BDO

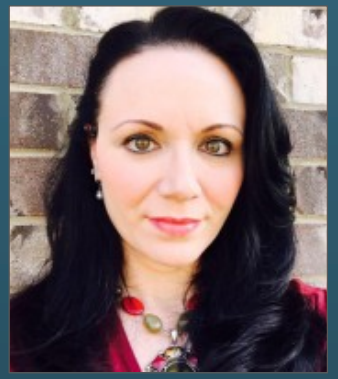
pillsbury

CMMC–New Cybersecurity Rules Will Change the Way DoD Contractors Do Business

Brian P. Cruz | Counsel
Pillsbury Winthrop Shaw Pittman LLP
brian.cruz@pillsburylaw.com
213.488.7101

Meghan D. Doherty | Senior Associate
Pillsbury Winthrop Shaw Pittman LLP
meghan.doherty@pillsburylaw.com
703.770.7519

Christina Reynolds | Director
C|HFI, C|EH, C|NDA
BDO Industry Specialty Services Group
creynolds@bdo.com
703-893-0600



BDO pillsbury

Cybersecurity in Three Acts

- The Rules
  - Cyber Security Standard established in DFARS 252.204-7012
  - Established December 31, 2017
- The Reality
  - New DFARS rules require self-assessments and reporting to DoD
  - Contract awards contingent on reporting of primes and subs
- The Future
  - CMMC – Third-party audits to certify compliance
  - Still in implementation phase

BDO pillsbury

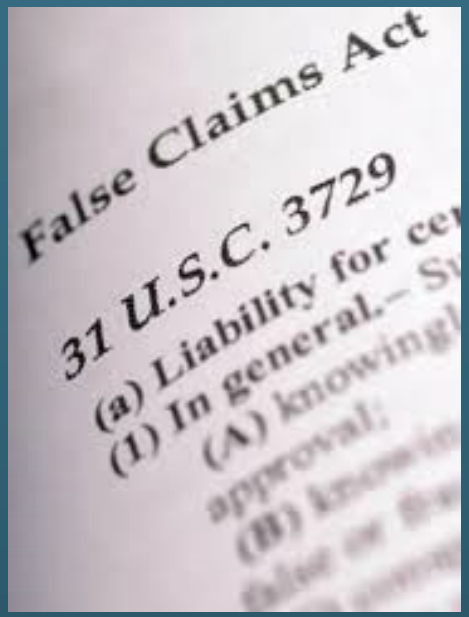
What Changes for Contractors

- Prime contractors will need to evaluate their support structures based upon the data provided by subcontractors
- Supply chain management must include evaluation of cyber security
  - Supply chain choices will be data driven, *i.e.* who has or gets CUI
  - What cyber scores are reported in SPRS
- Contract awards will be contingent upon cyber security compliance
  - Near term, based upon Assessment scores
  - After CMMC implementation, based upon certification level of prime contractor and subcontractors

BDO pillsbury

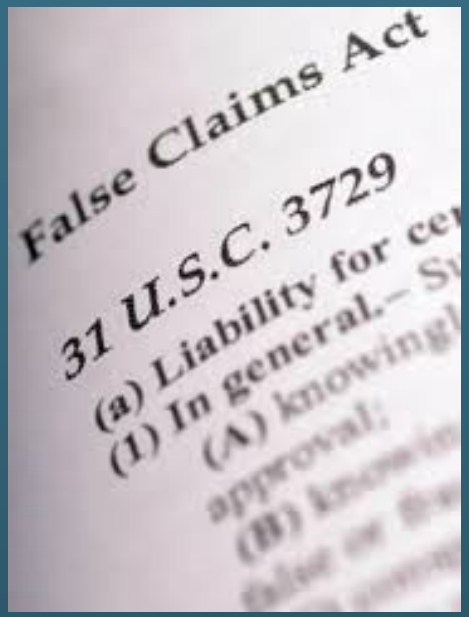
FCA Liability for Failure to Comply with -7012 Clause

- *Markus v. Aerojet Rocketdyne Holdings, Inc.*, 2:15-cv-2245 WBS AC
  - Court held that qui tam relator pleaded sufficient facts to establish that the contractor misrepresented its compliance with the cybersecurity requirements to fraudulently obtain contracts with NASA and DoD
  - The FCA claim survived SMJ because relator plausibly pleaded that defendant's alleged failure to disclose fully its noncompliance was material to the government's decision to enter into and pay on the relevant contracts



FCA Liability for Cybersecurity Flaws

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



Assessments

- Implications of reporting self-assessments
  - FCA liability for a self-Assessment that is improperly conducted or reported
  - Potential liability for the credibility of subcontractors' self-reported Assessments
- Implications of government performed assessments
  - Interim Rule allows contractors 14 days to submit additional information
  - No further information on challenging government assessment

pillsbury

You are Here….

Brian P. Cruz
213.488.7101
brian.cruz@pillsburylaw.com

pillsbury

Meghan D. Doherty
703.770.7519
meghan.doherty@pillsburylaw.com

pillsbury

BDO pillsbury

Start Here: Basic Cyber Hygiene
FAR Cause: FAR 52.204-21

- FAR 52.204–21, “Basic Safeguarding of Covered Contractor Information Systems,”
  - Requires application of basic safeguarding requirements when processing, storing, or transmitting Federal Contract Information (FCI) in or from covered contractor information systems
  - 15 Controls (they cross-map to 15 of the NIST 800-171 controls)
  - Implements what the DoD refers to as “Basic cyber hygiene”

BDO pillsbury

The Rule
DFARS 252.204-7012

- DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is required in all contracts except for contracts solely for the acquisition of COTS items
- Requires defense contractors to provide “adequate security” for covered defense information which “at a minimum” requires contractors to implement 110 Security controls from NIST SP 800-171
- In addition, the contractor should include the clause in subcontracts for which performance will involve covered defense information or operationally critical support
- DFARS Clause 252.204-7012 requires contractors/subcontractors to:
  - Safeguard covered defense information (both in transmission and at rest)
  - Report cyber incidents within 72 hours of discovery
  - Report malicious software
  - Facilitate damage assessment

BDO pillsbury

The Reality
Self-Attestation of Compliance

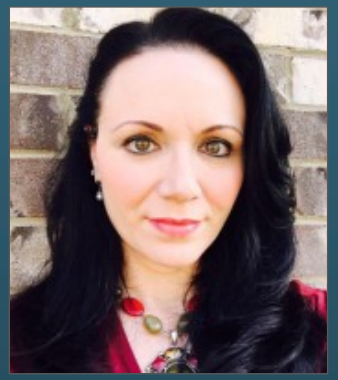
- DFARS 252.204-7008 Compliance With Safeguarding Covered Defense Information Controls is required in every solicitation, except for those solely for the acquisition of commercially available off-the-shelf (COTS) items
- The offeror represents that:

  "By submission of this offer, the offeror represents that it will implement the security requirements specified by [NIST SP 800-171] that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017. "

- DoD had interpreted "implementation" of NIST SP 800-171 as having a completed SSP and a PoA&M for the relevant covered contractor information systems.

BDO pillsbury

Into the Woods…



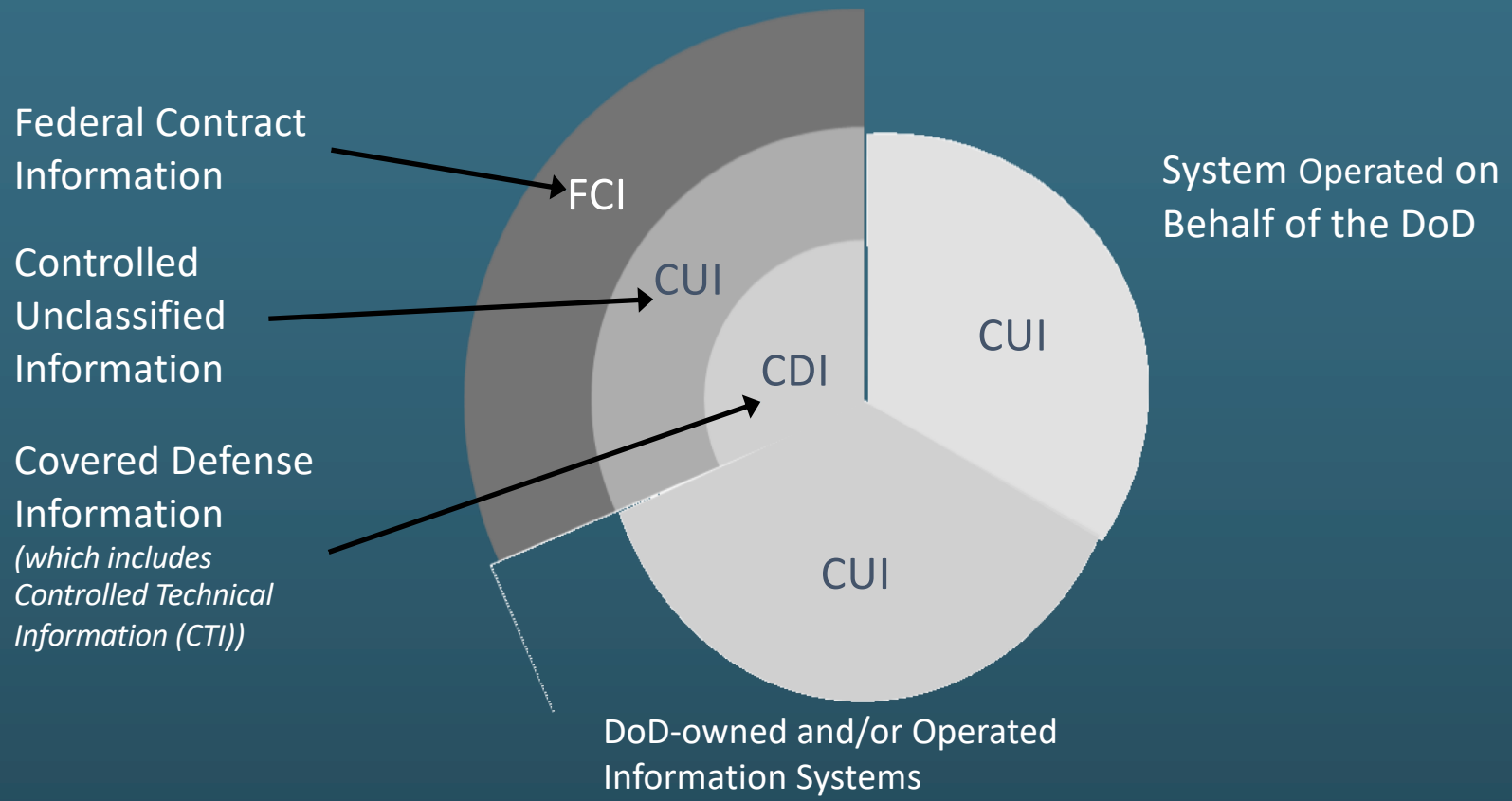
Christina Reynolds| Director
C|HFI, C|EH, C|NDA
BDO Industry Specialty Services Group
+703-893-0600
creynolds@bdo.com

BDO

BDO pillsbury

Information Being Targeted

Contractor's Internal System



Graphic adapted from https://www.acd.osd.mil/dpap/pdi/p2p%20training%20presentations/Cybersecurity%20Initiatives%20Requirements.pdf

BDO pillsbury

The “Fork” of FCI and CUI

- The DFARS 7012 clause does not currently require verification of contractors’ implementation of NIST SP 800-171 prior to contract award.
- BOTH FCI and CUI may be
  1. Provided to the contractor by the Government OR
  2. Developed by the contractor in performance of work under the contract.
- Many contractors erroneously believe that because they do not receive data from the Government marked as CUI, that they claim not to have processed any CUI on-site.
- This may not be true as CUI could be produced on the contractor’s site within normal performance of work products under the contract.
- Consult your Contract Officer for clarification on CUI

BDO pillsbury

Interim DFARS Rule

DFARS Case D041

- Issued September 29, 2020; effective November 30, 2020
- Three new DFARS clauses: DFARS 252.204-7019, 7020, and 7021
- Interim rules provides implementation of two assessment components:
  - NIST SP 800-171 DOD Self-Assessment with an immediate requirement for contractors to upload to SPRS database, and
  - The Cybersecurity Maturity Model Certification (CMMC) framework that will be rolled out over the next five years.
- DOD will require all contractors to post assessment results to the SPRS system to validate compliance with NIST SP 800-171, starting on November 30, 2020.

BDO pillsbury

New DFARS Clauses Issued

- DFARS 252.204-7019, *Notice of NIST SP 800-171 DOD Assessment Requirements*
  - Amends DFARS 7012 by requiring KOs to verify offeror has current NIST 800-171 Assessment on record
  - Summary-level assessment scores (from -311 to +110) must be uploaded to SPRS
  - Assessments may not be more than 3 years old, entered per CAGE code
- DFARS 252.204-7020, *NIST SP 800-171, DOD Assessment Requirements*
  - Provides DOD NIST SP 800-171 Assessment Methodology, formerly used during DIBCAC assessments, based on NIST 800-171 controls and a scoring range of -311 to +110
  - Basic, Medium, High level assessments
- DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification (CMMC) Level Requirements*
  - Cybersecurity Maturity Model Certification Requirements
  - Prescribed for use in solicitations and contracts, including FAR part 12 procedures for the acquisition of commercial items (exl. COTS)

BDO pillsbury

Scoring for NIST 800-171 Assessments

- To be eligible for awards on or after November 30, a contractor must complete the first level called a *Basic Assessment*.
- If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements.
- For each security requirement not met, the associated value is ***subtracted*** from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.
- Certain requirements have more impact on the security of the network and its data than others.
- This scoring methodology incorporates this concept by weighting each security requirement based on the impact to the information system and the DoD CUI created on or transiting through that system, when that requirement is not implemented.

BDO pillsbury

SPRS: Weighted Security Controls

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

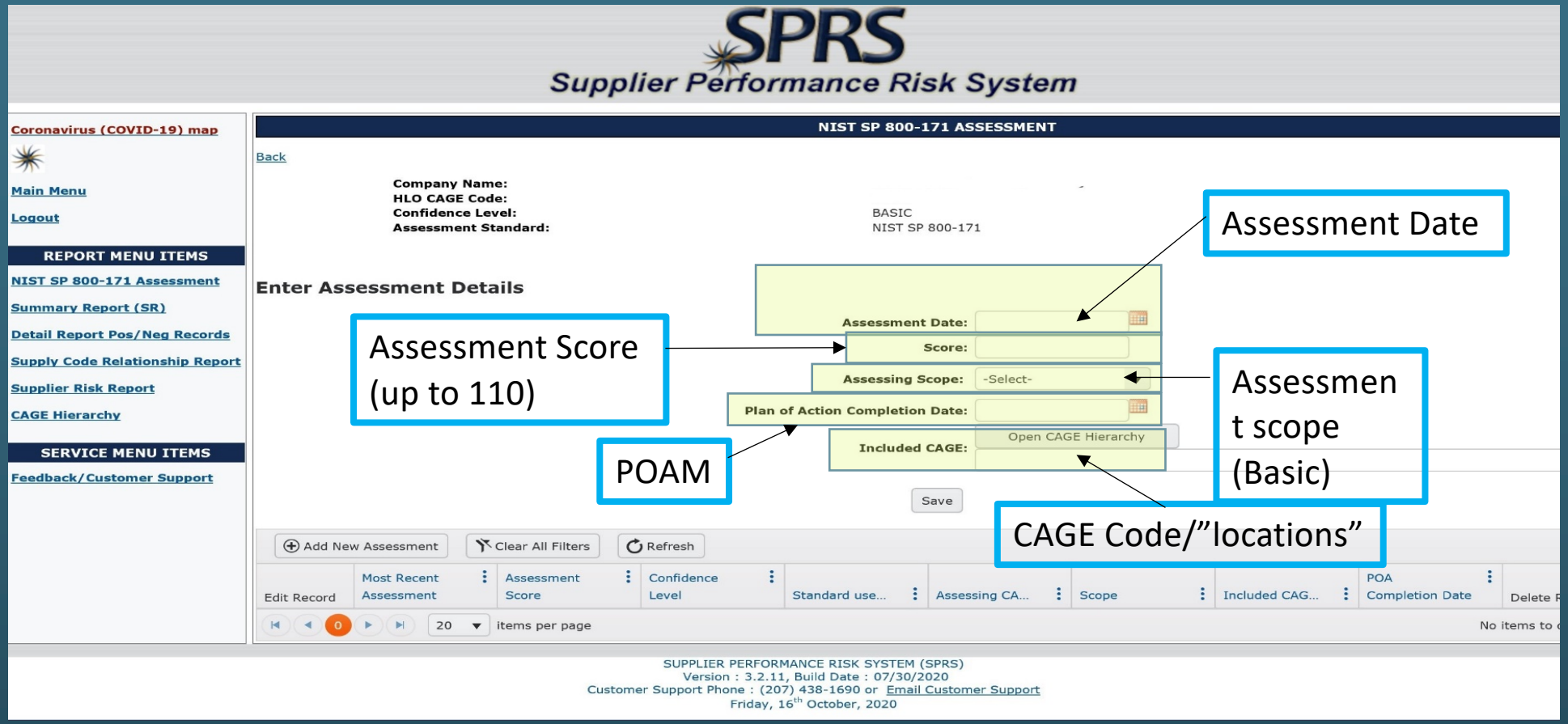
The cost of unimplemented security controls:

"Significant Exploitation of the Network"		"Specific and confined effect"	
-5 points	-5 points	-3 points	-3 points
Basic Security Requirements: 3.1.1, 3.1.2, 3.2.1, 3.2.2, 3.3.1, 3.4.1, 3.4.2, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.7.2, 3.8.3, 3.9.2, 3.10.1, 3.10.2, 3.12.1, 3.12.3, 3.13.1, 3.13.2, 3.14.1, 3.14.2, and 3.14.3.	Derived Security Requirements: 3.1.12, 3.1.13, 3.1.16, 3.1.17, 3.1.18, 3.3.5, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.5.10, 3.7.5, 3.8.7, 3.11.2, 3.13.5, 3.13.6, 3.13.15, 3.14.4, and 3.14.6.	Basic Security Requirements 3.3.2, 3.7.1, 3.8.1, 3.8.2, 3.9.1, 3.11.1, and 3.12.2.	Derived Security Requirements 3.1.5, 3.1.19, 3.7.4, 3.8.8, 3.13.8, 3.14.5, and 3.14.7.

- 1 point is subtracted from the score of 110 for all remaining unimplemented Derived Security Requirements that have a limited or indirect effect on the security of the network and its data.
- +1 point per control for each security control, if fully implemented for a maximum of 110.

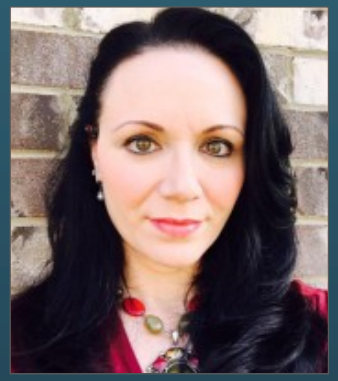
BDO pillsbury

SPRS Assessment Entry Screen



Welcome to the Jungle….

Cybersecurity Maturity Model Certification (CMMC)



Christina Reynolds| Director
C|HFI, C|EH, C|NDA
BDO Industry Specialty Services Group
+703-893-0600
creynolds@bdo.com

BDO

BDO pillsbury

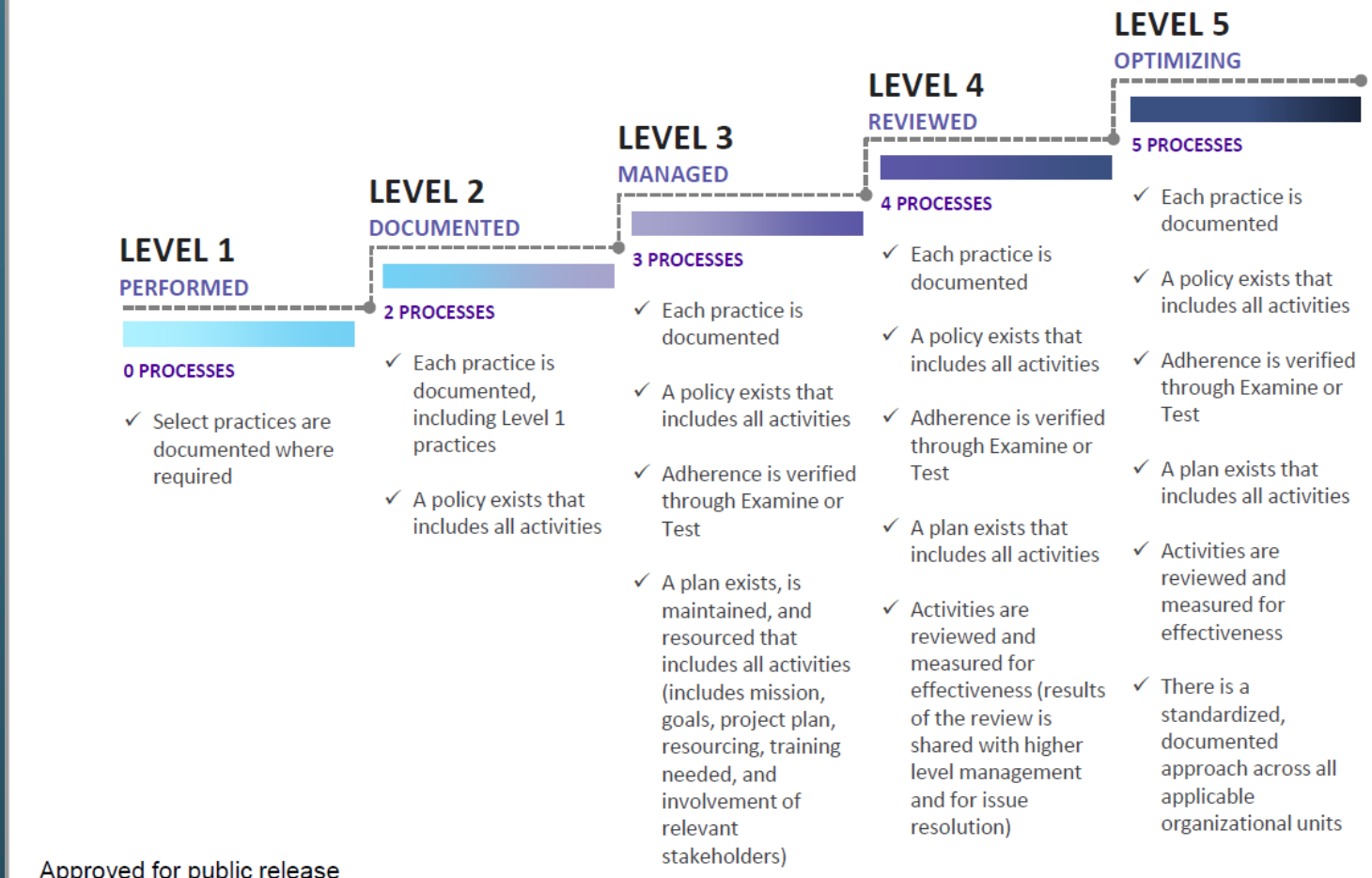
Cybersecurity Maturity Model (CMMC)

- CMMC is a cybersecurity certification program advocated by the DoD.
  - Five cybersecurity maturity levels (1-5), builds on NIST 800-171/172, 800-53, CIS
  - Measures a contractor's cybersecurity program maturity, evidenced by the implementation of prescribed NIST and other frameworks' security practices/processes
  - CMMC requirements will appear in the requirement document or statement of work.
- Initial aggressive timeline, with "Crawl, Walk, Run" approach
  - DOD will begin to roll out CMMC requirements on November 30, 2020.
  - By October 1, 2025, CMMC to be included in virtually all DOD contracts.
  - Rule does not identify criteria for determining which solicitations or contracts will include CMMC requirements.
  - Contracting officers will implement these requirements by including a third new clause introduced in the interim rule: DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement*.

BDO pillsbury

UNCLASSIFIED

CMMC Maturity Process Progression



Approved for public release

2

CMMC Maturity Levels – Building on NIST 800-171

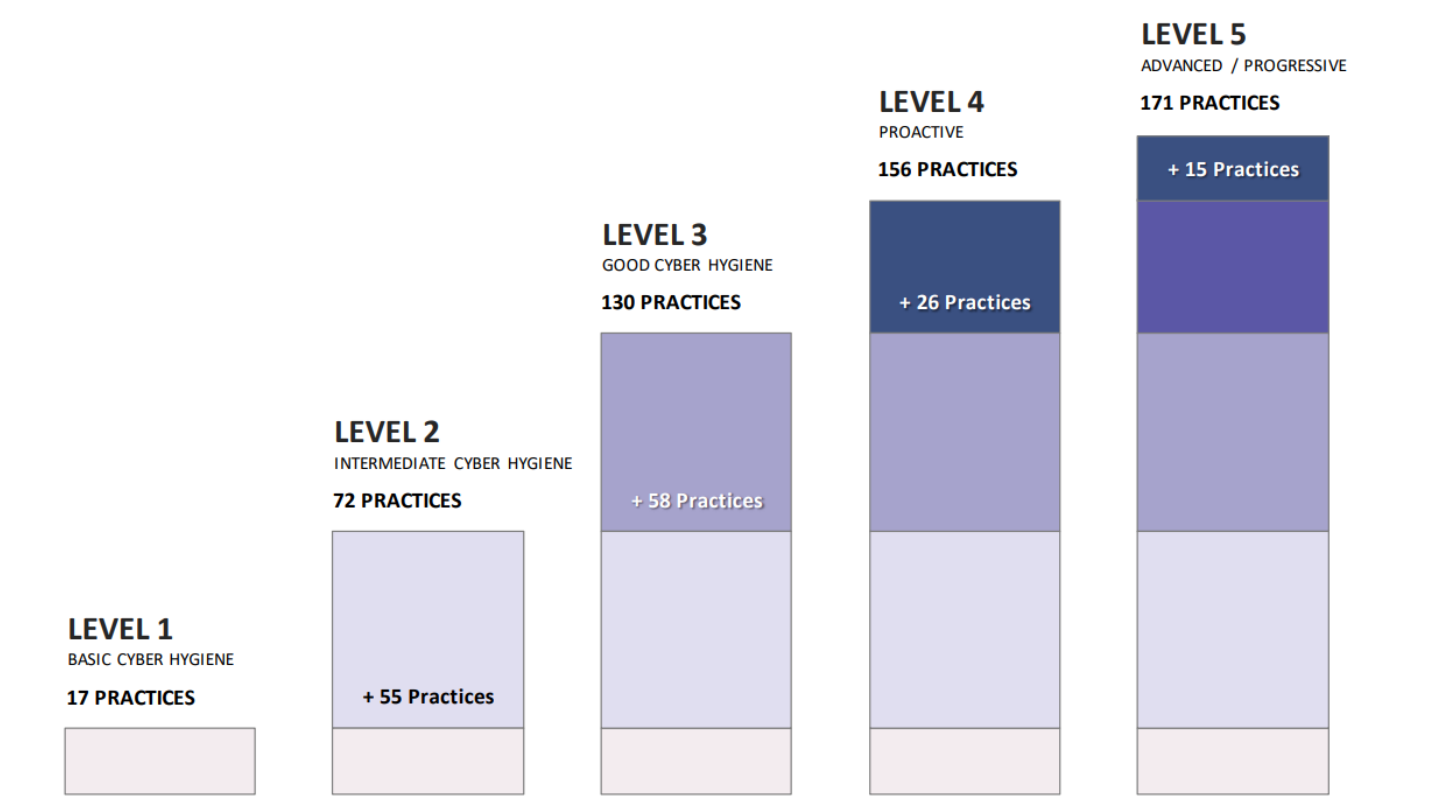


Figure 5. CMMC Practices Per Level

The Fireswamp….

Brian P. Cruz
213.488.7101
brian.cruz@pillsburylaw.com

pillsbury

Meghan D. Doherty
703.770.7519
meghan.doherty@pillsburylaw.com

pillsbury

BDO pillsbury

Prime Notifications to Subcontractors (10/15/2020)

Primes are now sending out a letter to their Teammates/subcontractors:

*"**Provide Status to [PRIME CONTRACTOR]. **

In order for [PRIME CONTRACTOR] to assess risk and preparedness for the November 30 effective date of the new rules, we must receive the status of our applicable suppliers. You will be receiving a survey link on Thursday, October 29 asking to provide the following. Please complete the survey by Thursday, November 5.

- Confirmation of NIST 800-171 Assessment Score in SPRS
- POAM ECD for any unimplemented NIST 800-171 requirements
- Status/ECD for additional 20 (7 Level 2 / 13 Level 3) CMMC practices
- Status/ECD for Level 2/3 maturity processes

Going forward, we are requesting you provide updates to this set of information until all outstanding practices and processes are implemented. When responding to this email, please provide the estimated date for closure of all NIST SP 800-171 POAM items, and the expected closure date for the additional controls."

BDO pillsbury

The Future
Cybersecurity Maturity Model Certification (CMMC)

- DFARS 252.204–7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement (NOV 2020)
  - Contractor must be CMMC Certified and ensure all subcontractors are also certified
- Five levels of certification from “basic compliance” to “state-of-the-art”
- Timeline for rollout is 2020-2025
- CMMC-AB a 501(c)(3) created in January 2020
- C3PAO - Certified Third-Party Assessment Organizations
  - Certified independent third-party organizations to conduct audits and inform risk

BDO pillsbury

CMMC Assessments

Prime Contractor

- CMMC-AB suggest will be a six-month process to be certified
- CMMC-AB Marketplace will list qualified C3PAO
- After C3PAO assessment, CMMC-AB provides quality audit
- Contractor has 90 days to resolve any findings by C3PAO
- CMMC Maturity Level Certificate Issued at appropriate level

Subcontractors

- Primes will need to ensure subs are certified to proper level prior to award
- Primes will need to manage CUI delivered or developed by subcontractors

BDO pillsbury

The Road Ahead…

- Submit your Assessment now to avoid delays in potential contract awards
  - Summary-level scores will be posted 30 days from an 800-171 Assessment to DOD in the Supplier Performance Risk System (SPRS)
  - Full gap assessments can take about 2 weeks, and feed into PoAM
  - Systems Security Plan will take another 2-4 weeks to construct
- Existing contracts?
  - Contracting officers must verify that the contractor has a current assessment before exercising an option or extending a contract "with a contractor that is required to implement the NIST SP 800-171 in accordance with the clause at 252.204-7012."
  - DOD plans to strategically assess a contractor's implementation of NIST SP 800-171 on existing contracts that include DFARS clause 252.204-7012
- Flow down requirements
  - Prime contractors must flow down these requirements "in all subcontracts and other contractual instruments" as long as neither of the two exceptions listed above apply (micro-purchase threshold or COTS items).
  - If a subcontractor does not have a current Basic Assessment, the prime "shall not award a subcontract or other contractual instrument."
  - SPRS scores are only visible to DoD, so primes will need verification of compliance from their subcontractors

BDO pillsbury

CLE Code: 2020-135

BDO pillsbury

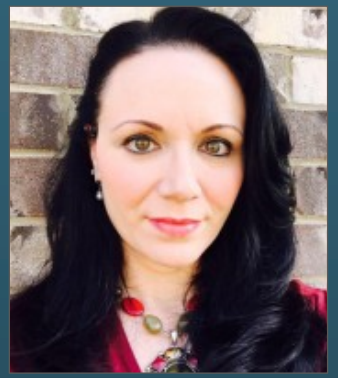
Presenters:

Brian P. Cruz
213.488.7101
brian.cruz@pillsburylaw.com

pillsbury

Meghan D. Doherty
703.770.7519
meghan.doherty@pillsburylaw.com

pillsbury



Christina Reynolds| Director
C|HFI, C|EH, C|NDA
BDO Industry Specialty Services Group
+703-893-0600
creynolds@bdo.com

BDO

BDO pillsbury

BDO

pillsbury