Posting NIST SP 800-171 DoD Assessment Self Assessment Scores in the Supplier Performance Risk System (SPRS)

Defense Pricing and Contracting

Lt Col Bryan Lamb

Program Manager, Supplier Performance Risk System

Mr. John Duncan

February 23, 2021
Overview

DFARS Interim Rule 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements

- Requirements concerning NIST SP 800-171 DoD Self-Assessment Scores in SPRS

Supplier Performance Risk System (SPRS) Overview
DFARS 204.7303, Procedures.

Directs contracting officers to verify in SPRS that an offeror has the summary level scores of a current NIST SP 800-171 DoD Assessment on record if the offeror is required to implement NIST SP 800-171, in accordance with DFARS clause 252.204-7012

- Must occur prior to awarding a contract, task order or delivery order; and
- Must occur prior to exercising an option period or extending the period of performance

DFARS 252.204-7019, “Notice of NIST SP 800-171 DoD Assessment Requirements”

- Notifies offerors that in order to be considered for award, the offeror is required to have a current NIST SP 800-171 DoD Assessment and that it shall be posted in SPRS
  - The offeror/contractor must submit Basic (self) Assessment scores for each system supporting the performance of the contract
  - Entity (CAGE) codes must also be mapped to the appropriate system security plan(s)
  - The offeror/contractor may submit scores via encrypted email to webptsmh@navy.mil for posting to SPRS. SPRS now has increased functionality for offerors/contractors to enter scores directly into SPRS.

DFARS clause 252.204-7020, “NIST SP 800-171 DoD Assessment Requirements”

- Requires contractors to flow-down the clause, and to ensure applicable subcontractors have the results of a current Assessment posted in SPRS prior to awarding subcontract/other contractual instruments. Also, requires contractors to provide access to the Government for medium/high assessments.
Supplier Performance Risk System (SPRS)

SPRS is a web-enabled enterprise application that serves as DoD’s single, authorized application to retrieve supplier performance information.

In 2020, SPRS was updated to document, store, and retrieve summary results from NIST SP 800-171 DoD Assessments:

- Access is granted to authorized acquisition Government personnel using a single sign-on capability in the Procurement Integrated Enterprise Environment (PIEE).
- Access is also granted to Government Contractors to view their own company contract information.
### NIST SP 800-171 DoD Assessments in SPRS

#### Supplier Performance Risk System (SPRS)

**Assessments by DCMA**
- BASIC are self-assessed

**CAGEs and facilities subject to SSP**

<table>
<thead>
<tr>
<th>Company</th>
<th>Total Assessments</th>
<th>Most Recent Assessment</th>
<th>Score</th>
<th>Confidence Level</th>
<th>Assessment Standard</th>
<th>Assessing CAGE or DoDAAC</th>
<th>Scope</th>
<th>Plan of Action Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. COMPANY</td>
<td>1</td>
<td>08/08/2019</td>
<td>110</td>
<td>HIGH</td>
<td>NIST SP 800-171</td>
<td>D12345</td>
<td>ENTERPRISE</td>
<td>11/01/2019</td>
</tr>
<tr>
<td>A. COMPANY</td>
<td>1</td>
<td>09/01/2019</td>
<td>105</td>
<td>MEDIUM</td>
<td>NIST SP 800-171</td>
<td>D12345</td>
<td>ENTERPRISE</td>
<td>12/01/2019</td>
</tr>
<tr>
<td>A. COMPANY</td>
<td>1</td>
<td>06/01/2019</td>
<td>104</td>
<td>BASIC</td>
<td>NIST SP 800-171</td>
<td>AAAA1</td>
<td>ENTERPRISE</td>
<td>02/01/2020</td>
</tr>
<tr>
<td>B. COMPANY</td>
<td>1</td>
<td>09/01/2019</td>
<td>109</td>
<td>HIGH</td>
<td>NIST SP 800-171</td>
<td>D12345</td>
<td>CONTRACTS</td>
<td>11/01/2019</td>
</tr>
<tr>
<td>B. COMPANY</td>
<td>1</td>
<td>08/08/2019</td>
<td>104</td>
<td>MEDIUM</td>
<td>NIST SP 800-171</td>
<td>D12345</td>
<td>CONTRACTS</td>
<td>12/01/2019</td>
</tr>
<tr>
<td>E. COMPANY</td>
<td>1</td>
<td>06/01/2019</td>
<td>101</td>
<td>BASIC</td>
<td>NIST SP 800-171</td>
<td>BBBB1</td>
<td>CONTRACTS</td>
<td>02/01/2020</td>
</tr>
</tbody>
</table>

**Note:** The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (FOIA).
Questions?
Overview of CMMC eMASS

CMMC-AB Town Hall Briefing

23 Feb 2021
CMMC eMASS

The Enterprise Mission Assurance Support Service (eMASS) application supports Information Assurance (IA) program management and automates DoD’s Risk Management Framework (RMF) process.

CMMC eMASS is a tailored, customized version of eMASS that provides:

- Assessment Data Repository
- Data Ingest
- CMMC Certificate Generation
- Dispute Resolution Processes
- Process and Data Flows
- Reporting and Metrics

CMMC eMASS production environment to be deployed in March 2021.
CMMC Assessment Data Standard

- The data standard defines the data contents and format needed for assessment data ingest into CMMC eMASS.
- Assessment information and results must be uploaded to CMMC eMASS by a designated C3PAO staff member as part of the certification process:
  - No sensitive or proprietary artifacts from the assessments will be stored by CMMC eMASS or in the C3PAO’s infrastructure.
  - Access to CMMC eMASS requires a positive suitability determination for account activation and use of a DoD hard token (e.g., ECA token or CAC).
- Excel spreadsheets will be made available from the CMMC-AB and from the CMMC eMASS application that may be used by authorized C3PAOs to collect CMMC assessment data.
- CMMC assessment tools developed by third parties must be compliant with CMMC assessment data standard, a JSON* schema.

*CMMCeMASS will ingest either JSON files or the spreadsheets directly.

Pilots and initial assessments of C3PAOs can use the spreadsheets.

* JSON is a commonly used language-independent open standard file and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and array data types. [Wikipedia]

DISTRIBUTION A. Approved for public release
CMMC Environments
CMMC eMASS Initial Deployment

Assessor and Instructor Data:
- C3PAOs
- Assessors
- Instructors
- Licensed Training Partners
- Licensed Publishing Partners

CMMC eMASS
- Assessment Data Repository
- Data Ingest
- CMMC Certificate Generation
- Dispute Resolution Processes
- Reporting and Metrics

SPRS
CMMC Data:
- Company Information
- Assessment Scope
- CMMC Level
- Expiration Date

Certificate generated by CMMC eMASS, retrieved by C3PAO, and sent securely to DIB company

DISTRIBUTION A. Approved for public release
CMMC eMASS CONOPS and Job Aids

• The Database-Infrastructure WG is developing a CMMC eMASS CONOPS document
  – Describes the CMMC eMASS stakeholders, users, requirements for use, and functional capabilities available to each user type
  – Draft to completed end of February 2021

• The CMMC eMASS developers will provide CMMC eMASS Job Aids
  – Provides step-by-step instructions for using CMMC eMASS, including screen shots to aid new users
  – To be delivered end of March 2021
Cybersecurity Maturity Model Certification (CMMC)
Pilots

CMMC-AB Town Hall Briefing

23 Feb 2021
CMMC Risk Reduction: Pathfinders

- OUSD(A&S) funded risk reduction activities to inform CMMC implementation
- Mock Assessments are non-attributional, non-punitive and don’t result in certification

<table>
<thead>
<tr>
<th>Missile Defense Agency (MDA) Pathfinder (Apr 2020 – Feb 2021)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity:</strong> Mock Assessments</td>
</tr>
<tr>
<td>Mock Assessors trained by CMMC-AB</td>
</tr>
<tr>
<td>Conducted mock assessments:</td>
</tr>
<tr>
<td>• CMMC Level 3 ‘delta’ of prime contractor</td>
</tr>
<tr>
<td>• CMMC Level 3 and Level 1 of two subcontractors</td>
</tr>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td>Validate drafted CMMC Assessment Guides and gather lessons learned</td>
</tr>
<tr>
<td><strong>Outcome</strong></td>
</tr>
<tr>
<td>Identified Lessons Learned to improve draft documentation and assessment processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defense Logistics Agency (DLA) Pathfinder (Sep 2020 – present)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Planned Activity:</strong> Mock Assessments</td>
</tr>
<tr>
<td>Conduct two mock assessments:</td>
</tr>
<tr>
<td>• CMMC Level 3 of two prime contractors</td>
</tr>
<tr>
<td>• Assessed by authorized C3PAOs</td>
</tr>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td>Identify and reduce risks associated with newly authorized C3PAOs</td>
</tr>
</tbody>
</table>

**Activity:** Acquisition Tabletop

Conducted a sequence of evolving TTXs that focus on the DoD’s acquisition processes from RFI to post contract award.

**Objective**

Identify and reduce risks associated with implementing CMMC in future acquisitions

**Outcome**

Developed exemplar RFI, RFP and flow down language to support contract actions

**Update:** MDA Pathfinder is completed

DLA Pathfinder assessments will be conducted by Authorized C3PAOs

DISTRIBUTION A. Approved for public release
CMMC Implementation: Pilots

The following candidate programs were identified in a DoD Press Release (15 Dec 20):

<table>
<thead>
<tr>
<th>Service or Agency</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Army</td>
<td>Foreign Military Sales (FMS) Field Service Representative Support</td>
</tr>
<tr>
<td></td>
<td>Woman, Infant, &amp; Children (WIC) Overseas Program for DHA-10-TRICARE</td>
</tr>
<tr>
<td></td>
<td>Main Operating Base-Installation Service Nodes (MOB-ISN)</td>
</tr>
<tr>
<td>Navy</td>
<td>Integrated Common Processor</td>
</tr>
<tr>
<td></td>
<td>F/A-18E/F Full Mod of SBAR &amp; Shut off Valve</td>
</tr>
<tr>
<td></td>
<td>DDG-51 Lead Yard Services / Follow Yard Services</td>
</tr>
<tr>
<td>Air Force</td>
<td>Mobility Air Force Tactical Data Links</td>
</tr>
<tr>
<td></td>
<td>Consolidated Broadband Global Network Area Network Follow-On</td>
</tr>
<tr>
<td></td>
<td>Azure Cloud Solution</td>
</tr>
<tr>
<td>Missile Defense Agency</td>
<td>Technical Advisory and Assistance Contract</td>
</tr>
</tbody>
</table>

DoD plans to implement CMMC in a phased rollout (FY21-FY25) over five years, commencing with up to 15 new acquisitions in FY21:
- The rollout ramps up over 5 years with CMMC in up to 475 new prime contracts by FY25
- Until 1 Oct 2025, USD(A&S) must approve use of the CMMC clause for new acquisitions

Update: 14 new acquisitions identified CMMC requirements actively being added to pilot RFPs

DISTRIBUTION A. Approved for public release