DEFENSE CONTRACT MANAGEMENT AGENCY

Defense Industrial Base Controlled Unclassified Information Protection and Cybersecurity Assessment

Lessons Learned/Cybersecurity Maturity Model Certification

Presented By:

Dana Mason and Carley Salmon

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), DCMA

Version 1.1

Agenda

- **Part 1: Overview**
  - **Defense Contract Management Agency (DCMA)**
  - **Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)**
  - **Assessment Confidence Levels**
  - **Pre-coordination**
- **Part 2: Assessment Process**
  - **Assessment**
  - **Post Assessment**
  - **Lessons Learned/Observations**
- **Part 3: Cybersecurity Maturity Model Certification (CMMC)**

Defense Contract Management Agency

The Defense Contract Management Agency (DCMA) is, first and foremost, a product delivery organization. Our nation's warfighters expect our defense industry to produce and deliver the equipment they need to fight, survive and win. DCMA's integrated team of acquisition and support professionals makes this happen.

- DCMA has around **12,000 employees**
- Manages over **350,000 contracts** valued at more than **$5 trillion**
- Over **19,000 locations** worldwide
- Receive **1,000** new contracts daily
- We authorize **$650 million in payments daily,** for the DoD that comes out to a 1.5 million items in "stuff" we sign into inventory for our military.

Defense Industrial Base Cybersecurity Assessment Center

Mission

Support the warfighter by assessing the Defense Industrial Base compliance in the protection of DoD Controlled Unclassified Information, ensuring contractors implement appropriate cybersecurity requirements, in support of acquisition decision making.

Vision

Security-focused, highly trained cybersecurity professionals providing comprehensive and repeatable assessments for risk-based decision making.

Security through compliance
Securitatis in obsequio

This All Started in 2013

2013

- Information Security Oversight Office (ISOO) issued a memorandum (Executive Order 13556) (April 2013). Details what CUI is.

2014

- OSD working with DIB and NIST determined that Availability and Integrity was DoD centric and Non Federal Systems need to concentrate on Confidentially

2015

- ✓ Final Drafts of NIST 800-171 out to Industry. Published June 2015
- ✓ DEC 2015 - Must be compliant in providing adequate security ASAP but NLT 31 DEC 2017

2016

- Managing Cyber Risks to Facility-Related Control Systems memo (Mar 2016)
- FAR Clause 52.204-21, "Basic Safeguarding of Contractor Information Systems," Final Rule, (June 2016)
- 32 CFR Part 236, "[DoD] Defense Industrial Base (DIB) Cyber Security (CS) Activities," Updated final rule published (October 4, 2016)
- NIST SP 800-171, Rev 1 (Dec 2016)
- Final DFARs 7012 Clause updates and clarification

2017 Showtime

- ✓ Implementation of DARS Clause 252.204-7012, Safeguarding Covered Defense, OSD Memo (21 Sept 2017). Change 2 to DoDI5000.02, Enclosure14 issued Feb 2, 2017
- ✓ DEC 31 2017 Mandated Compliance Deadline

2018-2019

- NIST SP 800-171A (June 2018)
- Strategically Implementing Cybersecurity Contract Clauses memo (Feb 2019)
- Defense Contract Management Agency Mission Changes memo (20 May 2019)
- DIBCAC Pilot Program (June 2019)
- DoD Guidance for review System Security Plans (SSPs) (6 Nov 2019)
- NIST SP 800-171 DoD Assessment Methodology v1.0 released (7 Nov 2019)
  - Assessment Scoring Template
  - Basic (Self-Assessment) results format
- Assessing Contractor Implementation of Cybersecurity Requirements to DoD and DCMA memo (14 Nov 2019)
- NIST SP 800-171 Rev2 Draft (June 2019)

Today

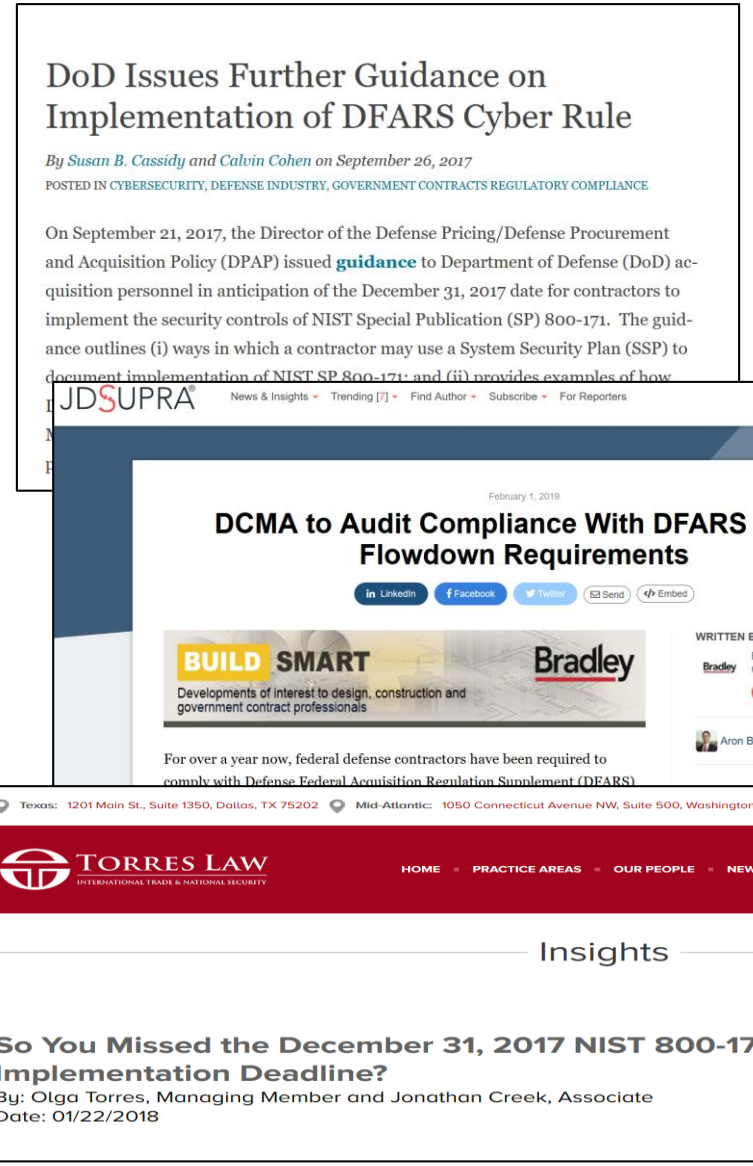
- Cybersecurity Maturity Model Certification (CMMC) v1.02 (18 Mar 20)
- NIST SP 800-171 Rev2 (June 2019)
- DoDI 5200.48, "Controlled Unclassified Information (CUI)," (6 Mar 2020)
- NIST SP 800-171 Rev2 (June 2019)
- Cybersecurity Maturity Model Certification (CMMC) v1.0 (30 Jan 2020)

DFAR Clause Changes over time

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

	Nov 18, 2013 *(Final Rule)*	Aug 26, 2015 / Dec 30, 2015 *(Interim Rules)*	October 21, 2016 *(Final Rule)*
Scope – What Information	• Unclassified Controlled Technical Information	• Covered defense information • Operationally Critical Support	• Revised/clarified definition for covered defense information
Adequate Security - Minimum Protections	• Selected controls in NIST SP 800-53	• Aug 2015 NIST SP 800-171	• NIST SP 800-171
Deadline for Adequate Security	• Contract Award	• Dec 2015 – As soon as practical, but NLT 31 Dec 17	• As soon as practical, but NLT 31 Dec 2017
Subcontractor/ Flowdown	• Include the substance of the clause in all subcontracts	• Include in subcontracts for operationally critical support, or when involving covered contractor information system	• Contractor to determine if information required for subcontractor performance retains identity as CDI

When Contractors are faced with implementing multiple versions of the clause, Contracting Officers may work with Contractors, upon mutual agreement, to implement the latest version of the clause



DoD Issues Further Guidance on Implementation of DFARS Cyber Rule

By Susan B. Cassidy and Calvin Cohen on September 26, 2017

POSTED IN CYBERSECURITY, DEFENSE INDUSTRY, GOVERNMENT CONTRACTS REGULATORY COMPLIANCE

On September 21, 2017, the Director of the Defense Pricing/Defense Procurement and Acquisition Policy (DPAP) issued **guidance** to Department of Defense (DoD) acquisition personnel in anticipation of the December 31, 2017 date for contractors to implement the security controls of NIST Special Publication (SP) 800-171. The guidance outlines (i) ways in which a contractor may use a System Security Plan (SSP) to

JDSUPRA News & Insights Trending [7] Find Author Subscribe For Reporters

February 1, 2019

DCMA to Audit Compliance With DFARS Cyber Flowdown Requirements

BUILD SMART Bradley

Developments of interest to design, construction and government contract professionals

WRITTEN BY:

Aron Beezley

For over a year now, federal defense contractors have been required to

Texas: 1201 Main St., Suite 1350, Dallas, TX 75202 Mid-Atlantic: 1050 Connecticut Avenue NW, Suite 500, Washington, DC 20036

TORRES LAW INTERNATIONAL TRADE & NATIONAL SECURITY

HOME PRACTICE AREAS OUR PEOPLE NEWS & EVENTS

Insights

So You Missed the December 31, 2017 NIST 800-171 Implementation Deadline?

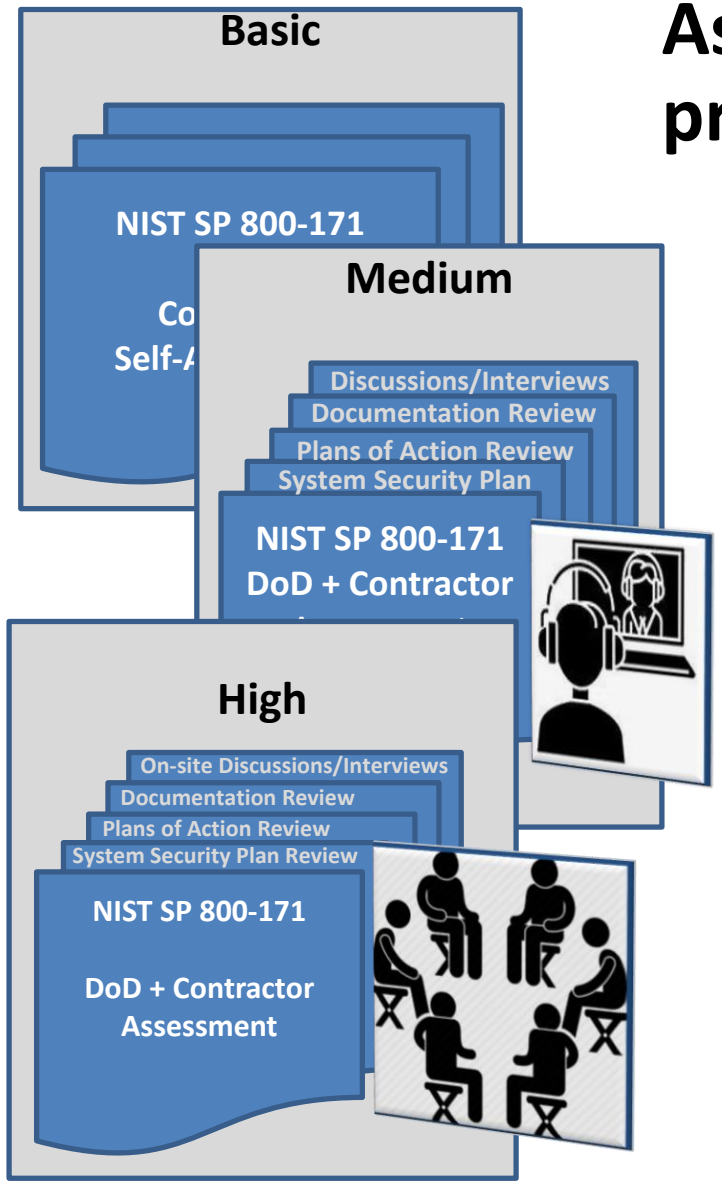
By: Olga Torres, Managing Member and Jonathan Creek, Associate

Date: 01/22/2018

What DCMA Is Tasked to Do

- **Establish the tools, databases, processes, and requirements that will apply to all**
- **Partner with other Services/Agencies to implement the same assessment mechanisms to assess the contractors and contracts that they administer**
- **Ensure the Contractor is compliant (at time of award) with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* requirements in DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting***
- **Develop the proposed path using its administration authority under Federal Acquisition Regulation (FAR) Part 42, *Contract Administration and Audit Services*; FAR Part 43, *Contract Modifications*; and DFARS Clause 242.302, *Contract Administration Functions* to modify contracts that are administered by DCMA to achieve a set of business strategies to obtain and assess contractor System Security Plan (SSPs) by leveraging its review of a contractor's purchasing system in accordance with DFARS Clause 252.244-7001, *Contractor Purchasing System Administration***

What is Assessed



Assess contractor's Enterprise level system(s) that process Controlled Unclassified Information (CUI)

- Scoring criteria defined in the NIST SP 800-171 *DoD Assessment Methodology*,
  - High Confidence (over-the-shoulder) Validation *(includes all of the below)*
  - Medium Confidence (Document Review/Discussion)
  - Basic (Contractor Self-Assessment)
- Objective assessment of contractor's requirements implementation status; not designed to credit partial implementation (with minor exceptions).
- Score reflects net effect of security requirements "not yet implemented." If all implemented = score of 110.

Confidence Levels

Assessing Contractor Implementation of DFARS 252.204-7012

There are 3 levels of DoD assessment methodology, each resulting in a different level of confidence:

Trust

Basic

- Plans of Action Review (If Req'd)
- System Security Plan Review

NIST SP 800-171

Contractor Self-Assessment

Trust & Examine

Medium

- Discussions/Interviews
- Documentation Review
- Plans of Action Review (If Req'd)
- System Security Plan Review

NIST SP 800-171

DoD + Contractor Assessment

Trust & Verify

High

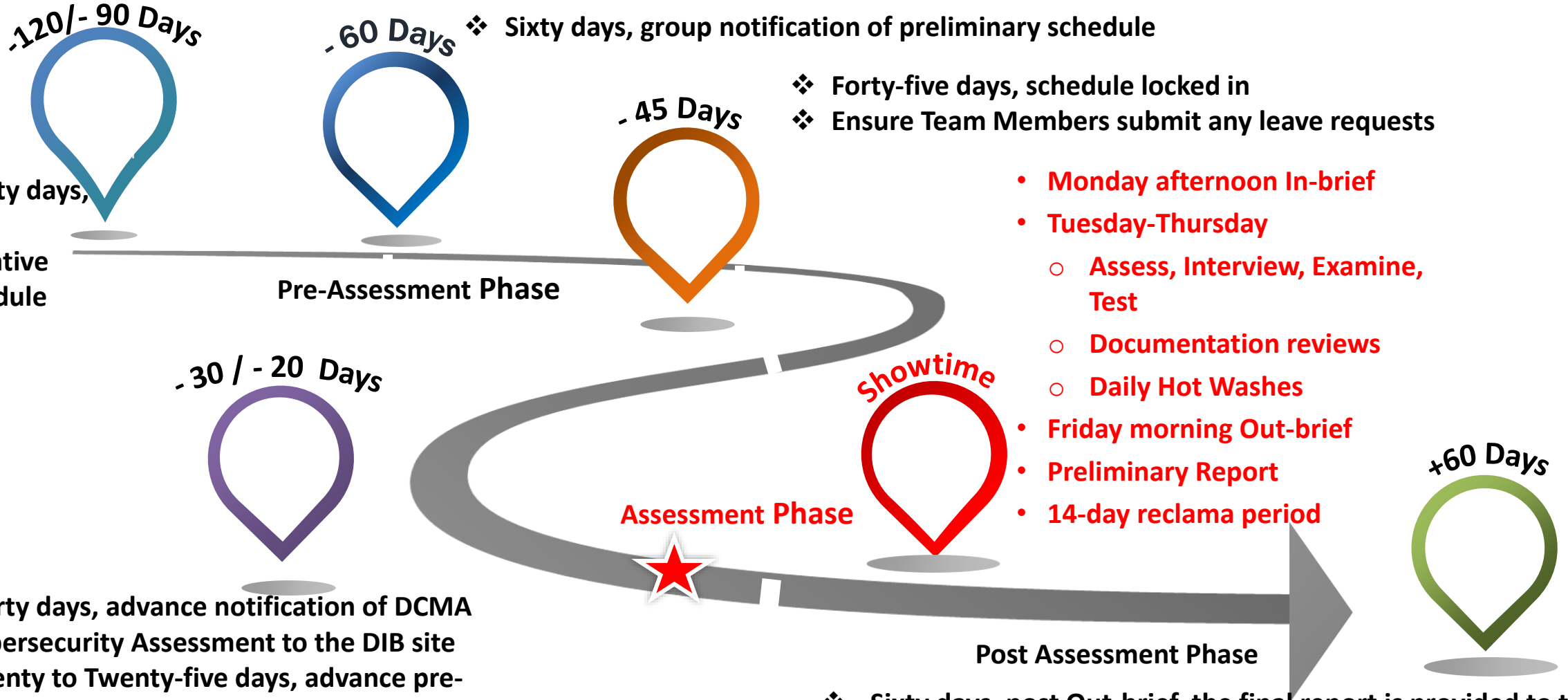
- On-site Discussions/Interviews
- Documentation Review
- Plans of Action Review (If Req'd)
- System Security Plan Review

NIST SP 800-171

DoD + Contractor Assessment

NIST 800-171 DoD Assessment Methodology

DCMA Cybersecurity Assessment Rhythm



- ❖ Ninety days, plan tentative schedule
- ❖ Sixty days, group notification of preliminary schedule
- ❖ Forty-five days, schedule locked in
- ❖ Ensure Team Members submit any leave requests
- Monday afternoon In-brief
- Tuesday-Thursday
  - Assess, Interview, Examine, Test
  - Documentation reviews
  - Daily Hot Washes
- Friday morning Out-brief
- Preliminary Report
- 14-day reclama period
- ❖ Thirty days, advance notification of DCMA Cybersecurity Assessment to the DIB site
- ❖ Twenty to Twenty-five days, advance pre-coordination meeting with the DIB site
- ❖ Sixty days, post Out-brief, the final report is provided to the DIB site through the C/D/ACO
- ❖ Sixty + days, post Out-brief, final score uploaded into SPRS

Pre-Assessment Phase

Notification Package:

- Identify Scope
- Documentation requests
- Track the artifacts from DIB site

Administration:

- Coordination meeting with DIBCAC Coordinator/DIB Site C/D/ACO
- Develop and disseminate schedule
- Identify DIBCAC POCs
- Align assessment with assessment team
- Submit DIBCAC Incoming Visit Verification Guidance to DIB site C/D/ACO
- In/Out Briefs (DCMA focused overview)
- Develop compliance status DIB Leadership Team briefings
- Any Right Seat Rider participation logistics

Coordination:

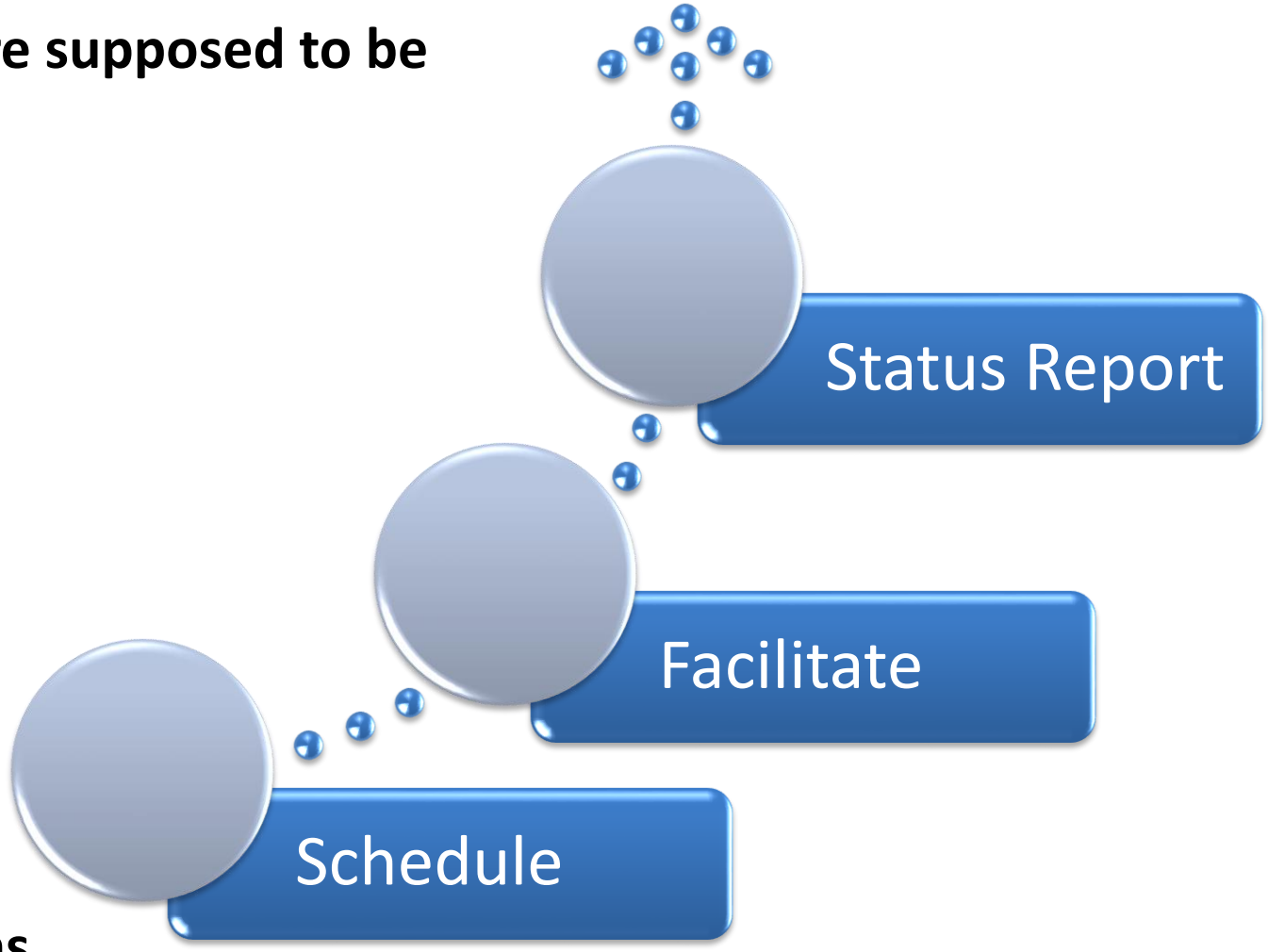
With C/D/ACO for receipt of artifacts

Pre-Assessment

- **What to do when DIBCAC contacts you**
- **Pre-coordination**
  - **basic assessment**
  - **documentation that you should have**
  - **process and programs needed**

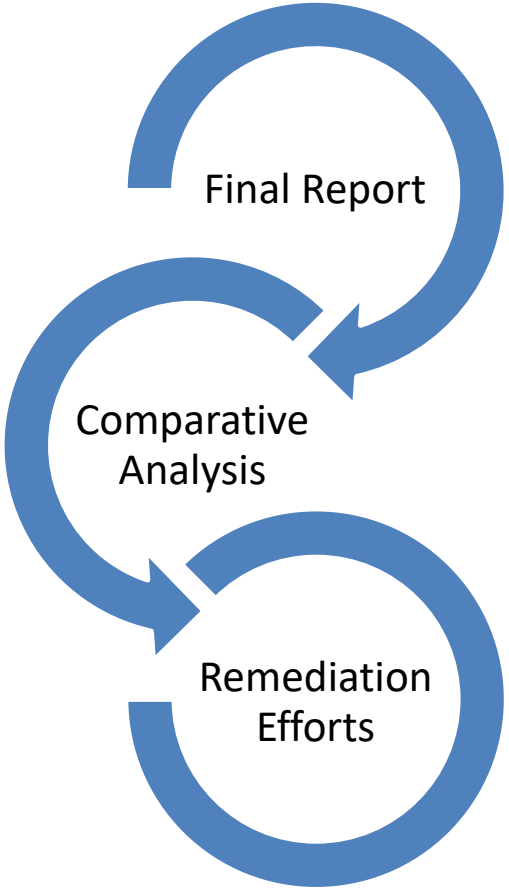
Assessment Phase

- **Maintain and manage the schedule (Team Lead)**
  - Keep all involved in the loop of statuses and schedule changes
  - Ensure personnel are where they are supposed to be
- **Facilitate meetings (Team Lead)**
  - In and Out briefs
  - Daily Hot washes
- **Daily Status reports (All Hands)**
  - What was accomplished
  - Identify preliminary deficiencies
  - The plan for the next day
  - Remaining requirements and actions



Post Assessment Phase

- **Complete Final Report:**
  - **Ensure all final report are met (internal and external)**
  - **Disseminate (brief) final report to assessment Team Lead and DIBCAC leadership within 72 hours**
  - **Coordinate any required follow on discussions regarding final report with DIB site (via C/D/ACO)**
- **Comparative Analysis:**
  - **Gap between DIB site's self-assessment and final assessment results for metrics (future efforts can also be leveraged to do a DIB metric to view a broad spectrum of the industry at large, i.e. FY21)**
  - **Assessment team collaboration, lessons learned, After Action Review (AAR), etc.**
- **Progress Brief on Remediation Activities: Any Plans of Action (POA)**



Output of High Confidence Assessment

- **DCMA generates two documents after completion of an assessment:**
  - **Assessment Memorandum:**
    - **States DCMA conducted an assessment of the contractor's compliance to the DFARS 252.204-7012.**
    - **Contains the contact information for the DIBCAC director in the event a component would like to discuss reciprocity.**
  - **Assessment Report:**
    - **Detailed description of the assessment conducted to include any items scored 'other than satisfied.'**
    - **Results - Company is compliant / non-compliant with DFARS Clause 252.204-7012**
      - **Compliant = requirements implemented, or Plan of Action (POA) in place with the expected date by when the Company will be compliant**
      - **Company goal is to reach compliance via 110**
      - **Not a Pass / Fail**
- **Score entered into Supplier Performance Risk System (SPRS)**
- **If 110 not reached:**
  - **DCMA DIBCAC re-assesses requirement post POA completion / validates compliance**
  - **Issues new Memorandum with updated score**
  - **Updates score in SPRS**

DIBCAC Dashboard

As of 12 Jun 20

FY19 Pilot: Completed 16 out of 16 Assessments

FY20: Completed 53 out of 110 Assessments

****31 Medium Confidence Assessments**

Fundamental Boot Camps:

FY19: 3

FY20: 8

Intermediate Boot Camp: 1

*Fundamentals Boot Camp – Introduction to NIST SP 800-171, Assessment Methodologies

*Intermediate Boot Camp – Subject Matter Expert (SME) Training, Lead Assessor Training, Advanced Requirements Training

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Cybersecurity Maturity Model Certification (CMMC)

- **CMMC Model combines multiple cybersecurity standards and references (i.e. NIST SP 800-171 Revision 1; Draft NIST SP 800-171B; International Organization for Standardization (ISO) 27001, *Information Security Management*; Aerospace Industries Association/National Aerospace Standards (AIA/NAS) 9933, *Critical Security Controls for Effective Capability in Cyber Defense*; and others) into one unified standard for cybersecurity**
- **Intent is to specify the required CMMC level in Requests for Proposals (RFP)**
  - **Winning offeror to achieve this CMMC level as condition of contract award.**
  - **Guiding principle underlining CMMC framework - "trust but verify"**
- **Department is currently working with military services and agencies to identify candidate programs that will implement CMMC requirements during the FY2021-FY2025 phased roll-out**
- **All new DoD contracts will contain the CMMC requirement starting in FY2026**

CMMC Methodology Under Construction

CMMC: Several Year Phase-in

Outside Government

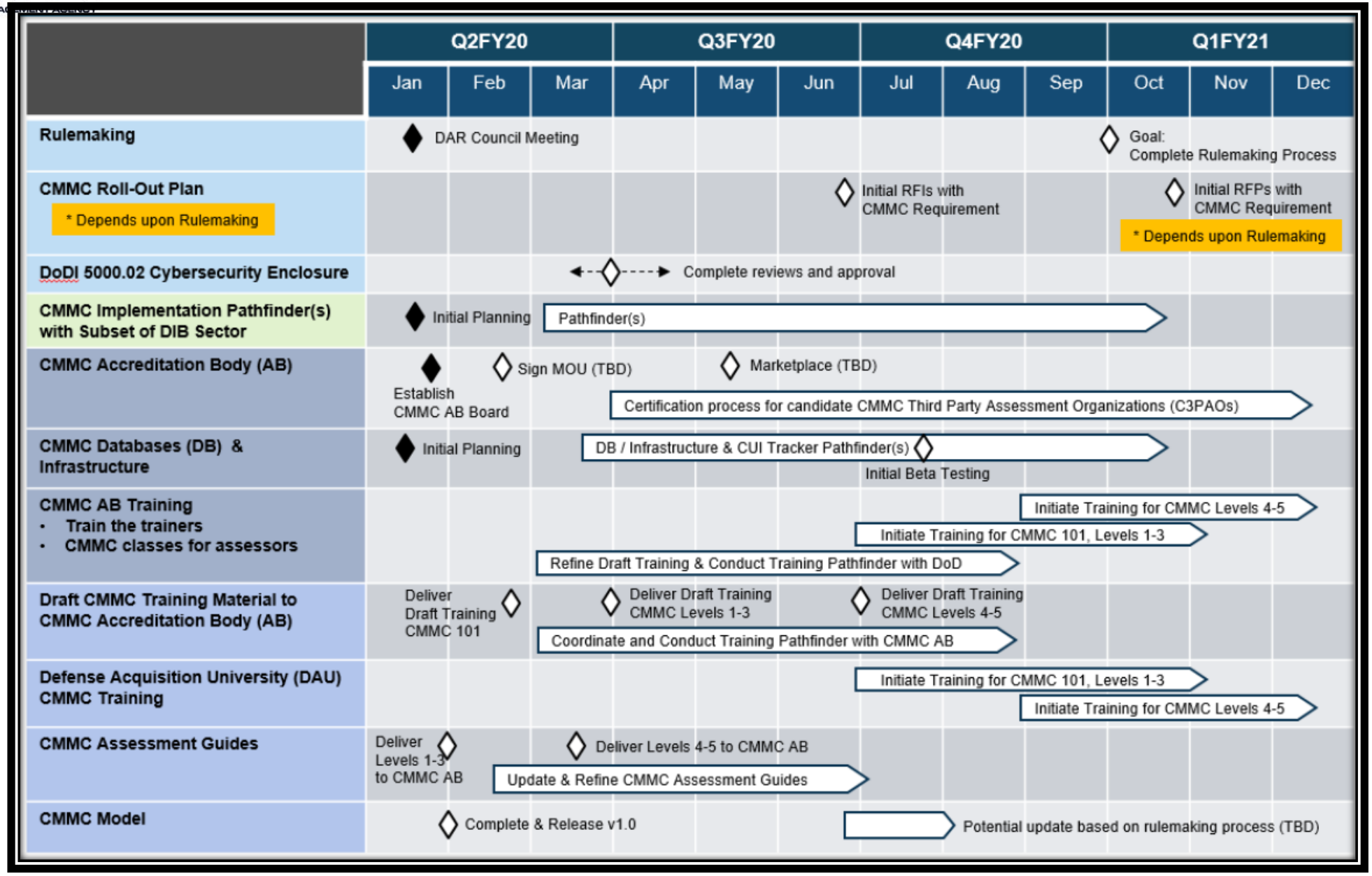
- **Governing Body**
- **Training and certification development**
- **Third Party Assessors (who, what, when, where, why, how much $)**
- **Defense Industrial Base (DIB) Companies need to become certified**
- **Need a tool to track scheduled and or certification results**

Within Government

- **DFARS Language changes**
- **DoD Procurement Activities need CMMC training**
- **DoD Contracts need CMMC language**

No matter what happens, NIST SP 800-171 still needs to be implemented as per the DFARS and is the foundation of CMMC

CMMC Draft Schedule: CY20



NIST 800-171 is Foundation for CMMC

- Currently the DFARS Clause 252.204-7012 defines 110 requirements for CMMC those 110 requirements are mixed into CMMC Level 1, 2 and 3
- CMMC adds Process Maturity Level for Level 2 and above
- CMMC adds new requirements in Level 2 & 3
- CMMC Level 1 is same requirements as identified FAR Clause 52.204-21, *Basic Safeguarding of Covered Contractor Systems*, published in 2016

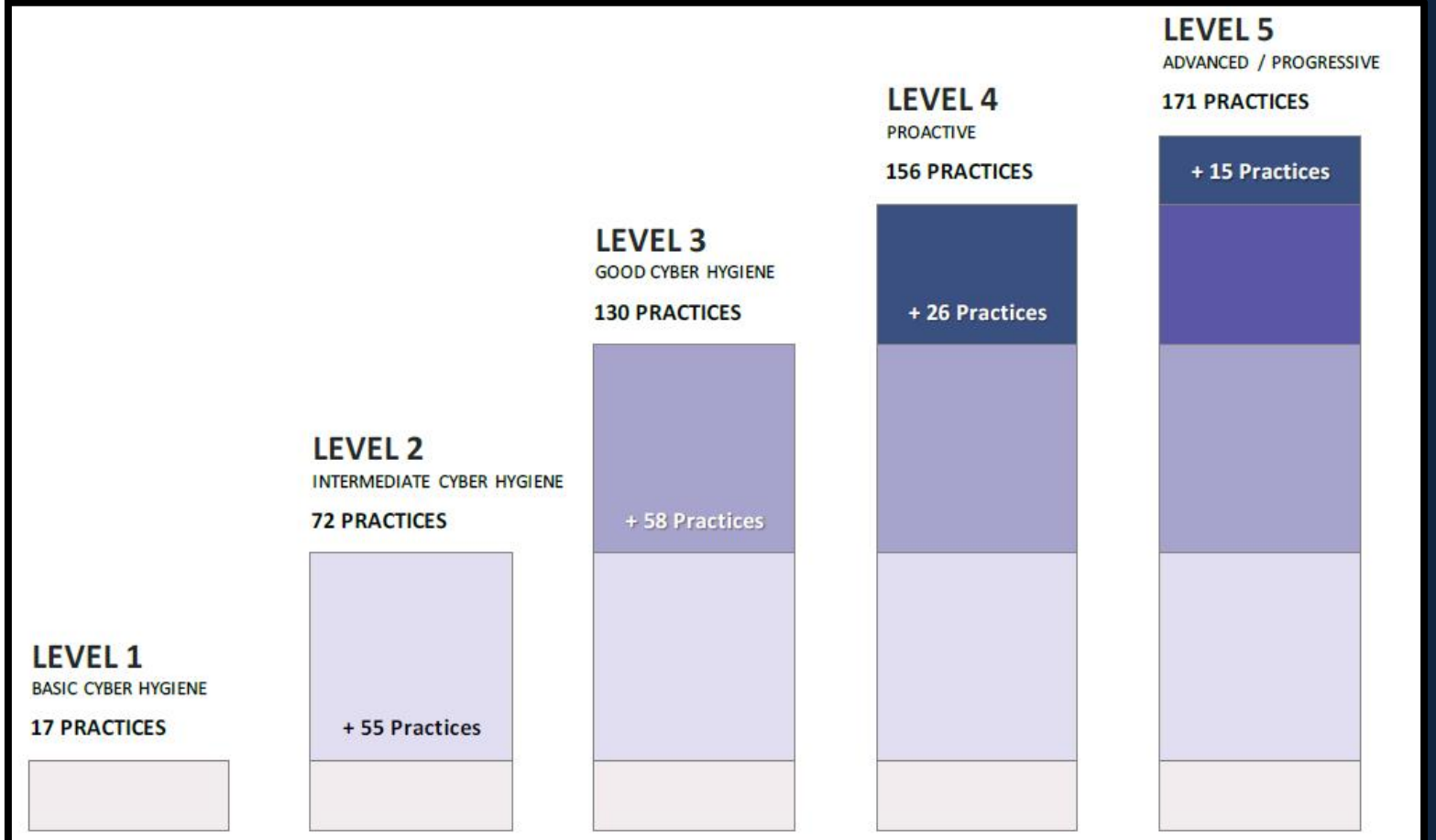


Figure 5. CMMC Practices Per Level

From CMMC Version 1.0

Final Thoughts

- **Most important take away, read:**
  - **DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting***

    There are many requirements sprinkled in there. NIST 800-171 compliance, use of cloud providers, how to and when to report cyber intrusions, Adequate security, CDI, CUI, and subcontracts.
  - **NIST SP 800-171R2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations***
  - **NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information.***

    This is our primary assessment methodology.
  - **CMMC version 1, Link: https://www.acq.osd.mil/cmmc/**

- **Everything you do for NIST 800-171 compliance relates to a CMMC Certification level!**

Questions?

dcma.lee.hq.mbx.tdx-inbox@mail.mil

Information Sharing/Details of a Specific Assessment

- Program offices may contact the contractor directly to request information pertaining to a specific assessment
- Results available via SPRS:
  - Organization that conducted the assessment (e.g., DCMA, Defense Counterintelligence and Security Agency (DCSA), or DoD component)
  - Scope of information system/system security plan(s) assessed (e.g., the internal unclassified information system(s)/network(s) , mapped to contractor Commercial and Government Entity (CAGE) codes, that support(s) performance of DoD contracts)
  - Date / Level of the assessment (i.e., Basic, Medium, or High)
  - Total summary score for each system security plan(s) assessed
  - Date that score of 110 (full implementation) expected to be achieved

Acronyms

Letters	Phrase
ACO	Administrative Contract Officer
AIA/NAS	Aerospace Industries Association/National Aerospace Standards
C/ADO	Corporate Administrative Contract Officer
CAGE	Commercial and Government Entity
CDI	Controlled Defense Information
CDRL	Contract Data Requirements List
CIO	Chief Information Officer
CMMC	Cybersecurity Maturity Model Certification
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
D/ACO	Divisional Administrative Contract Officer
DC3	DoD Cyber Crime Center
DCMA	Defense Contract Management Agency

Letters	Phrase
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
DoDI	Department of Defense Instruction
E-CFR	Electronic Code of Federal Regulations
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
GFI	Government Furnished Information
ICF	Incident Collection Format
	continued next page

Acronyms (Continued)

Letters	Phrase
ISO	International Organization for Standardization
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
PIEE	Procurement Integrated Enterprise Environment
POA	Plans of Action
Req'd	Required
SP	Special Publication
SPRS	Supplier Performance Risk System
SSP	System Security Plan

BACK UP

Alternative, Equally Effective Security Measures

- **Per DFARS Clause 252.205-7012(b)(2)(ii)(B), if the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, a written explanation of:**
  - **Why security requirement is not applicable; OR**
  - **How an alternative but equally effective security measure is used to achieve equivalent protection**
- **When DoD CIO receives a request from a contracting officer, representatives in DoD CIO review the request to determine if the proposed alternative satisfies the security requirement, or if the requirement for non-applicability is acceptable**
  - **The assessment is documented and provided to the contracting officer, generally within 5 working days**
  - **If request is favorably adjudicated, the assessment should be included in the contractor's system security plan**

Demonstrating Implementation of NIST SP 800-171

To document implementation of NIST SP 800-171, companies should have a system security plan (SSP) in place, in addition to any associated plans of action (POAs):

System Security Plan

Approved 2 May 2020
Review NLT 11 May 2021

- **<u>Security Requirement 3.12.4 (System Security Plan)</u>: Requires the contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems**
- **<u>Security Requirement 3.12.2 (Plans of Action)</u>: Requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems, and to describe how and when any unimplemented security requirements will be met**

Cyber Incident Reporting

DFARS Clause 252.204-7012(c)(1)

When a cyber incident occurs, the contractor/subcontractor shall:

- **Review contractor network(s) for evidence of compromise of covered defense information using contractor's available tools, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts.**
- **Identify covered defense information that may have been affected in the cyber incident.**
- **If contract contains requirement for operationally critical support, determine if the incident affects the contractor's ability to provide operationally critical support**
- **Rapidly report (within 72 hours of the discovery of an incident) directly to DoD.**
- **Subcontractors provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.**

Cyber Incident Reporting

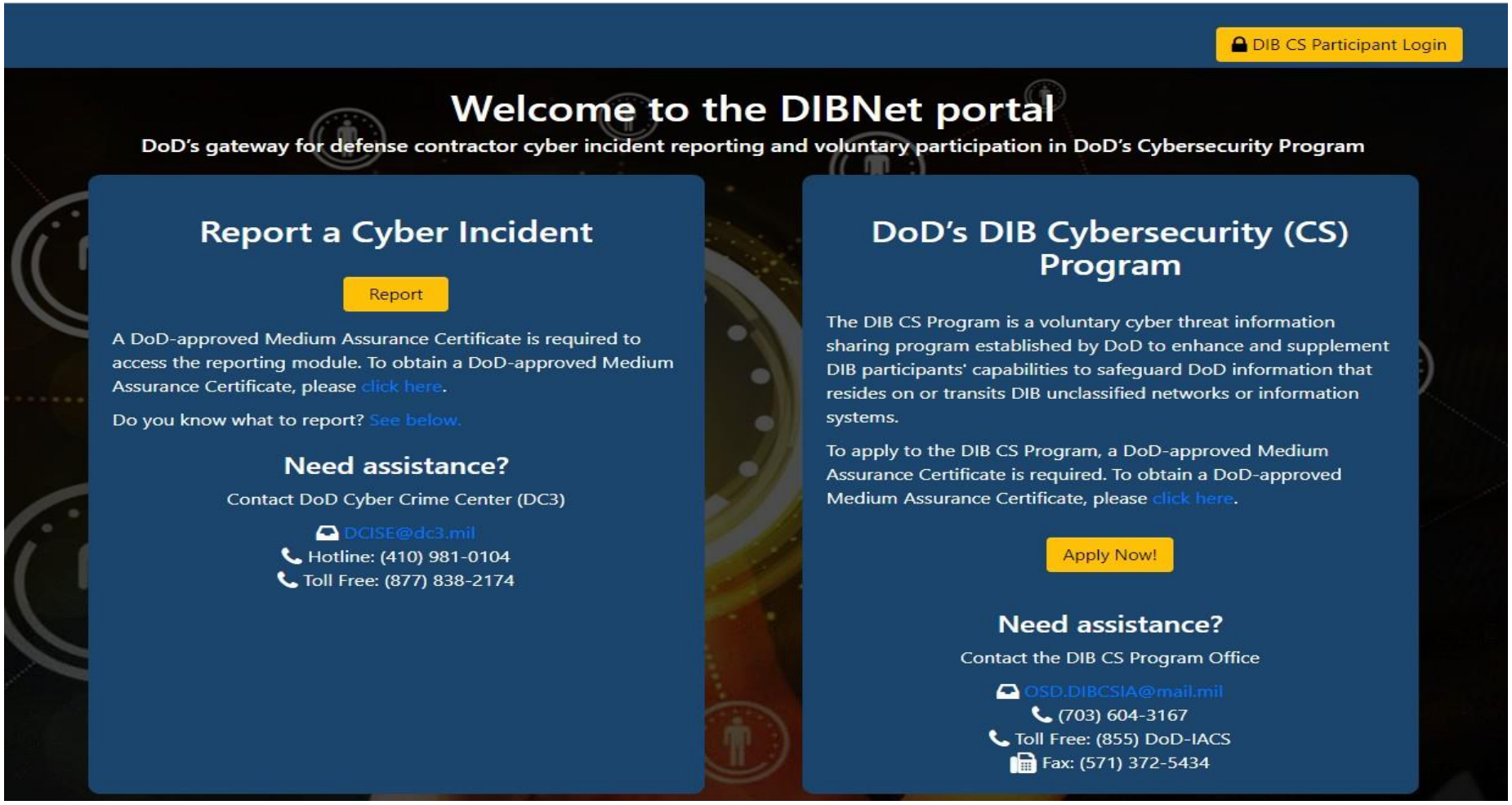
When reporting a cyber incident, contractors/subcontractors submit to DoD:

- A cyber incident report via https://dibnet.dod.mil/
- Malicious software if detected and isolated
- Media or access to covered contractor information systems and equipment when requested by the requiring activity/contracting officer

Upon receipt of a cyber incident report :

- The DoD Cyber Crime Center (DC3) sends the report to the contracting officer(s) identified on the Incident Collection Format (ICF) via encrypted email; the contracting officer(s) provides the ICF to the requiring activity(ies)
- DC3 analyzes the report to identify cyber threat vectors and adversary trends
- DC3 contacts the reporting company if the report is incomplete (e.g. no contract numbers, no contracting officer listed)

DIB Cybersecurity Web Portal

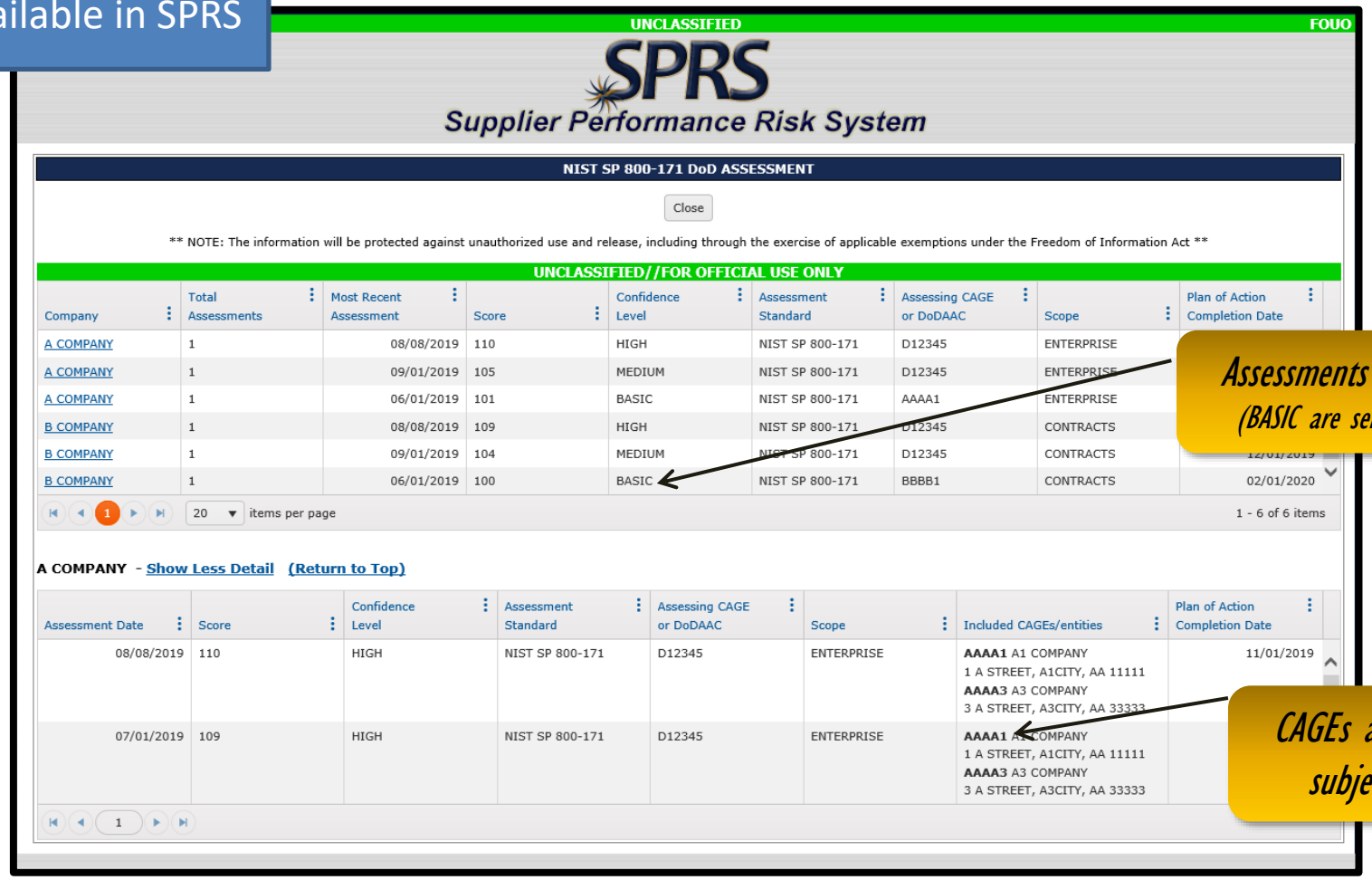


Access beyond this page requires a DoD-approved medium assurance certificate. For more information please visit the ECA website

Link: https://www.DIBNet.dod.mil

Supplier Performance Risk System (SPRS)

What will be available in SPRS



Supplier Performance Risk System (SPRS)

Overview

FOUO UNCLASSIFIED FOUO

SPRS

Supplier Performance Risk System

NIST SP 800-171 DoD ASSESSMENT

Close

** NOTE: The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act **

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Company	Total Assessments	Most Recent Assessment	Score	Confidence Level	Assessment Standard	Assessing CAGE or DoDAAC	Scope	Plan of Action Completion Date
BAE				BASIC	NIST SP 800-171			
BAE				MEDIUM	NIST SP 800-171			
BAE				HIGH	NIST SP 800-171			
BELL TEXTRON INC.				HIGH	NIST SP 800-171			
BOEING				BASIC	NIST SP 800-171			
BOEING				MEDIUM	NIST SP 800-171			
BOEING				HIGH	NIST SP 800-171			
GENERAL ATOMICS				BASIC	NIST SP 800-171			
GENERAL ATOMICS				HIGH	NIST SP 800-171			
GENERAL DYNAMICS				HIGH	NIST SP 800-171			
GENERA DYNAMICS				BASIC	NIST SP 800-171			
GENER CS ELEC				HIGH	NIST SP 800-171			
GENER CS ELECTRIC BOAT				BASIC	NIST SP 800-171			

SPRS - Detail Company View

GENERAL DYNAMICS - Show More Detail (Return to Top)

Assessment...	Score	Confidence Level	Assessment Standard	Assessing C... or DoDAAC	Scope	Included CAGEs/entities	Plan of Action Completion Dat
[redacted]	[redacted]	HIGH	NIST SP 800-171	[redacted]	ENTERPRISE	04 [redacted] 04 [redacted] 07 [redacted] 1F [redacted] 1G [redacted] 1G [redacted] 1L [redacted] 1U [redacted] 1V [redacted] 1V [redacted] 1V [redacted] 31 [redacted] 34 [redacted] 34 [redacted] 3A [redacted] 3B [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted] 3C [redacted]	[redacted]

Top Five – Most Common

MOST COMMON FINDINGS?

1. Multi-factor authentication not implemented completely
2. Not using FIPS 140-2 validated cryptography for data in transit and at rest protections
3. Poorly written and detailed system security plans
4. Network segregation (see concern above)
5. Configuration management, user installed software lack of policy & enforcement to not allow it

Top Five – Most Concerning

"MOST CONCERNING" FINDINGS?

1. DFAR Clause 252.204-7012 not being on DoD contracts, creating the question if they have CUI and are not protecting it, what can we do about from the DoD?
2. No enclave separation or segmentation from parts of corporations with presence in other countries (China, Taiwan, Hong Kong, Singapore, Eastern Europe, Middle East, former Russian Republics)
3. Lack of definition of CUI by DoD Contracts making it hard for DIB and DIBCAC to discern what should be protected or limited within the corporate boundaries
4. Not having Multifactor authentication and FIPs validated cryptography making CUI potentially visible in clear text (see below)
5. Lack of supplier implementing DFAR Clause 7012 in DoD Prime contracts for their suppliers, not being able to validate the supply chain to the companies assessed, adversaries will go after the weakest link/ easiest target