ACC Association of Corporate Counsel HOUSTON

WOMBLE BOND DICKINSON

Handling Data, IP rights, and Cybersecurity Requirements Under Government Contracts

April 27, 2021

Gary Campbell, Womble Bond Dickinson
Gary Machetta, KBR
Jon Mellis, VMWare

Agenda

1. Protecting Intellectual Property (IP)
   a. Government IP Rights Framework
   b. Marking and delivering technology
2. Information Security Requirements
   a. Cybersecurity Background
   b. CMMC Overview
   c. What contractors should be doing now
   d. Prohibitions of acquisitions from certain companies

Patents

Copyrights

Trademarks

Trade Secrets

Protecting Intellectual Property

Basic Framework

- Set forth in Federal Acquisition Regulation (FAR) 48 CFR Part 27 and Defense FAR Supplement (DFARS) 48 CFR Part 227
  - Patent Rights
  - Rights in Technical Data and Computer Software
  - Rule of Thumb - Government's rights depend on when the item was developed and who paid for it

Government IP Rights Framework

	Patents	Software	Technical Data
Potential license grant:	FAR 52.227-11 FAR 52.227-13	FAR 52.227-19 DFARS 252.227-7014	FAR 52.227-14 DFARS 252.227-7013 DFARS 252.227-7015
Limited Rights			✖
Restricted Rights		✖	
Government Purpose rights		✖	✖
Unlimited Rights	✖	✖	✖
Specially Negotiated License Rights		✖	✖

Practice Tip: 4 Steps to Preserve Your IP

Step 1: Determine what rights the government might obtain

Step 2: Submit a properly marked proposal identifying restrictions

Step 3: Negotiate the contract or subcontract

Step 4: Control delivery of the technology

Step 1: Determine what rights the Government might obtain

Checklist:

- What is being delivered?
- When/where was it developed? Who paid for it?
- What agency am I dealing with?
- What regulations apply (FAR, DFARS)?
- Does my product qualify as a commercial item?

Nature of Government's Patent Right

- A Contractor's Patent Rights are Governed by Part 27 of the Federal Acquisition Regulation (Title 48 of the CFR) and the Patent Rights Clause (FAR 52.227-11), which implements the Bayh-Dole Act
- Contractor retains title
  - Some narrow exceptions to right to retain title, See FAR 27.302(b)(1)-(4)
- Government gets a nonexclusive, irrevocable, paid-up license to practice or have practiced on its behalf such an invention throughout the world
- In What?
  - "Subject Inventions"
  - "Subject Invention" (FAR 27.301): any invention of the contractor made in the performance of work under a Government contract
  - "Made" (FAR 27.301): means the conception or first actual reduction to practice of the invention
- March-in rights

Technical Data and Computer Software Rights (FAR 52.227-14)

- FAR 52.227-14 sets the paradigm
- Unlimited Rights (Government funding)
  - means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so
  - Government shall have unlimited rights in "data **delivered** under this contract unless provided otherwise for limited rights data or restricted computer software"
- Limited Rights (technical data) (private funding)
  - Data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government
  - Limited Rights Data means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications

Technical Data and Computer Software Rights (FAR 52.227-14)

- Restricted Rights (software) (private funding)
  - means the rights of the Government in restricted computer software
- Specially Negotiated License Rights (case by base basis)
- Must Examine FAR and DFARS, slight differences
- Government Purpose Rights (mixed funding)

Practice Tip: 4 Steps to Preserve Your IP

Step 1: Determine what rights the government might obtain

Step 2: Submit a properly marked proposal identifying restrictions

Step 3: Negotiate the contract or subcontract

Step 4: Control delivery of the technology

Step 2: Submit a Properly Marked Proposal

- Provide a proposal cover page restriction (FAR 52.215-1)
  - Restricts data which should not be disclosed or used for any purpose other than proposal evaluation
  - This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction.
- Mark each sheet containing proprietary data with a legend
  - Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.
- Include an assertion of technical data to be delivered with less than unlimited rights - DFARS 252.227-7017

Assertion of IP Rights

Technical Data or Computer Software to be Furnished with Restrictions	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
Apple Watch 5 Technical Data	Developed 100% at Private Expense	Limited Rights	Tim Cook
Apple Watch 5 Firmware	Developed 100% at Private Expense	Restricted Rights	Tim Cook

Practice Tip: 4 Steps to Preserve Your IP

Step 1: Determine what rights the government might obtain

Step 2: Submit a properly marked proposal identifying restrictions

Step 3: Negotiate the contract or subcontract

Step 4: Control delivery of the technology

Step 3: Negotiate the Contract

2 Ways to Preserve IP

1. Negotiate contract language for modified clauses or limited licenses
2. Negotiate what is being delivered
   - Deliver form, fit and function data instead of proprietary technical data
   - CLINs (end products)
   - Contract Data Requirements Lists (CDRLs)

Practice Tip: 4 Steps to Preserve Your IP

Step 1: Determine what rights the government might obtain

Step 2: Submit a properly marked proposal identifying restrictions

Step 3: Negotiate the contract or subcontract

Step 4: Control delivery of the technology

Step 4: Control Delivery of the Technology

- Mark the deliverables properly
  - ***Data received without a restrictive legend is furnished with unlimited rights!***
- Correct any marking errors or omissions promptly
  - 60 days to correct errors
  - 6 months to correct omissions

Cybersecurity Requirements

DoD Cybersecurity Background

- DFARS cybersecurity clause in effect since 2013
  - DFARS 252.204-7012
  - Definitions and standards have evolved over time
- NIST SP 800-171 incorporated as of 12/31/2017
  - Protection of Controlled Unclassified Information (CUI)
  - Implement 110 security requirements on covered contractor IS
  - Document in a System Security Plan (SSP) and Plan of Action and Milestones (POAM) requirements not yet implemented
- Self-verification
  - DCMA verification of subcontractor flow down
  - Limited DoD verification of contractor compliance, generally rely on contractor agreement to DFARS Cyber clause

DoD Cybersecurity Background

- DoD determination that current government contractor Cybersecurity approach is not sufficiently effective
- Malicious cyber actors successfully targeting Defense Industrial Base ("DIB") and DoD Supply Chain
- Aggregate loss of intellectual property and sensitive unclassified information undercutting U.S. technical advantages and endangering national security
- Inconsistent contractor compliance
  - Many subcontractors unaware and/or non-compliant with DoD cybersecurity requirements

DFARS 252.204-7020

- DoD Assessment Requirements
  - Assess implementation of cybersecurity requirements
  - Determines how well a contractor has implemented NIST SP 800-171 controls
    - Basic – Self Assessment
    - Medium – DoD Assessment
    - High – DoD Assessment
  - Depends on criticality of the program or information
  - Allows for rebuttal and adjudications
  - Scores posted in Supplier Performance Risk System (SPRS)

Cybersecurity Maturity Model Certification (CMMC) – current version 1.2

- Combines various NIST and other standards into a unified cyber security standard
- 5 maturity levels from basic cybersecurity hygiene (Level1) to highly robust (Level 5)
- Must demonstrate both the process and practice maturity identified at the requisite level across 17 capability domains
- DoD RFPs will assign a minimum CMMC certification level based upon the nature and amount of government information to be handled by contractors / subcontractors
  - Level 1 or 2 – likely no CUI
  - Level 3 – Default
  - Levels 4 and 5 - intended to reduce the risk from Advanced Persistent Threats (APTs)
  - Industry concern that Level 4/5 will become default for DoD RFPs

CMMC (*cont'd*)

- Paradigm shift - independent third-party auditor assessment vs. DFARS self-certification
  - Cost to contractors not yet determined
  - Certification cost will be "allowable"
  - Duration of certification not yet determined
  - DCMA or other DoD entity may perform some higher level assessments
- Broad application
  - DoD only initially
  - DoD estimates 300,000 companies will seek CMMC certification
  - Likely to expand beyond DoD eventually
  - Applies to subcontractors
  - No commercial item or COTS exemption

CMMC Implementation Schedule

- Phased implementation over 5 years
- Implementation will not be “across the board” – begin with selected RFIs and RFPs
  - Test Requests for Information (RFIs) with CMMC certification requirements are anticipated to issue in FY 2021
  - Test Requests for Proposals (RFPs) with CMMC certification requirements were anticipated to issue in FY 2021
  - All DoD contracts by 2026
- CMMC is not retroactive, will not apply to previously-awarded contracts

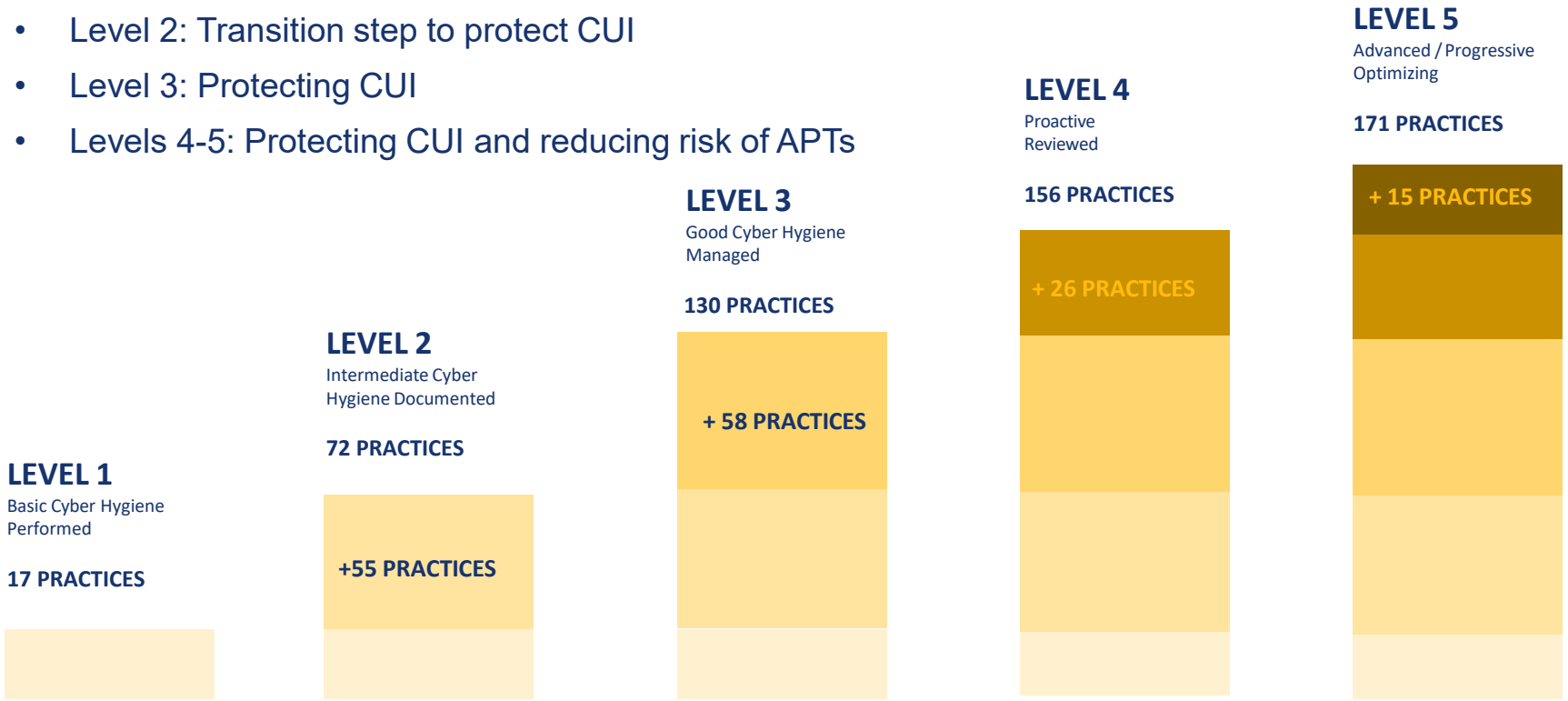
CMMC Model Level Descriptions

	Description of Practices	Description of Processes
Level 1	• Basic cybersecurity • Achievable for small companies • Subset of universally accepted common practices • Limited resistance against data exfiltration • Limited resilience against malicious actions	• Practices are performed, at least in an ad-hoc matter
Level 2	• Inclusive of universally accepted cyber security best practices • Resilient against unskilled threat actors • Minor resistance against data exfiltration • Minor resilience against malicious actions	• Practices are documented
Level 3	• Coverage of all NIST SP 800-171 rev 1 controls • Additional practices beyond the scope of CUI protection • Resilient against moderately skilled threat actors • Moderate resistance against data exfiltration • Moderate resilience against malicious actions • Comprehensive knowledge of cyber assets	• Processes are maintained and followed
Level 4	• Advanced and sophisticated cybersecurity practices • Resilient against advanced threat actors • Defensive responses approach machine speed • Increased resistance against and detection of data exfiltration • Complete and continuous knowledge of cyber assets	• Processes are periodically reviewed, properly resourced, and improved across the enterprise
Level 5	• Highly advanced cybersecurity practices • Reserved for the most critical systems • Resilient against the most-advanced threat actors • Defensive responses performed at machine speed • Machine performed analytics and defensive actions • Resistant against, and detection of, data exfiltration • Autonomous knowledge of cyber assets	• Continuous improvement across the enterprise

CMMC Practices Per Level

Levels align with the following focus:

- Level 1: Basic safeguarding of FCI
- Level 2: Transition step to protect CUI
- Level 3: Protecting CUI
- Levels 4-5: Protecting CUI and reducing risk of APTs



What Contractors Should Be Doing (*cont'd*)

- CMMC
  - Begin assessing your controls now using draft Version 1.02
  - Identify which requirements you currently meet and where gaps exist at Levels 1-5
  - Plot a course to close existing gaps as soon as reasonably possible
  - Track compliance costs
  - Identify and communicate with subcontractors who will need to be CMMC-certified to support your DoD prime contracts
  - Plan to flow down and collect appropriate CMMC contract commitments from subcontractors
- Resource: https://www.acq.osd.mil/cmmc/faq.html

Chinese and Russian Prohibitions

- FAR 52.204-23 - Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
- FAR 52.204-25- Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Huawei Rule)
  - Part A – Contractors cannot supply these products to the U.S. Government
  - Part B – As of 9/13/2020, Government cannot do business with companies who use these products
- Huawei, ZTE, Hytera, Hangzhou Hikvision, or Dahua
- What Contractors need to do:
  - Screen supply chain for prohibited vendors (Huawei, ZTE, Kaspersky)
  - Flow down clauses to applicable subcontractors and suppliers
  - Policies and procedures
  - May want representations from suppliers

Contact Information

- Gary Campbell – Gary.Campbell@wbd-us.com
- Gary Machetta – Gary.Machetta@kbr.com
- Jon Mellis – Jmellis@vmware.com

WOMBLE
BOND
DICKINSON