of Liability

- Actual false claim (e.g., invoice for services not rendered)
- Express false certification (e.g., contractor directly certifies its compliance with a requirement it breached).
- Implied false certification. Applies where the contractor:
  - makes specific representations about the goods/services provided; and
  - fails to disclose noncompliance with material statutory, regulatory or contractual requirements.
- Promissory fraud (aka "fraud in the inducement")
  - May apply if a contract/option was obtained by false statements or fraudulent conduct.
  - Liability attaches to each claim for payment submitted under a contract secured by fraud (i.e., potential liability = all money paid under the contract)

Liability and "Whistleblowers" Provisions

"Whistleblowers with inside information have been critical to identifying and pursuing new and evolving fraud schemes that might otherwise remain undetected. They also bring considerable technical expertise to complex investigations. As they have in many other aspects of False Claims Act enforcement, we expect whistleblowers to play a significant role in bringing to light knowing failures and misconduct in the cyber arena. False Claims Act enforcement and whistleblower reporting will help spur compliance by contractors and grantees." [Brian Boynton, Oct. 13, 2021]

- The FCA includes strong financial incentives and protections for whistleblowers (company insiders).
  - *Qui tam* plaintiffs are entitled to 15-30% of the Government's recovery.
  - Anti-retaliation provisions protect whistleblower efforts to report and stop fraud.
- The FCA imposes significant liability for violations.
  - Treble damages (3x the Government's actual damages)
  - Fines ($11,665 to $23,331 per false claim)
- Defense of FCA allegations are very expensive and disruptive.

FCA Results – So Far

DoJ Has Recovered Substantial Sums

More Cases Are Pending

U.S. ex rel. Markus v. Aerojet Rocketdyne

- Markus, Aerojet's former Senior Director of Cybersecurity brought a "qui tam" case under the FCA, filing a complaint under seal on Oct. 29, 2015. The Court denied Aerojet's Motion to Dismiss on May 8, 2019.
- On October 6, 2021, DoJ announced the "Civil Cyber Fraud Initiative."
- Two weeks later, on Oct. 20, 2021, DoJ filed a "Statement of Interest" in the case, arguing that Aerojet's alleged false claims were "material" to the Government's decision to pay, despite the defendants' argument position that the Government continued to do business knowing knew of the cyber deficiencies.
- On February 1, 2022, the Court ruled on cross Motions for Summary Judgment and permitted the case to go to trial. See notes below.
- The case was settled on April 27, 2022– after 1 day of trial. Aerojet paid the U.S. $9M; Marcus received $2.61M (29% of recovery). The Company denied wrongdoing.

MSJ Decision: Aerojet argued there could not have been "fraud in the inducement" because Aerojet disclosed to both NASA and DoD that it was not fully compliant with the cyber requirements then in the DFARS. The Court found these disclosures hold "less weight" because they may have been incomplete. (p. 11) The Court was particularly interested in allegations that Aerojet failed to timely report four cyber incidents that allegedly caused "huge quantities of data" to leave the contractor's network.

My comment, just after the settlement:

"Taking the length of the proceeding into account, whistleblowers and their 'relator' counsel and even the Department of Justice, should temper their enthusiasm for using the False Claims Act as a weapon to 'police' contractor cyber compliance." "FCA cases are tough to bring and expensive to pursue."

Other Federal FCA Decisions (+ RSM comments)

- *Comprehensive Health Services*
  - Settled on Feb. 28, 2022, DoJ recovered $930,000. Much of the case included mischarging for medical services in Iraq, but there also were allegations that CHS failed to adequately secure medical records.
- *Jelly Bean Communications Design*
  - Settled on March 14, 2023, DoJ received $293,771. DoJ alleged Jelly Bean knowingly failed to properly maintain, patch, and update software, exposing personal information that was hacked

Neither case concerned DoD DFARS cyber requirements. The cyber violations arguably were collateral to other False Claims. These defendants likely were incapable of vigorous defense.

DoJ and whistle blowers may be pursuing bigger cases against prominent companies. But the facts in these cases rarely are so clear as (arguably) were present in *Aerojet,* where the settlement arguably was modest in context.

Some FCA cases present egregious facts with strong evidence to satisfy required elements of proof and where damages are provable. These may be rare, IMO.

It may prove tough to succeed with FCA cases that allege violations of the cyber DFARS and/or failure to satisfy NIST SP 800-171. Where complex rules and requirements are ambiguous, and subject to variable interpretations and fair debate, proving required elements of an FCA violation may be elusive.

About the Presenter

Robert S. Metzger

Bob Metzger, of Rogers Joseph O'Donnell, PC, is recognized for his expertise and leadership in DoD cyber and supply chain security measures. He was a 2016 "Federal 100" awardee, recognized for his "ability to integrate policy, regulation and technology." As a Special Government Employee of DoD, Bob was on the Defense Science Board task force that produced the April 2017 "Cyber Supply Chain Report." He also is a co-author of influential August 2018 MITRE "Deliver Uncompromised" Report and has been a consultant to MITRE on several other projects involving cyber and supply chain security, as well as digital asset crimes, ransomware, and cyber insurance. In the just-released *Chambers and Partners* 2023 ratings, Bob is ranked in "Band 1" for "USA – Nationwide - Government Contracts: Cybersecurity." In his legal practice, Bob advises a wide variety of prominent companies on compliance, cyber and security subjects. He was Counsel of Record for Microsoft in the 2019-2021 "JEDI" bid protest litigation.

ROBERT METZGER
Shareholder
Rogers Joseph O'Donnell PC
rmetzger@rjo.com
https://www.linkedin.com/in/robertmetzger/
202-777-8951