Cybersecurity: How to Successfully Navigate CMMC & the DFARS

Reggie Jones & Kristen Ward Broz

October 5, 2020

Alphabet Soup

FISMA FISMA REFORM NIST 800-53 NIST 800-171 FAR 52.204-21 DFARS 252-204-7012 SSP POA E.O. 13556 CUI CTI CDI DOD Instruction 5200.48 NIST 800-172 APT DOD OUSD(A&S) CMMC Version 1.0 C3PAO CMMC-AB FedRAMP DIB SCC CyberAssist

The Threat

- "It's no secret that the U.S. is at cyber war every day," Ellen Lord, the Undersecretary of Defense for Acquisition and Sustainment, said, as part of a keynote address during the Professional Services Council's 2020 Defense Services Conference. "Cybersecurity risks threaten the defense industrial base, national security, as well as partners and allies."
- “The CMMC,” Lord said, “is the DOD's metric to measure a company's ability to secure its supply chain from cyber threats, protecting both the company and the department.”

https://www.defense.gov/Explore/News/Article/Article/2312512/dod-focuses-on-minimizing-cyber-threats-to-department-contractors/

The Goal

To promote and achieve:

- Penetration-resistant cyber architecture
- Damage limiting operations
- Designs to achieve cyber resiliency and survivability

NIST 800-172 (Draft), Section 1.1, Lines 255-258 (July 2020)

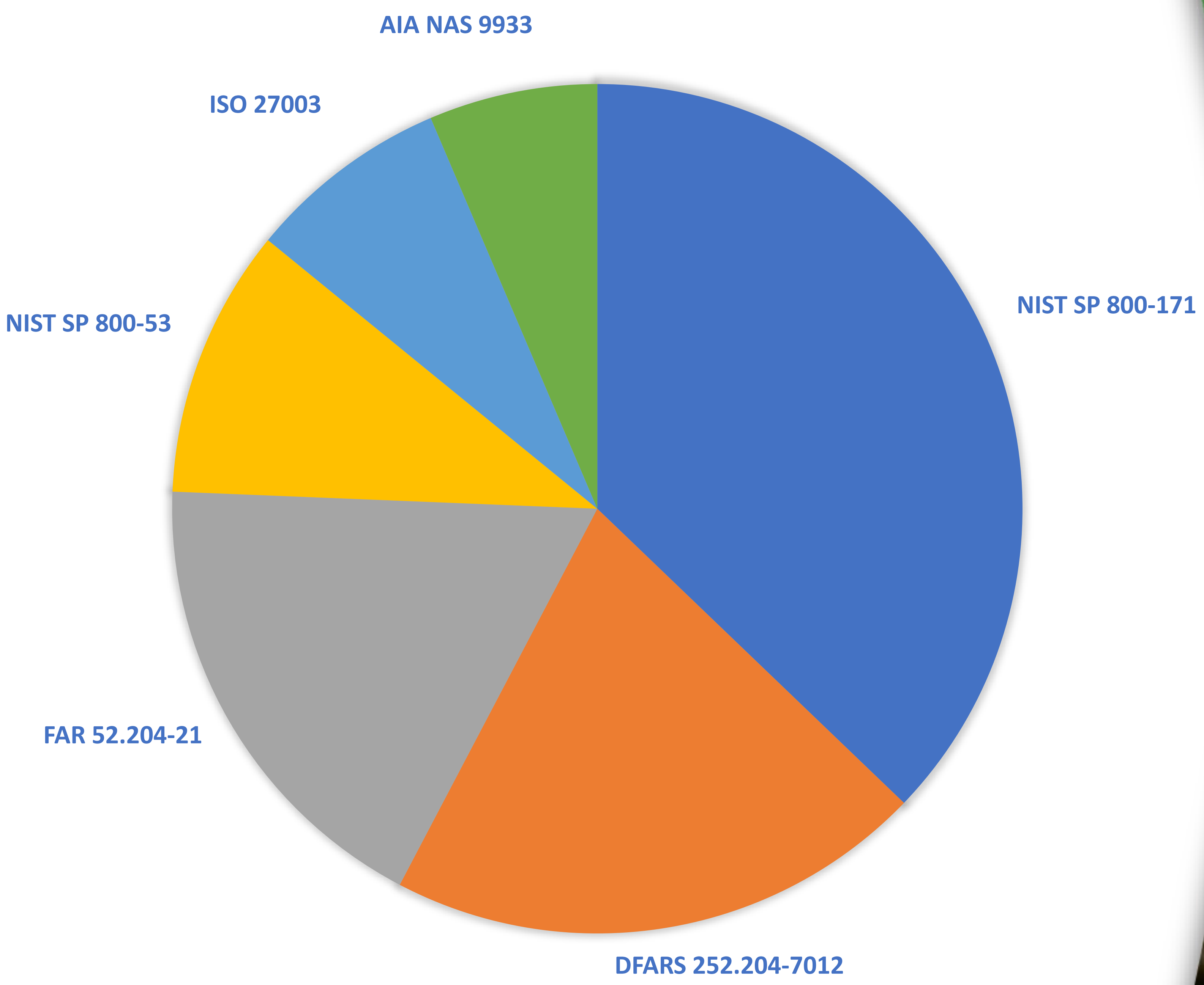
The Path to Achieve the Goal

- FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
- DFARS 252.204.7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)
- DFARS 252.204.7010 (Cloud Computing Services)
- *New Interim Rule:* DFARS clause 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7020, (NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

What Is the Cybersecurity Maturity Model Certification (CMMC)?

- A mandatory third-party certification of DoD contractors and subcontractors’ information systems that is intended to protect sensitive, but unclassified data against cyber threats (CUI).
- Created with federal funding by:
  - Carnegie Mellon University
  - Johns Hopkins University Applied Physics Laboratory, LLC
- First draft version released in September 2019 (Version 0.4)
- Final version released January 30, 2020
- Reassessments/re-certification required every 3 years

COMPONENTS OF CMMC



CMMC-AB & C3PAOs

The CMMC Accreditation Body (CMMC-AB) will train and certify CMMC Third Party Assessment Organizations (C3PAOs) to assess contractors' processes and practices. Based on those assessments, the CMMC-AB will award Level 1 through Level 5 certifications.

- C3PAOs will:
  - Explain certification process
  - Provide training
  - Gather information and report metrics on compliance
  - ***The first 25 Provisional Assessors have been certified; 72 are expected to be certified in total by the end of October 2020***.
- The certification will be documented in the Supplier Performance Risk Assessment (SPRS) at https://www.sprs.csd.disa.mil/

Roll Out: Crawl, Walk, Run

January 2020	CMMC Version 1.0 released
March 2020	CUI Instruction released by DoD outline definitions and handling requirements of CUI
June 2020	CMMC requirements added to certain RFPs
October 2020	CMMC requirements added to certain RFPs as approved by DOD's OUSD for Acquisition & Sustainment
After October 2025	CMMC will apply to all DOD solicitations

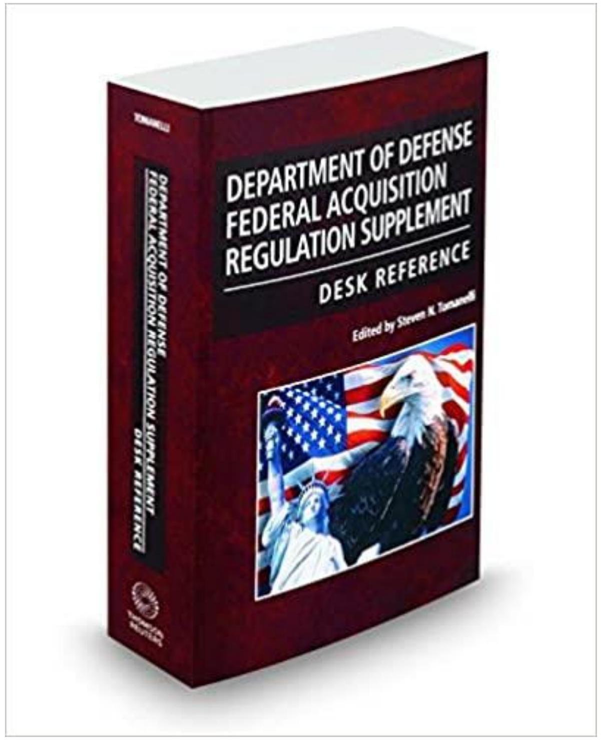
FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

- Only covers ***information systems***, not the information contained on the system (CUI)
  - CUI = Controlled Unclassified Information
- FAR 52.204-21= CMMC Level 1
- First contract clause to meaningfully address cybersecurity information systems across all agencies, not just DOD
- Supposed to reflect actions that any “prudent business person” would use
- Rather basic requirements. No requirements for training, penetration testing, cyber incident reporting or cybersecurity insurance

Fox Rothschild LLP
ATTORNEYS AT LAW

DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)

- Covers ***information*** contained on the system, not just ***information system*** itself.
- Incorporates NIST SP 800-171
- Requires implementation of 110 security requirements on covered contractor information systems; and (***or*** under Interim Rule)
- Document in System Security Plan & Plans of Action those requirements not yet implemented and when they will be implemented



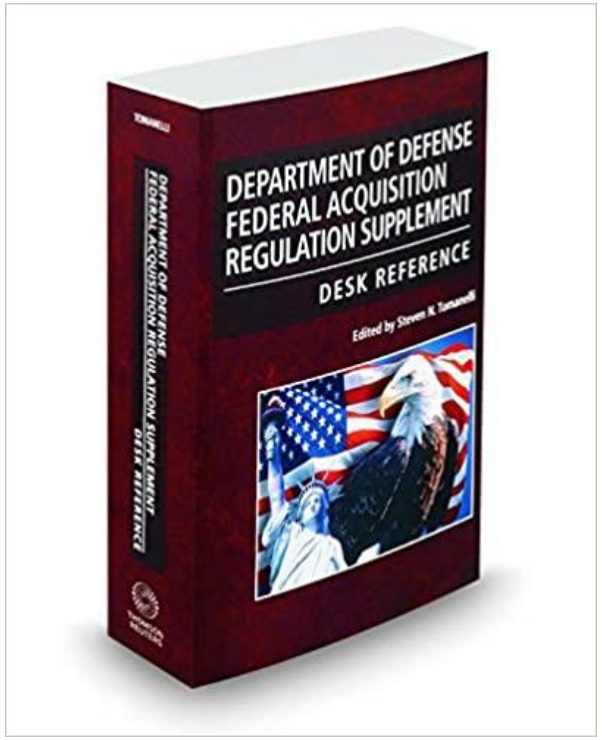
What Role Does the NIST Play?

The National Institute of Standards & Technology (NIST) is responsible for developing information security standards and guidelines, including for federal systems.

- NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)
- NIST SP 800-171 (Protecting Controlled & Unclassified Information in Nonfederal Systems and Organizations)
- **New** - ***NIST SP 800-172 (Enhanced Security Requirements for Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)(July 2020)***

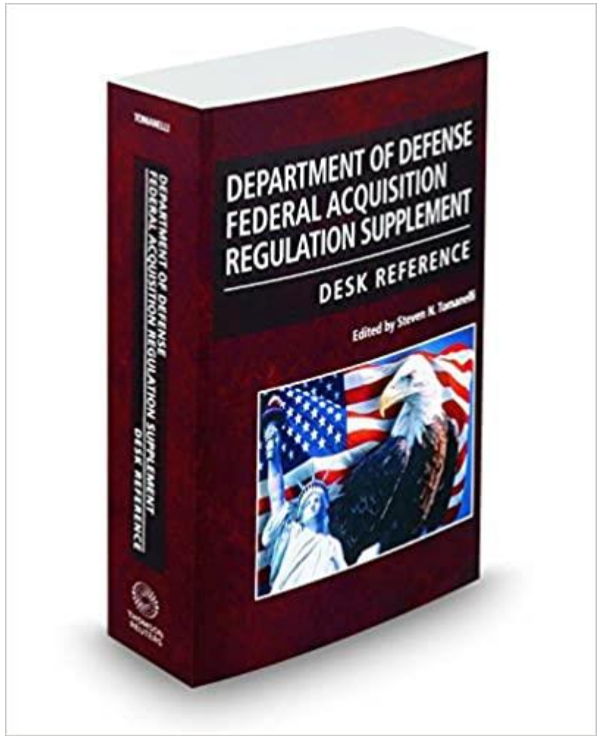
DFARS 252.204-7020 (NIST SP 800-171 DoD Assessment Requirements)

- *New DoD assessment methodology!*
- Requires contractors subject to DFARS 252.204-7012 to self complete a Basic Assessment and upload the resulting score into the Supplier Risk Management System (SPRS) prior to contract award
- Medium and high assessments will be completed by the government
- Transition clause until October 1, 2025



DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

- *New DoD assessment methodology!*
- Requires contractors to maintain the requisite CMMC level for the duration of the contract
- Requires contractors to flow same requirement down to subcontractors in “all subcontracts and other contractual instruments”
  - 7020 Clause for SP 800-171 Assessments
    - “information systems relevant to its offer”
  - 7021 Clause for CMMC Requirements
    - “CMMC level that is appropriate for the information”
- *See 85 Fed. Reg. 61,505 (Sept. 29, 2020)*



How Do Flow-Down Requirements Work in Practice?

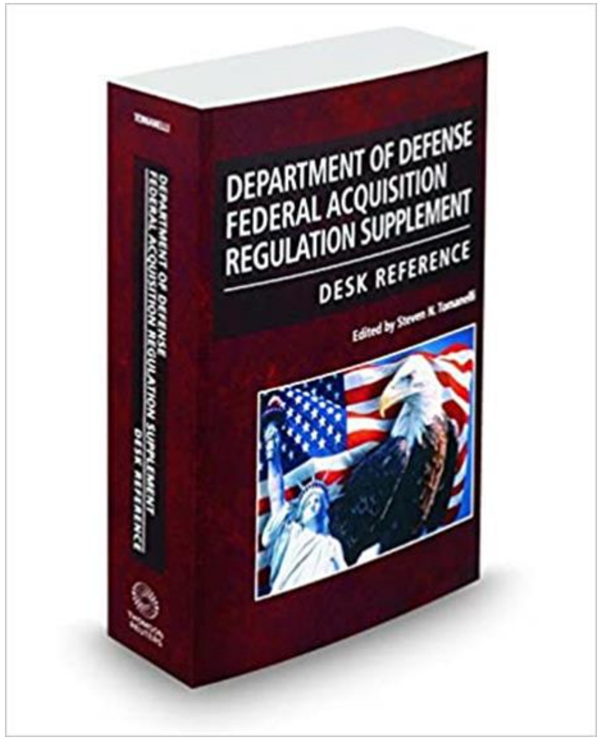
- DFARS – mandatory flow down
- With CMMC, subcontractors not necessarily required to meet same certification level as the prime contractor
  - Required certification depends on data involved
- Third party will determine subcontractor certification
- Other considerations
  - Identifying CMMC levels for subcontractors?
  - How does prime know subcontractor certification levels?
  - Providers on existing programs?

How Do You Meet the DFARS Requirements?

- **Step 1** – What information is covered?

- **Step 2** – What are the cyber incident reporting requirements?

- **Step 3** – Develop a system security plan and a plan of action



Step 1: What Information Is Covered?

- The clause applies to "all ***covered defense information***" (CDI), which is defined as:
- **Unclassifed Controlled Technical Information (CTI)**
  - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html; ***or***
- **Controlled Unclassified Information (CUI)**
  - https://www.archives.gov/cui/registry/category-list
  - Executive Order 13556 defines and calls upon management of CUI

DOD Instruction 5200.48 (March 6, 2020)

- 5.3.a. – “Whenever DOD provides information to contractors, it must identify whether any of the information is CUI via the contracting vehicle … and mark such documents … .”
- 5.3.b. – “Whenever the DOD provides CUI to, or CUI is generated by, non-DOD entities, protective measures and dissemination controls … will be articulated in the contract.”
- Creates a parallel, more detailed DOD CUI registry
- No requirement to remark legacy material unless shared outside of DOD

NIST 800-172 (Enhanced Security Requirements for Protecting CUI) (Draft July 2020)

- Applies to nonfederal systems that process, store or transmit CUI or that provide security protection for such components when the designated CUI is associated with a ***critical program*** or ***high value asset***.
- Examples include: Financial services, providing web and e-mail services to federal agencies, processing security clearances or healthcare data; providing cloud services; and developing communications, satellite and weapons systems).
- To fight the Advanced Persistent Threat (APT)

Step 2: What are the Cyber Incident Reporting Requirements?

- Must “***rapidly report***” cyber incident within “***72 hours of discovery***”
  - Report “whatever information is available”
  - Continuing obligation to disclose new information
  - Must preserve and protect images of all known affected information systems for at least 90 days to allow DOD to request the media
- A cyber incident is defined as: “actions taken through the use of computer networks that result in a compromise or an actual or potential adverse effect on an information system and/or the information residing therein”
- Much faster than the mandatory disclosures required under FAR 52.203-13 (Contractor Code of Business Ethics)
- ***Have agreement with third-party forensic consultant already in place!***

Step 3: Develop a System Security Plan & Plans of Action

System Security Plan (SSP)	Plan of Action (POA)
• Required by NIST SP 800-171 Rev. 1 • Plan company asserts to follow in order to be compliant with regulations • Serves as documentation of company's process for insuring system is protected • NIST creates step by step guide to help create an SSP	• Plan outlining how company intends to better itself over the long run • Anticipates and plans action items to eventually be included in company's practices and overall plan • Mandated by FISMA in order to track and plan resolutions for security weaknesses

So What Is CMMC?

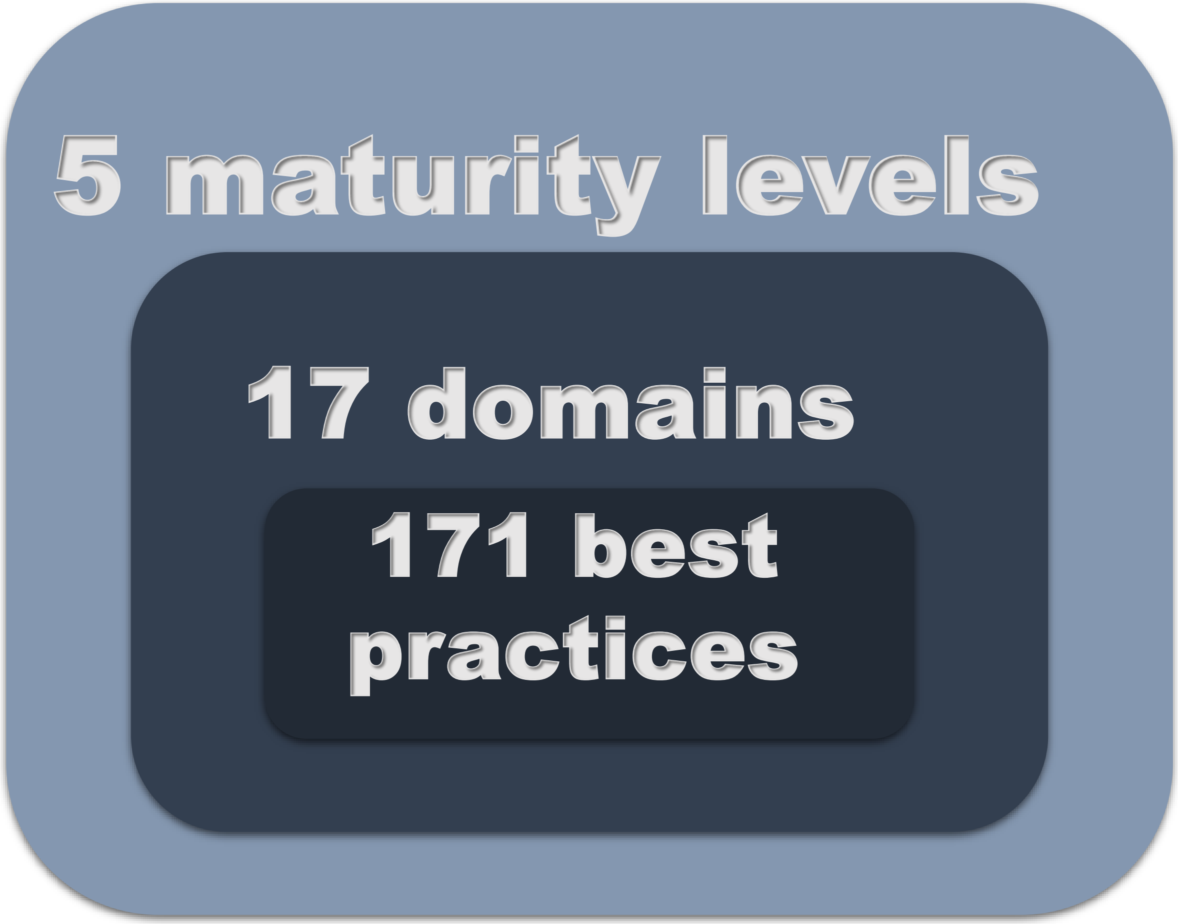
- Need for more consistency from contractors
  - NIST 800-171 requirements were often too rigid, while companies could extend Plan of Action and Milestones (POA&M) to cover gaps indefinitely
  - THIRD PARTY VERIFICATION
- Findings that contractors were non-compliant with NIST SP 800-171
  - “DOD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information.” (Findings in OIG report)
  - Information losses included theft of transport plane and fighter jet data, among other losses
  - FAQs: https://www.acq.osd.mil/cmmc/faq.html

The Basics

- Basic underpinnings of maturity model for Defense Industrial Base (DIB) cybersecurity:
  - Retain all practices from NIST 800-171
  - Method by which DIB members of varying cyber-sophistication can participate without POA&Ms
- Practices go beyond NIST 800-171
- Level 3 example:
  - NIST 800-171 consists of 110 security requirements
  - CMMC adds 20 practices and 2 processes

CMMC Structure

- 5 maturity levels
- 17 domains
- 171 best practices



Five Maturity Levels

- Level 1: Basic Cyber Hygiene
- Level 2: Intermediate Cyber Hygiene
- Level 3: Good Cyber Hygiene
- Level 4: Proactive
- Level 5: Advanced/Progressive

CMMC Version 1.0, supra note 46, at 3–4

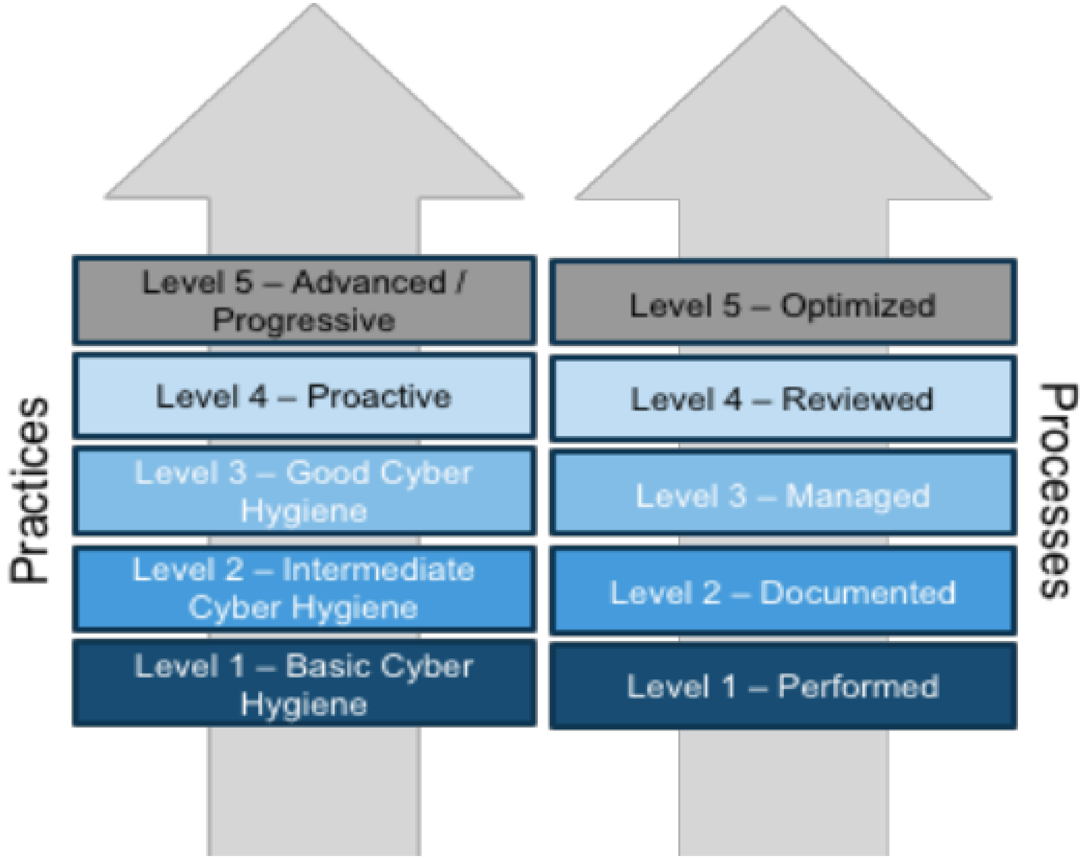
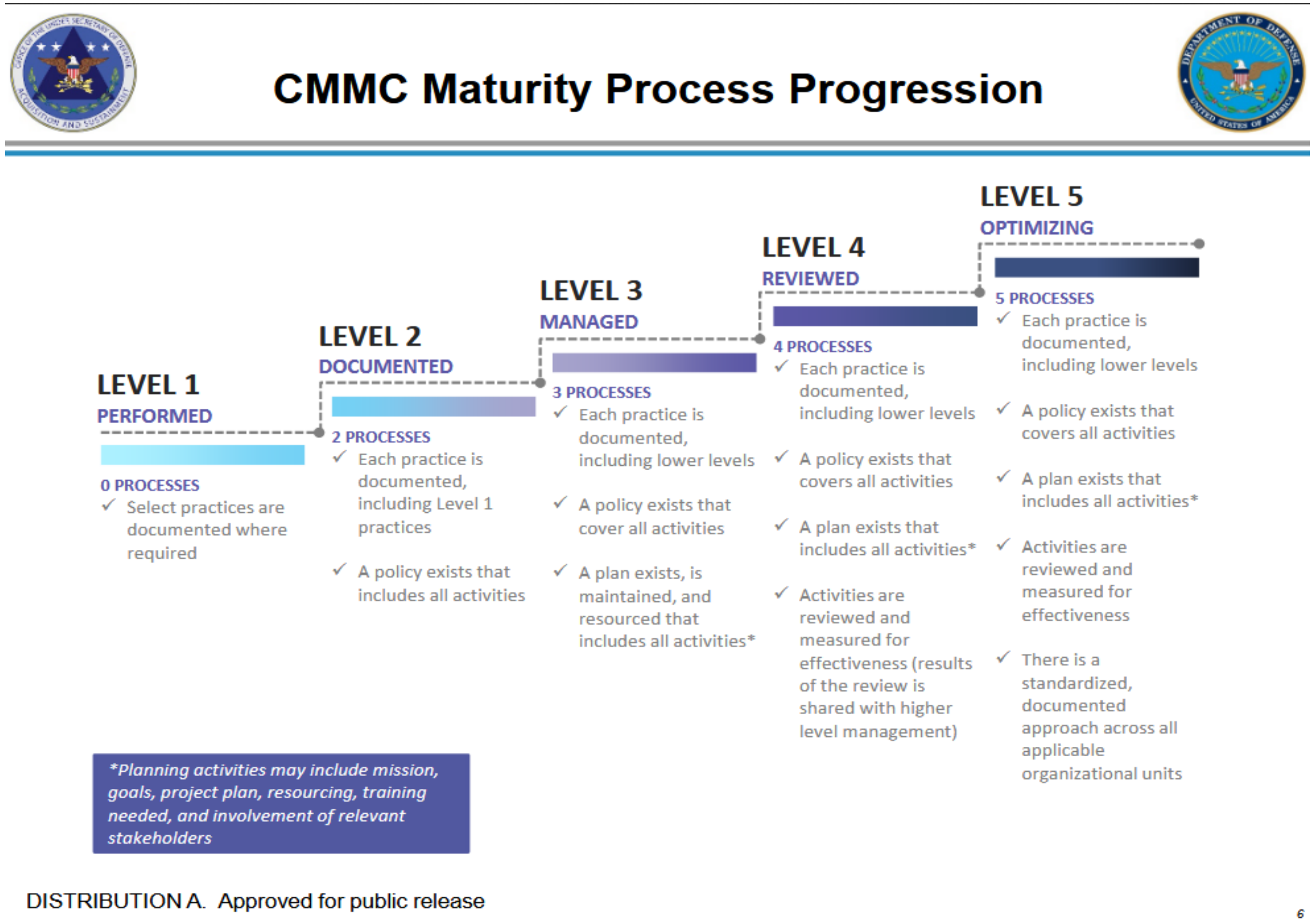


Figure 2. CMMC Level Descriptions

Maturity Process Progression



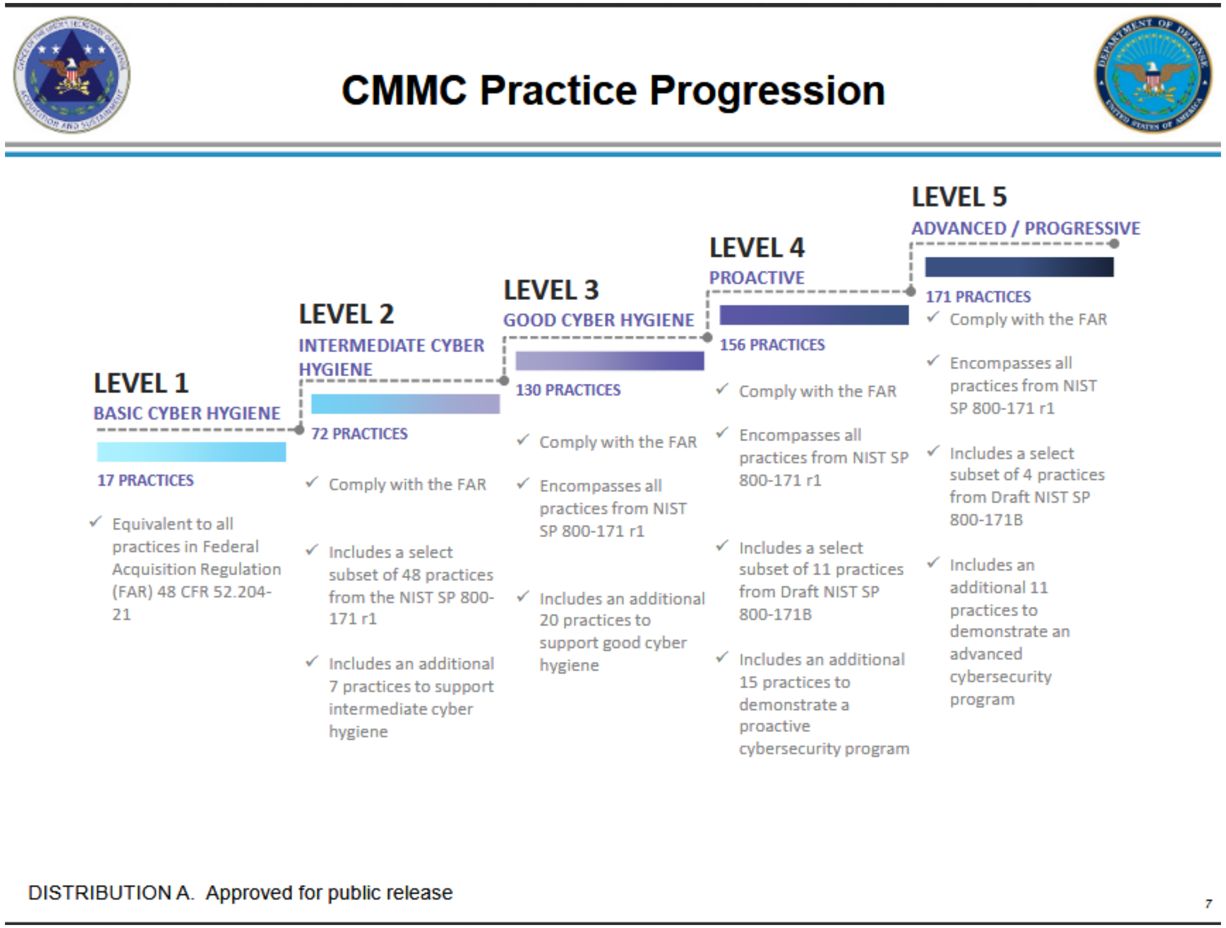
Process Maturity: Extent to which activity is embedded in operations.

- Continued performance
- Consistent, repeatable outcomes

CMMC Version 1.0, supra note 46, at 3–4

Fox Rothschild LLP
ATTORNEYS AT LAW

Practice Progression



Practices performed at each level of the domain

CMMC Version 1.0, supra note 46, at 3–4

Domains

Access Control (AC)	Asset Management (AM)	Audit and Accountability (AA)	Awareness and Training (AT)	Configuration Management (CM)
Identification and Authentication (IDA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)
Physical Protection (PP)	Recovery (RE)	Risk Management (RM)	Security Assessment (SAS)	Situational Awareness (SA)
System and Communications Protections (SCP)	System and Information Integrity (SII)			

What Is the Difference Between Level 1 and Level 3?

- The majority of the practices (110 of 171) originate from the safeguarding requirements and security requirements specified in FAR 52.204-21 and DFARS 252.204-7012, respectively.

  - Level 1 is equivalent to all of the safeguarding requirements from FAR 52.204-21

  - Level 3, building on Levels 1 and 2, includes all of the security requirements in NIST SP 800-171 plus other practices

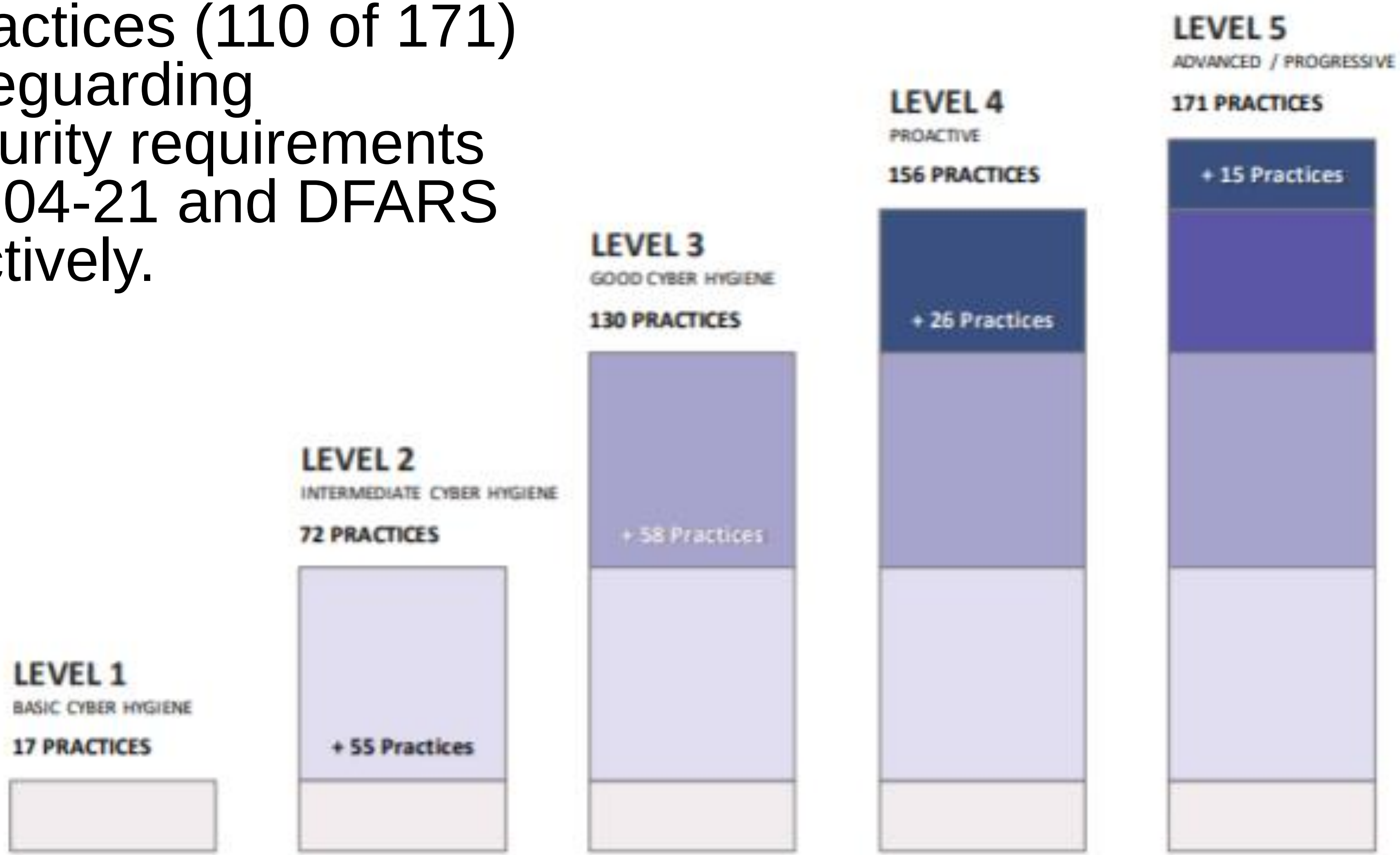


Figure 5. CMMC Practices Per Level

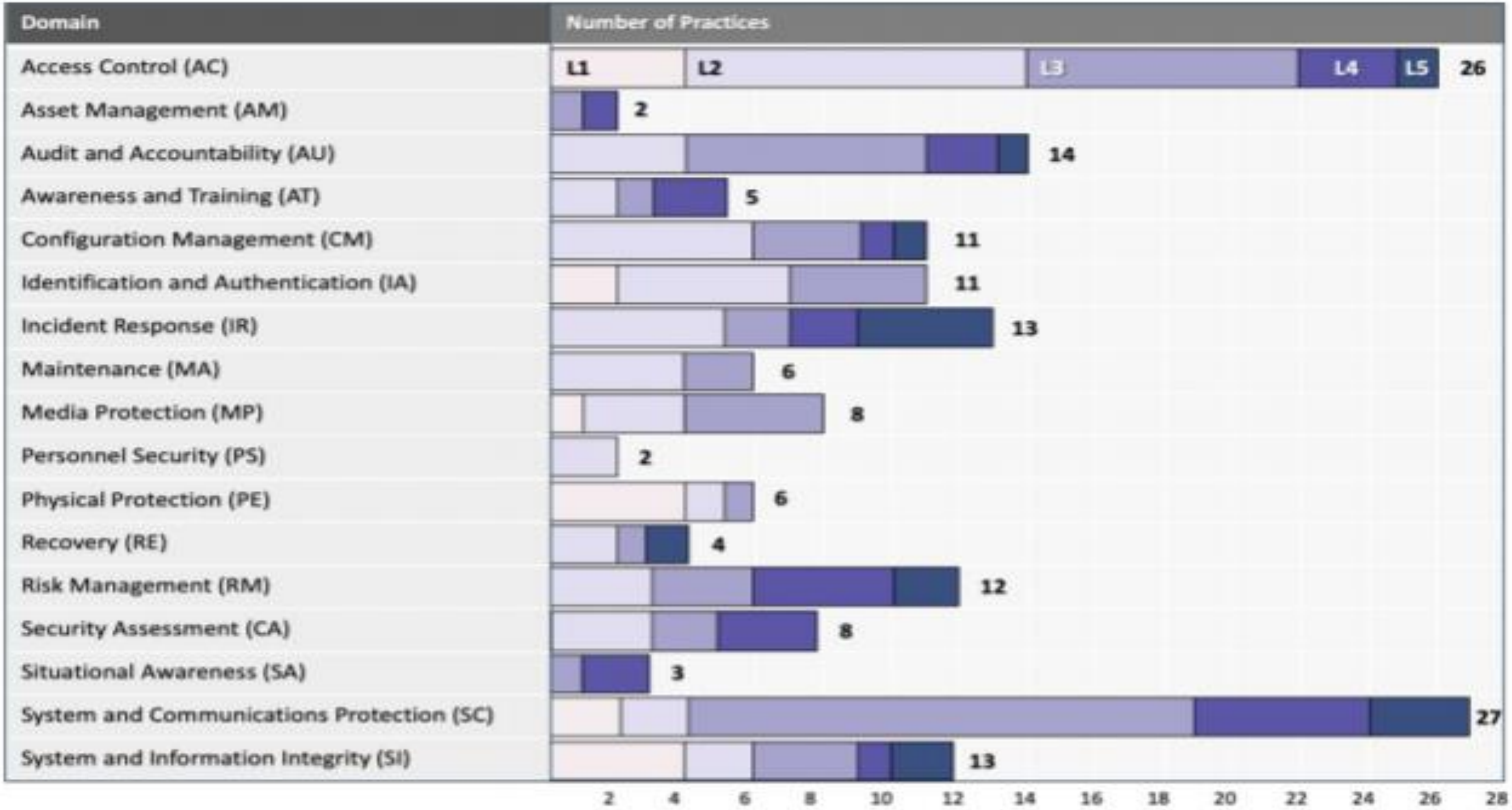


Figure 6. CMMC Practices Across Domains Per Level

Using SSPs and POAs as Tools for CMMC Certification

- Use SSP to organize best practices into your existing system
  - Use domains as a guide to help with organization
  - Can be helpful tool in efficiently delegating duties and cutting down on cost
- “The CMMC framework does not allow a DoD contractor or subcontractor to achieve compliance status through the use of plans of action.”
- But, POAs can help you reach next CMMC level
  - Use as plan to efficiently achieve next certification level
  - Will allow you to make a determination on what you can realistically do

Cybersecurity Maturity Model Certification (CMMC)

Physical Access

1. Limit Physical Access
2. Control Physical Access
3. Maintain Physical Access Log
4. Always Escort and Monitor Visitors

Operations & Maintenance

1. Software Supported by Original Vendor
2. System Configuration Baselines in Place
3. System Configuration Management Performed
4. System Maintenance is Performed
5. Install Anti-Virus Protection
6. Keep Anti-Virus Protection Updated
7. Use Anti-Virus Protection in Real-Time
8. Events are Reported
9. Incidents are Declared
10. Incidents are Resolved
11. System Flaws are Corrected
12. Audit Logs Retained
13. Audit Logs Reviewed
14. Properly Sanitize Media Containing CUI

Based on the 59 pages of DoD's rev 0.4 draft.
This is meant to serve as a guide when understanding the LOE to be compliant with CMMC Level 1.

Documentation & Knowledge Sharing

1. Guidelines in Place
2. Sensitive Data is Identified and Controlled
3. Assets are Tracked
4. Define Security Controls
5. Stay Informed on Cyber Threats
6. Share Cyber Threat Information with Team
7. Cybersecurity Objectives Defined
8. Cybersecurity Objectives Implemented

System Access

1. Identify Authorized Users, Processes and Devices
2. Screen People Before Giving Access to CUI
3. Protect CUI During Personnel Actions
4. Authenticate System Access
5. Limit Unsuccessful Logon Attempts
6. Limit System Access to Authorized Users
7. Limit System Access to Approved Activity
8. Separate Public Facing Systems from Internal Systems
9. Protect Communications at System Boundaries

"Government Contracting is NOT a Secret, it's just a Process." Neil McDonnell

www.GovConChamber.com   www.LinkedIn.com/in/Neil-McDonnell

Certification & Disputes

- Certifications and assessments current for three years
  - Agency may modify
- SP 800-171 Assessments
  - Rebuttal process
- CMMC Certifications
  - Submit dispute adjudication request to CMMC-AB
  - May request additional assessment

DOD's Estimated Cost of Compliance for Small Entities

Level	Certification Costs (Est.)	Total Annual Assessment Costs (Est.)
1	$2,999.56	$1,000.00
2	$22,466.88	$28,050.00
3	$51,095.60	$60,009.00
4	$70,065.04	$371,786.00
5	$110,090.80	$482,874.00

Who Pays for Certification?

Direct Costs	Indirect Overhead Costs
• Cost of actual certification • Likely to be a few thousand dollars • In-practice cost of having someone from the accreditation body certify your business	• Cost of all of the planning, implementation, etc. it will take to become compliant • Likely several thousand dollars, if not more • Can be added to your indirect overhead overtime • Contractors likely to bear most of the burden

DFARS 252.204.7010 (Cloud Computing Services)

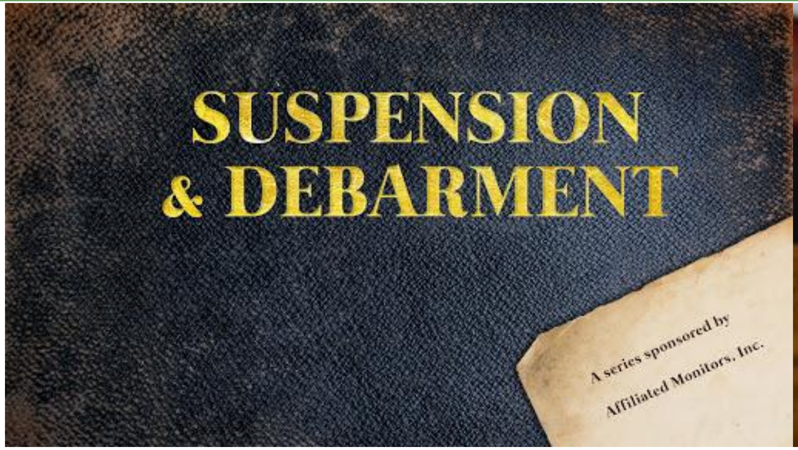
- Cloud Service Providers (CSPs) must:
  - Provide adequate security to safeguard CDI that resides on or is transiting through contractor’s internal information system
  - Report cyber incidents
  - Submit malicious software
  - Submit media to support damage assessment
  - Flow down the clause in subcontracts for operationally critical support
- Any CDI must meet DoD contractor standards

CMMC vs. FedRAMP

- CMMC requirements for cloud providers with DoD contracts
  - Incident reporting requirements will remain
  - Subcontractor flow-down will remain
- Reciprocity between CMMC and FedRAMP
  - <u>**But**</u>, will have to close POA&Ms and adjudicate POA&Ms to get CMMC
  - Even those with FedRAMP high approval will need to close gaps with the accreditation body
  - Reconciling CMMC and FedRAMP likely to revolve around type of information, rational comparison of FedRAMP “low, med, high” to CMMC levels 1-5
- At least CMMC level 1 for CSPs

What Are Potential Consequences of Noncompliance?

- False Claims Act
- Suspension
- Debarment
- CPARS evaluations
- Soft consequences
  - Less likely to be awarded a contract if not compliant



Reggie Jones
rjones@foxrothschild.com
202.461.3111

Kristen Ward Broz
kbroz@foxrothschild.com
202.794.1220

Fox Rothschild LLP
ATTORNEYS AT LAW

When to Conduct Internal Investigations and How to Avoid False Claims Act Violations

Doug Hibshman & Brian Stolarz

October 5, 2020

Panelists and Practice Groups

- **Doug Hibshman, Partner**
  - Federal Government Contracts and Procurement; Privacy & Data Security; White-Collar Criminal Defense & Regulatory Compliance

- **Brian Stolarz, Partner**
  - White-Collar Criminal Defense & Regulatory Compliance

  - **Federal Government Contracts and Procurement and White-Collar Criminal Defense & Regulatory Compliance**
    - Represent small, medium, and large contractors, subcontractors, suppliers, owners, sureties, developers in all varieties of federal contracting matters
    - Represent contractors, subcontractors, owners, sureties, developers in disputes between each other related to federal or state procurements
    - Represent contractors in defending against allegations of fraud, the False Claims Act, and other violations of federal or state law

Presentation Outline

- **When to conduct internal investigations**
  - How do internal investigations arise?
  - When are internal investigations required?
  - What are the benefits of internal investigations?
  - How to conduct internal investigations?
- **The False Claims Act**
  - What is the False Claims Act and how is it used by the government?
  - False Claims Act damages
  - False Claims Act recent trends
  - Best practices for avoiding False Claims Act allegations

When to Conduct Internal Investigations

Fox Rothschild LLP
ATTORNEYS AT LAW

How Do Internal Investigations Arise?

- Caused by allegations/belief of wrongdoing or noncompliance
  - (1) Contractor discovers potential violation
  - (2) Procuring agency alleges contract noncompliance
  - (3) Whistleblower allegation
  - (4) A Civil Investigative Demand or subpoena is issued to contractor
  - (5) Search warrant is executed
- In that moment, contractor faces a critical decision as to whether to conduct an internal investigation and the scope
- “Bet the company” decision
- Follow pre-existing, standard internal investigation protocol to effectively gather information and minimize risk

When Are Internal Investigations Required?

- Clients routinely ask why they have to conduct internal investigations – concerns over cost and business disruption
- Two main reasons why they should be conducted:
  - **It’s required by law!**
  - **It’s good business!**

When Are Internal Investigations Required? (Cont’d)

- **Required by Law**
  - FAR 52.203-13 (Contractor Code of Business Ethics and Conduct) requires contractors to:
    - Have a Code of Business Ethics and Conduct, Compliance Program and Internal Control System
    - Establish standards and procedures “to facilitate timely discovery of improper conduct” in connection with Government contracts
    - Ensure “corrective measures are promptly instituted” and carried out
    - Timely disclosure, in writing, to the agency OIG (copy to the Contracting Officer)
      - In connection with the award, performance, or closeout of any Government contract
      - The Contractor has “credible evidence” that a principal, employee, agent, or subcontractor
      - Has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violation of the civil False Claims Act (31 U.S.C. 3729-3733)
  - FAR 52.203-13 applies to contracts/subcontracts over $5.5 million/120 days

When Are Internal Investigations Required? (Cont'd)

- **Required by Law**
  - What is "credible evidence" and why self-disclose?
    - Not defined in FAR
    - "More likely true than not true that a violation occurred"
    - Use common sense
    - Never self-disclose without investigation
    - Never self-disclose or not self-disclose without legal guidance
  - Is it better to disclose or not disclose?

What Are the Benefits of Internal Investigations?

- **It's Good Business**
  - Determine who, what, when, where and why
  - Prevent future violations
  - Shape corporate behavior and improve processes
  - Weed out violators
  - Get the government off your back – exonerate and keep it local
  - Mitigate sanctions on contractor and employees
    - Limit civil False Claims Act penalties
    - Obtain "cooperation credit" from DOJ in criminal cases – Yates Memo
    - Limit criminal sanctions under the Federal Sentencing Guidelines

How to Conduct Internal Investigations

- Have a plan and a standard protocol
  - No one-size-fits-all – no required format
  - Preserve data, review documents and interview witnesses
  - Notify employees
  - Be quick
  - Answer the ultimate question(s)
  - Anticipate the “why” questions
- Conduct under supervision of legal counsel
  - In-house or external counsel
  - Must be independent – who is the client?
  - Upjohn Warning
  - Protection of attorney–client privilege
  - Advisory opinion protection

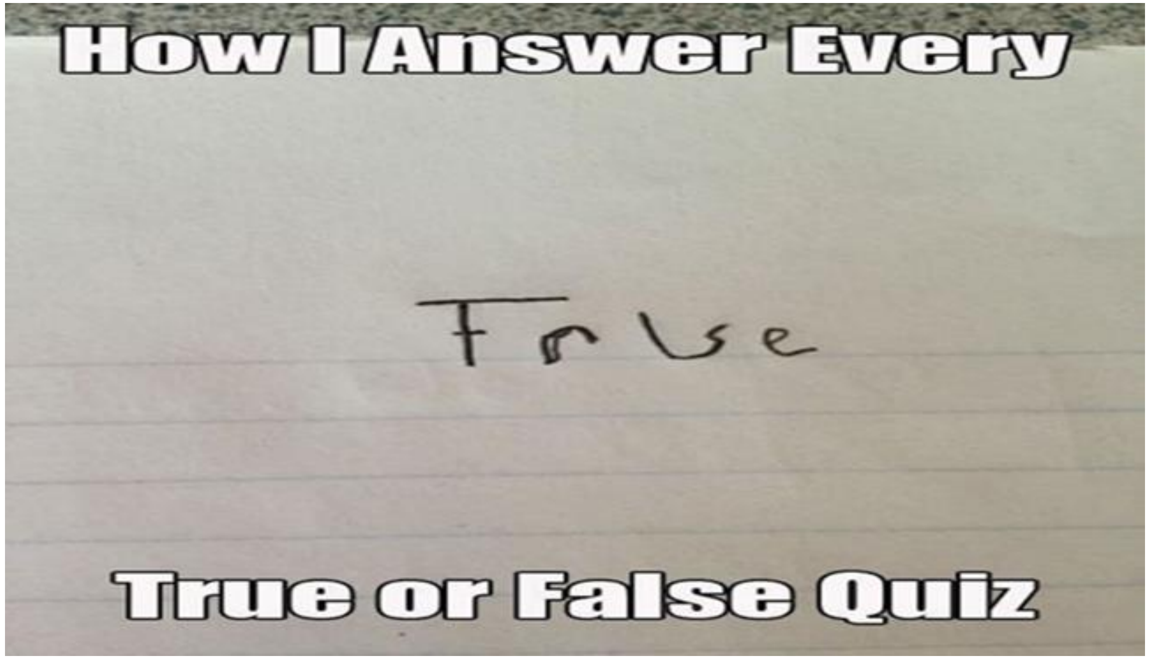
How to Conduct Internal Investigations (Cont’d)

- Prepare written investigation report
  - Pros and cons of written report
  - Memorialize findings and recommendations – give an answer
  - Independent and honest
  - Tool for analyzing options and next steps
- Determine whether you have to self-disclose
  - Report is foundation for self-disclosure – sword and a shield
  - Disclose strategically and emphasis the good
  - Focus on the lowest level possible

Internal Investigation Best Practices

- Be organized
- Take it seriously – understand what is at stake
- Be thorough – memorialize your findings
- Be prompt
- Protect data and privilege
- Seek assistance when needed

The False Claims Act



The False Claims Act

- **These are “bet the company” issues!**
  - **United Tech. settles with Army for $1 million**
    - United Tech. falsely certified authenticity of counterfeit parts. Had to divest of business arm as part of settlement. Criminal charges against employees
  - **General Dynamics settles with Navy for $4 million**
    - Billed Govt for defective parts. Former employees reported
  - **Northrop settles with NRO for $325 million**
    - Failed to properly test and certify (heterojunction bipolar transmitters) over 10 years for satellites. Qui tam suit from Ph.D. teaming partner
  - **Parts Supplier Debarred due to counterfeit parts**
    - Govt got substitute/counterfeit parts – office raided – criminal charges against employees – debarment for 3 years

What Is the False Claims Act?

Civil False Claims Act - 31 U.S.C. §§ 3729 *et seq.*

- Key government anti-fraud weapon – criminal and civil
- Prohibits submitting false documents or information to government
- Violations of False Claims Act lead to severe penalties
  - Suspension/debarment/contract termination
  - Civil penalties for 2020 are a minimum of **$11,463** and a maximum of **$23,331** *per false claim*
  - Treble damages even if the government is not harmed
- Criminal penalties include fines, sanctions, and incarceration
- Government can bring claims for up to 10 years

False Claims Act Statistics

- In 2019, DOJ recovered over $3 billion from False Claims Act cases, with total recoveries since the Act was amended in 1986 of more than $62 billion
- 633 *qui tam* actions were filed in 2019, an average of <u>12 new cases each week</u>
- Majority of cases are in health care industry – the construction and defense industries accounted for $250 million in 2019, and are growing sources of false claims prosecutions

What Is a False Claim?

- **Elements of a False Claim**
  - A “Claim” is any request for money or property submitted to government
    - Multiple requests = multiple false claims
    - Payment apps, proposals, small business certifications, etc.
  - Claim must be submitted “knowingly” to government, but not really
    - Know it is false
    - Act in deliberate ignorance of truth/falsity – could be false
    - Act in reckless disregard of truth/falsity – probably false

What Is a False Claim? (Cont’d)

- Three types of False Claims:
  - **Direct False Claim**
    - Knowingly presenting or causing to be presented a false claim
  - **False Statement**
    - Knowingly making, using or causing to be made or used a false record / statement material
  - **Reverse False Claim**
    - Knowingly concealing or decreasing an obligation to pay money to Government

False Claims Act – Damages

- “Benefit of the Bargain” damages – even if government received what it paid for, if there was a false claim the government can still seek penalties in cases with minimal losses.
    - *Morse Diesel Int’l v. U.S.,* 79 Fed. Cl. 116 (2007)
    - $467,000 claim led to $7 million in penalties
    - Penalties are for the harm caused to the specific government program.
- Application of the Presumed Loss Rule – damages are total amount of contract awarded regardless of what government receives.

False Claims Act – Source of Claims

- **Contracting Officer**
  - What must CO do if false contract claim is suspected?
    - FAR 33.209 – If contractor is unable to support any part of a claim, assumed to be false and must be reported to agency's fraud unit

- ***Qui Tam* Relator (Private Citizen Plaintiff)**
  - Whistleblower Action
  - Competitor
  - Disgruntled former employee
  - Prime contractor, subcontractor
  - Auditor
  - John or Jane Doe

False Claims Act – Origins

- ***Qui Tam* Relators**
  - Primary originators of False Claims Act cases
  - Statute amended to protect whistleblowers from retaliation
  - Very significant financial incentive
    - **<u>15 to 30% </u>** of the amount recovered by the government if it“intervenes” or takes over the case. Government intervenes in 1/5 cases.
    - If the government does not intervene, the relator will receive **<u>25 to 30% </u>** of the recovery
  - Millions of dollars to individuals
  - Cottage industry of law firms who take on these cases

False Claims Act – Examples

- Any false information submitted to the government for the purposes of claiming or leading to a payment – not for negligent statements or plain old breach of contract
  - False invoices
  - False contract claims
  - False certifications, to include small business certifications
  - Concealed rebates, credits, or overpayments
  - Illegitimately front-loaded invoices
  - Inflated material/personnel/equipment costs
  - Substituted non-conforming materials – i.e., Buy American Act
  - Concealed defective/non-conforming work
  - False testing reports

Civil False Claims Act – Recent Trends

- *Universal Health Services v. Escobar*, 136 S.Ct. 1989 (2016).
  - Supreme Court held that a misrepresentation in a False Claims Act case must be “material” to the government’s payment decision, and declared it to be a “rigorous” and demanding standard.
  - “*[n]ot every undisclosed violation of an express condition of payment automatically triggers liability*,” and the False Claims Act is not a “*vehicle for punishing garden-variety breaches of contract or regulatory investigations*.”
  - As a result of *Escobar*, **$1 billion of judgments** in False Claims Act suits were **reversed**.

Civil False Claims Act – Recent Trends (Cont’d)

- The DOJ issued the Granston Memo – directs government lawyers to consider dismissing meritless *qui tam* suits over a relator’s objection
- The DOJ has “an important gatekeeper role in protecting the FCA”
- Since 2018, DOJ has dismissed two dozen cases

False Claims Act – Recent Trends

- Cooperation credit –
  - An entity or individual that seeks to earn maximum credit in a False Claims Act matter generally should undertake a **<u>timely self-disclosure</u>** that includes identifying all individuals substantially involved in or responsible for the misconduct, **<u>provide full cooperation with the government's investigation</u>**, and take **<u>remedial steps</u>** designed to prevent and detect similar wrongdoing in the future.
- Credit will take the form of a reduction in the damages multiplier and civil penalties, as well as informing relevant agencies of a companies' cooperation in connection with administrative remedies.

“Best Practices” to Avoid False Claims Act Allegations

- Know the rules
- Educate your team – routine training
- Perception is reality
- Ask for permission first, not forgiveness later
- Good faith counts for a lot
- Keep records, keep records, keep records
- **USE COMMON SENSE!!!**

What to Do if You Suspect a False Claim?

- **<u>Report</u>** up the chain
  - Contact compliance officer
  - Call ethics hotline
- **<u>Investigate – Consult Counsel</u>**
  - Was a statement made? Was it a claim?
  - Was it a mistake?
  - Was it false?
  - Were your employees involved?
- **<u>Report</u>** to OIG if “credible evidence” of fraud exists
  - Report remedial steps implemented to avoid issues in the future

Doug Hibshman
202.461.3113
dhibshman@foxrothschild.com

Brian Stolarz
202.794.1224
bstolarz@foxrothschild.com


Fox Rothschild LLP
ATTORNEYS AT LAW

Bid Protests at the GAO and COFC: Strategic Planning to Optimize Litigation Success

Nicholas Solosky

October 5, 2020

Bid Protests: Why Litigate?

- **Improper** or even **unlawful** flaws in a solicitation or contract award decision
- The overwhelming number of bid protests:
  - Government Accountability Office (**GAO**)
  - Court of Federal Claims (**COFC**)
- There are proven strategies for litigating in both forums
- Don’t forget agency level protests

Bid Protests: Why Litigate? (Cont'd)

The Bid Protest Decision

- Cost-benefit analysis
- Enhanced debriefing
  - Dept. of Defense only (for now)
  - Opportunity to submit Q&A – agency must respond
  - Information gathering = enhanced decision making

Three Common Bid Protests

- **Pre-Bid Protests**
  - Solicitations by agencies for bids or proposals for proposed contracts that include incorrect, overly restrictive or other problematic information
- **Pre-Award Protests**
  - Erroneous exclusion from the competitive range
- **Post-Award Protests**
  - Erroneous awards or proposed awards of federal contracts

Bid Protests at the GAO

- The GAO is the **most common** venue for bid protests
- GAO bid protests serve two **primary purposes**:
  - To resolve solicitation defects prior to bid opening
  - To challenge procurement errors in connection with the award or proposed award of federal contracts
- Outcome: **Corrective Action**, **Agency Report** and/or **Written Decision**

Protest Timing at the GAO

- **Pre-Bid Standard**: File before the time set for receipt of initial proposals
- **Post-Award Standard:** To challenge the award or proposed award of a contract:
  - Within 10 days of when the protester knew or should have known of the basis for the protest
  - Impact of required debriefing

Stay of Contract Award

- **Competition in Contracting Act (CICA) Stay**: Automatic stay of contract award or performance
- **Pre-Bid Protests**: Mere act of filing the protest
  - But beware missing the deadline to submit an offer
- **Pre- or Post-Award Protests**:
  - File within **10 days** of award; or
  - **5 days** after required debriefing

GAO Bid Protest Timeline

- **100 Day Target:** Protest, agency report, protester comments and written decision
- **Outcomes:**
  - Early intervention corrective action by the agency
  - GAO decision sustaining the protest (corrective action vs. outright award)
  - Attorneys' fees (costs of filing and pursuing protest) available
  - Dismissed or denied

GAO Bid Protest Aftermath

- **100 Day Target:** Protest, agency report, decision
- **Requesting reconsideration**:
  - Must file the request within 10 days after learning the basis for reconsideration
  - Bar for reconsideration is high
- **Disappointed protester may “appeal” the GAO decision**
  - Assert the GAO’s decision was arbitrary, capricious, and an abuse of discretion at the COFC

GAO Statistics

Enclosure II
Bid Protest Statistics for Fiscal Years 2015-2019

	FY2019	FY2018	FY2017	FY2016	FY2015
Cases Filed[1]	2198 (down 16%)[2]	2607 (less than 1% increase)[3]	2596 (down 7%)	2789 (up 6%)	2639 (up 3%)
Cases Closed[4]	2200	2642	2672	2734	2647
Merit (Sustain + Deny) Decisions	587	622	581	616	587
Number of Sustains	77	92	99	139	68
Sustain Rate	13%	15%	17%	23%	12%
Effectiveness Rate[5]	44%	44%	47%	46%	45%
ADR[6] (cases used)	40	86	81	69	103
ADR Success Rate[7]	90%	77%	90%	84%	70%
Hearings[8]	2% (21 cases)	0.51% (5 cases)	1.70% (17 cases)	2.51% (27 cases)	3.10% (31 cases)

https://www.gao.gov/assets/710/702551.pdf

Fox Rothschild LLP
ATTORNEYS AT LAW

Bid Protests at the COFC

- Filed, prosecuted and resolved more like **traditional Federal Court litigation**
  - Importance of the administrative record
- **Protest timing:** COFC has a six-year statute of limitations
  - No unreasonable delay
- N**o automatic stay** of contract award or performance
  - Temporary Restraining Order (TRO) and Preliminary Injunction

COFC Decision and Aftermath

- COFC bid protests generally take about five to six months to resolve
  - o Compare with GAO’s 100 day timeline
- Cross-motions for judgment on the administrative record
- Declaratory and injunctive relief
- Automatic right of appeal if COFC denies the protest
  - Contractor must file appeal to the Federal Circuit within 60 days after COFC enters final judgment on the protest

Comparing and Contrasting GAO and the COFC

GAO

- Relatively informal proceedings
- Efficient, with a decision typically issued within 100 days
- Less access to discovery
- 44% effectiveness rate in 2019
- Mandatory CICA Stay for timely protests
- Typically less expensive than COFC

COFC

- More formal proceedings
- No set timeline for decisions
- More in-depth discovery, including the Administrative Record
- Legally binding decisions
- No mandatory CICA stay
- Typically more expensive to litigate

Pros and Cons of Protest Litigation Forums

- **GAO:** Clear solicitation errors and self-evident agency errors
  - Fast and efficient
  - Automatic stay
  - Less risk of reliance on agency discretion
- **COFC:** Complex legal/factual issues
  - Administrative record is the key
- **Ultimate Wildcard**: CICA Stay

Bid Protests With Limited Jurisdiction

- **IDIQ Task Orders**
  - GAO alone has jurisdiction of task and delivery order protests in excess of $25M (DoD, NASA, Coast Guard), or in excess of $10M for civilian agencies
- The COFC may not hear protests of IDIQ task orders
  - **FASA**: Bars COFC jurisdiction over protests “in connection with the issuance or proposed issuance of a task or delivery order”
  - <u>SRA Int’l, Inc. v. United States</u>, 766 F.3d 1409 (Fed. Cir. 2014): held the COFC did not have jurisdiction to hear a protest related to the issuance of a task order even where the protester alleged the GSA violated federal regulations by waiving an organizational conflict of interest.
  - **Exception:** protester alleges order is outside of the IDIQ’s scope

Bid Protests With Limited Jurisdiction (Cont’d)

Other Transaction Authority (OTA) Contracts

- COFC does not have jurisdiction under the Tucker Act
  - <u>Space Expl. Techs. Corp. v. United States</u>, 144 Fed. Cl. 433 (2019): COFC dismissed protest of an OTA procurement based on lack of subject matter jurisdiction because OTAs are not “procurement” contracts

- GAO will consider them in limited instances- pre-award protests alleging the agency is improperly using its OTA authority
  - <u>Blade Strategies, LLC,</u> B-416752 (Sept. 24, 2018): Dismissed protest challenging the award of an Army OTA contract because the protester challenged the Army’s use of OTA authority **after** receipt of initial proposals

Bid Protests with Limited Jurisdiction (Cont’d)

Suspension and debarment: Directly relates to agency “responsibility” determination

- GAO generally will not review suspension or debarment protests, claiming the contracting agency is the appropriate forum
  - <u>Matter of: Aria Target Logistics Servs.</u>, B-409055.2 (Feb. 27, 2014): Dismissed protest brought by a contractor who was excluded from the competitive range because it was on a list for proposed debarment
- COFC claims jurisdiction over suspension and debarment decisions that preclude the protester from contract award

Matter of: Blue Origin Fla., LLC, GAO (Nov. 18, 2019)

- GAO sustained a protest alleging that the Air Force improperly *combined* offers – rather than using the required best value trade-off process.
- Air Force planned to award contracts to the 2 offerors who "when combined" represented the best value to the government
  - Then, the Air Force would do further evaluation of the pair, with the better getting 60% of the work, and the other 40%

Fox Rothschild LLP
ATTORNEYS AT LAW

Matter of: Blue Origin Fla., LLC, GAO (Nov. 18, 2019) (Cont'd)

- Protester argued the "when combined" best value method was ambiguous
- GAO concluded the Air Force's basis for award did not provide "an intelligible and common basis" for competition
  - Not clear to offerors how they could intelligently compete
  - GAO supported its decision with FAR 3.301(a) (policy against collusive bidding) and FAR 3.303(c)(1) (filing joint bids can violate antitrust laws)

<u>PAE-Parsons Glob. Logistics Servs., LLC v. United States,</u> COFC (2019)

- Case of first impression: Whether the COFC has jurisdiction over a protest challenging the Army's rating of a contractor that resulted in the contractor losing *both* the IDIQ contract *and* a related task order
- The government opposed the protest, arguing the COFC lacked jurisdiction over protests of IDIQ task orders

PAE-Parsons Glob. Logistics Servs., LLC v. United States, COFC (2019)

- The COFC sided with the protester, concluding this was not a task order protest
  - Held this was a challenge to the underlying technical evaluations of the underlying IDIQ contracts
  - The Army ranked offerors in descending priority for each IDIQ contract, which in turn, directly impacted the task order for which a contractor could become eligible
- The COFC held the task order awards were “inextricably linked” to the ratings for the IDIQ contracts

Nicholas Solosky
202.696.1460

nsolosky@foxrothschild.com