Understanding CMMC Level 1 Certification

Mark Lupo, MBA, MBCP, SMP

The University of Georgia
Small Business Development Center

July 28, 2020
Overview

I. Background

II. Requirements

III. Compliance

IV. CMMC
Cybersecurity and Supply Chain Risk Management

STARS III bidders will be considered in light of the terms and conditions of as many as 38 cybersecurity and supply chain risk management (SCRM) laws, regulations, standards and policies listed in an attachment document to the RFP.

The RFP addresses the possibility that some STARS III task orders will be subject to the Pentagon’s contentious Cybersecurity Maturity Model Certification (CMMC) that requires all defense suppliers to undergo regular cybersecurity audits. It’s likely the initiative will soon extend to all agencies. The RFP instructs companies to “begin preparing for CMMC and SCRM accreditation by staying aware of developing requirements.” Although non-compliant CMMC companies will not be disqualified for a STARS III bid, but Bloomberg Government expects it may put companies at a competitive disadvantage for task orders in future years.
Background
Timeline

- **NIST SP 800-53**: Initial Release, Dec 2005
- **EO 13556 (CUI)**: 4 Nov 2010
- **EO 13636 Improving Critical Infrastructure (CS)**: 12 Feb 2013
- **NIST SP 800-171**: 18 Jun 2015
- **NIST SP 800-171**: Full Compliance Mandated, 31 Dec 2017
- **Rev 1 – 20 Feb 2018**

*Small Business Development Center*
*UNIVERSITY OF GEORGIA*
CMMC Timeline

- CMMC Version 0.3
  - June 2019
- CMMC Version 0.4
  - September 2019
- CMMC Version 0.6
  - November 2019
- CMMC Version 0.7
  - December 2019
- CMMC Version 1.0
  - January 2020
The CyberSecurity Framework
Requirements
Primary Trigger - DFARS Clause

(DFARS) 252.204-7012
(Safeguarding of Unclassified, Controlled Technical Information)

- This clause triggers compliance requirements to NIST SP 800-171, Rev 2
NIST SP 800-171 (Rev 2)

• 14 Families of Security Requirements
14 Families of Security Requirements

• Access Control
• Awareness and Training
• Audit and Accountability
• Configuration Management
• Identification and Authentication
• Incident Response
• Maintenance

• Media Protection
• Personnel Security
• Physical Protection
• Risk Assessment
• Security Assessment
• System and Communications Protection
• System and Information Integrity
NIST SP 800-171 (Rev 2)

• 14 Families of Security Requirements
• 110 Control Points
• System Security Plan (SSP) and Plan of Action and Milestones (POAM)
• Need a Breach Response Plan
When Present, Must Either...

• Not bid on the contract
• Take steps to comply with the information security requirements covered within NIST SP 800-171, Rev 2
• Seek an exception to the application of the rule
• Disclose and request approval of an alternative, but equally effective, security measure that may be implemented in place of compliance with requirements.
Some Definitions...

- Defense Industrial Base (DIB)
- Covered Defense Information (CDI)
- Federal Contract Information (FCI)
- Controlled, Unclassified Information (CUI)
- Code of Federal Regulations (CFR)
- Defense Contract Management Agency (DCMA)
- Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)
252.204-7012 Safeguarding of Unclassified Controlled Technical Information

All data shall be safeguarded when the material exceeds 250 lbs. (excluding the pallet), or exceeds 20 cubic feet, to comply with the requirements of Department of the Army Pamphlet 700-32 and MIL-STD-147E.

This is currently an unfunded requirement with a high expectation that funds will be available. When and if funds become available a contract will be awarded at that time.

Please address your questions through the FedBiz Buy. If your questions are not being answered in a timely manner, please send your question to the S2/P2 Contracting Officer - usarmy.mcc.mwoc.mbx.mcc.mucp@mail.mil or call 315-777-5522.

Additional Info:
www.fedbid.com (b-945955, n-252513)
General Information

Contract Opportunity Type: Combined Synopsis/Solicitation (Original)
All Dates/Times are (UTC-04:00) EASTERN STANDARD TIME, NEW YORK, USA
Original Published Date: Jul 17, 2020 01:42 pm EDT
Original Date Offers Due: Jul 22, 2020
Inactive Policy: Manual
Original Inactive Date: Jan 10, 2021

However, you can also protest to Headquarters (HQ), Army Material Command (AMC). The HQ AMC-Level Protest Program is intended to encourage interested parties to seek resolution of their concerns within AMC as an Alternative Dispute Resolution forum, rather than filing a protest with the Government Accountability Office (GAO) or other external forum. Contract award or performance is suspended during the protest to the same extent, and within the same time periods, as if filed at the GAO. The AMC protest decision goal is to resolve protests within 20 working days from filing. To be timely, protests must be filed within the periods specified in FAR 33.103. If you want to file a protest under the HQ AMC-Level Protest Program, the protest must be in accordance with that program and be sent to the address below. All other agency-level protests should be sent to the contracting officer for resolution. Headquarters U.S. Army Material Command Office of Contract Counsel 4400 Martin Road Rm: A6SE04.001 Redstone Arsenal, AL 35898-5900 Fax: (256) 450-8840. Packages sent by FedEx or UPS should be addressed to: Headquarters U.S. Army Material Command Office of Contract Counsel 4400 Martin Road Rm: A6SE04.001 Redstone Arsenal, AL 35898-5900 Fax: (256) 450-8840. The AMC-Level Protest Procedures are found at: http://www.army.mil/pa/COMMANDCOUNSEL.asp. If internet access is not available, contact the contracting officer or HQ, AMC to obtain the HQ AMC-Level Protest Procedures.

"52.204-9, Personal Identity Verification of Contractor Personnel; 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards; 52.222-41, Service Contract Act; 52.237-2, Protection of Government Buildings, Equipment and Vegetation; 252.201-7000, COR Clause; 252.223-7000, Protection on Storage and Disposal Of Toxic and Hazardous Materials; 252.243-7001, Pricing of Contract Modifications; 252.246-7000, Material inspection and receiving report."

Wide Area Workflow Payment Instruction:

252.204-7012 Safeguarding of Unclassified Controlled Technical Information

All deliveries shall be packaged when the material exceeds 10 lbs, (excluding the pallet), or exceeds 20 cubic feet, to comply with the requirements of Department of the Army Pamphlet 700-32 and MIL-STD-147E.
Assault Breacher Vehicle Remote Control System Market Survey

DESCRIPTION OF INTENT:

This is a market investigation requesting information in support of the following performance requirements: No contract will be awarded from this announcement. This is not a Request for Proposal (RFP) or an announcement of a forthcoming solicitation. Also, it is not a request seeking contractors interested in being placed on a solicitation mailing list. Response to this questionnaire is voluntary and no reimbursement will be made for any costs associated with providing information in response to the market survey and any follow-on information requests. Data submitted in response to this market investigation will not be returned. Although no solicitation document exists at this time, information derived from this market investigation will help the Government determine the suitability of the marketplace for satisfying this performance requirement. This requirement is a candidate for a CMMC pilot program. Any resulting contract may exercise the CMMC process as a non- attribution, not-for-credit assessment of the prime contractor and select subcontractors as part of the scope of work.
23. Have you ever been required by a Federal contract, subcontract, solicitation, or agreement to transmit, store, or process federal contract information on nonfederal information systems and comply with the FAR Clause 52.204-21? If so, which of the NIST SP 800-171 requirements have not been met, if any? Have you ever been required by a DoD contract, subcontract, solicitation, or agreement to transmit, store, or process controlled unclassified information (CUI) on nonfederal information systems and comply with the DFARS clause 252.204-7012? If so, which of the NIST SP 800-171 requirements have not been met, if any? Has your system security plan (SSP) ever been assessed by the DCMA DIBCAC? If so, what score did it receive? How many (or percentage) of your potential subcontractors have ever been required to comply with FAR clause 52.204-21? DFARS clause 252.204-7012? How many (or percentage) of subcontractors are expected to transmit, store, or process FCI or CUI in the performance of this contract, if any? How many or what percentage of your potential subcontractors have SSPs that have been assessed by the DCMA DIBCAC?

24. Please provide any information you believe we are missing or are overlooking.
Compliance

Step 1: Determine the Scope of the Contract
Step 2: Assess Level of Compliance
Step 3: Clarify Plan of Action/Milestones
Step 4: Develop System Security Plan
Step 5: Ongoing Compliance Initiatives
What is a maturity model?

• A tool for assessing an organization's effectiveness at achieving a particular goal.

• Enables organizations to identify where their practices are weak or not taken seriously and where their practices are truly embedded.

• Help to distinguish between organizations in which security is *baked in* and those in which it is merely *bolted on*.

• Gives an organization’s leadership a way to measure the progress made in embedding security into its day-to-day and strategic operations.

National Cyber Security Centre – Ann W
CyberSecurity Maturity Model Certification (CMMC)

• CMMC requires a third party, cybersecurity certification to validate the cybersecurity infrastructure of the company
The CMMC-AB estimates that up to 6,000 companies will require CMMC certification in Federal FY21.

https://www.cmmcab.org/c3pao-lp
CyberSecurity Maturity Model Certification (CMMC)

• CMMC requires a third party, cybersecurity certification to validate the cybersecurity infrastructure of the company

• Will grade cybersecurity infrastructure on a scale of 1 to 5, 5 being the most stringent

• Standards defined as of January 2020

• Certifying companies are being trained and ‘certified’ by summer of 2020.

• Approximately 300,000+ DOD contractors will need to be certified

• Contract solicitations (RFP’s) will begin incorporating CMMC requirements (#1 to #5) in September of 2020

• Will require a company, Tier 1 and subs, to have the CMMC certification to match the level required on the solicitation prior to being awarded the contract
CMMCM Model Framework

- **Domains**: 17 Categories for cybersecurity
- **Capabilities**: 43 Achievements to ensure cybersecurity within each domain
- **Practices and Processes**: Activities required by level to achieve a capability (total of 171)
CMMIC
17 Domains

Figure 3. CMMIC Model Domains
Figure 2. CMMC Levels and Descriptions

- Level 1: Performed (Basic Cyber Hygiene)
- Level 2: Documented (Intermediate Cyber Hygiene)
- Level 3: Managed (Good Cyber Hygiene)
- Level 4: Reviewed (Proactive)
- Level 5: Optimizing (Advanced / Progressive)
CMMC Practices Per Level

**LEVEL 1**
Basic Cyber Hygiene
17 Practices

**LEVEL 2**
Intermediate Cyber Hygiene
72 Practices
+ 55 Practices

**LEVEL 3**
Good Cyber Hygiene
130 Practices
+ 58 Practices

**LEVEL 4**
Proactive
156 Practices
+ 26 Practices

**LEVEL 5**
Advanced / Progressive
171 Practices
+ 15 Practices

Figure 5. CMMC Practices Per Level
48 CFR § 52.204-21

Basic Safeguarding of Covered Contractor Information Systems

• The Basis for CMMC Level 1 Compliance

• Consists of 17 Practices
48 CFR § 52.204-21
Basic Safeguarding of Covered Contractor Information Systems

I. Domain – Access Control (AC)
   3 Capabilities, 4 Practices

II. Domain – Identification and Authentication (IA)
    1 Capability, 2 Practices

III. Domain – Media Protection (MP)
    1 Capability, 1 Practice

IV. Domain – Physical Protection (PE)
    1 Capability, 4 Practices

V. Domain – System and Communication Protections (SC)
    1 Capability, 2 Practices

VI. Domain – System and Information Integrity (SI)
    2 Capabilities, 4 practices
CMMC Model overview briefing:

- CMMC Model Briefing PDF

CMMC Model v1.02:

- CMMC Model PDF

CMMC Model v1.02 Appendices:

- CMMC Model Appendices PDF

CMMC Model v1.02 (Appendix A) in tabular format:

- CMMC Model (Appendix A) Excel

CMMC Model Errata:

- CMMC Model Errata PDF

https://www.acq.osd.mil/cmmc/
CMMC V1.02 Appendices

- Appendix A – CMMC V1.0 Model Overview (Pg. 6 – 40)
- Appendix B – Process and Practice Descriptions (Pg. 41 – 295)
- Appendix C – Glossary (Pg. 296 – 322)
- Appendix D – Abbreviations and Acronyms (Pg. 323 – 324)
- Appendix E – Source Mapping (Pg. 325 – 332)
- Appendix F – References (Pg. 333 – 337)
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and is numbered with the reference number.
<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>Level 1 (L1)</th>
<th>PRACTICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO01</td>
<td>AC.1.001</td>
<td>Limit information system access to authorized users, processes acting on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>behalf of authorized users, or devices (including other information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>systems).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FAR Clause 52.204-21 b.1.i</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST SP 800-171 Rev 1 3.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CIS Controls v7.1, 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST CSF v1.1 PR.AC-1, PR.AC-3, PRAC-4, PR.AC-6, PR.AC-8, PR.AT-3,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CERT TRM v1.2 TM.SP4.SP1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AU ACSC Essential Eight</td>
</tr>
<tr>
<td></td>
<td>AC.2.005</td>
<td>Provide privacy and security notices consistent with applicable CUI rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST SP 800-171 Rev 1 3.1.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev 4 AC-8</td>
</tr>
<tr>
<td></td>
<td>AC.2.006</td>
<td>Limit use of portable storage devices on external systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST SP 800-171 Rev 1 3.1.21</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CIS Controls v7.1, 13.7, 13.8, 13.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST CSF v1.1 ID.ATM-4, PR.AT-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev 4 AC-10</td>
</tr>
<tr>
<td>CAPABILITY</td>
<td>PRACTICES</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| C002 Control internal system access | **AC.1.002** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.  
- FAR Clause 52.209-21.1.1  
- NIST SP 800-171 Rev 1 3.1.2  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts.  
- NIST SP 800-171 Rev 1 3.1.5  
- CIS Controls v7.1.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.3.017 Separate the duties of individuals to reduce the risk of malicious activity without collusion.  
- NIST SP 800-171 Rev 1 3.1.4  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.4.023 Control information flows between security domains on connected systems.  
- NIST SP 800-171 Rev 1 3.1.4  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network.  
- NIST SP 800-171 Rev 1 3.1.6  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials |
|                    | **AC.2.008** Use non-privileged accounts or roles when accessing nonsecurity functions.  
- NIST SP 800-171 Rev 1 3.1.6  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.2.009 Limit unsuccessful login attempts.  
- NIST SP 800-171 Rev 1 3.1.8  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.2.010 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.  
- NIST SP 800-171 Rev 1 3.1.8  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.2.012 Protect wireless access using authentication and encryption.  
- NIST SP 800-171 Rev 1 3.1.8  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials |
|                    | **AC.3.018** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.  
- NIST SP 800-171 Rev 1 3.1.7  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.3.019 Terminate (automatically) user sessions after a defined condition.  
- NIST SP 800-171 Rev 1 3.1.17  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.3.020 Secure wireless access using authentication and encryption.  
- NIST SP 800-171 Rev 1 3.1.17  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials |
|                    | **AC.4.025** Periodically review and update CUI program access permissions.  
- NIST SP 800-171 Rev 1 3.1.17  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network.  
- NIST SP 800-171 Rev 1 3.1.17  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials  
- AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network.  
- NIST SP 800-171 Rev 1 3.1.17  
- CIS Controls v7.1.2.4  
- CERT RMF v.2 KIM-SG8 SP1  
- NIST SP 800-53 Rev 4 AC-6(4), AC-6(5)  
- UK NCSC Cyber Essentials |
AC.1.001: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

**DISCUSSION FROM SOURCE: DRAFT NIST SP 800-171 R2**

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged versus non-privileged) are addressed in requirement 3.1.2 (AC.1.002).

**CMMC CLARIFICATION**

Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

**Example 1**

You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

**Example 2**

A coworker from the marketing department tells you their boss wants to buy a new multifunction printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network, and will stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it.

**REFERENCES**
Process to Move Forward

• Assess compliance to NIST SP 800-171, Rev 2
• Develop SSP and POAM
• Determine compliance to CMMC Level 1
  • Either internal or external assessment initially
• Move to comply with all Level 1 requirements
• Once implemented, have external assessment completed
• Move toward certification to CMMC Level 1 compliance
The Georgia Defense Industrial Base (GDIB) Task Force is here to help!

Resources:

Georgia Defense Industrial Base Task Force: https://www.tagonline.org/ga-dibt/

Georgia Department of Economic Development – Cybersecurity EDGE Program: https://www.georgia.org/cybersecurityedge

CMMC-AB Website: https://www.cmmcab.org

The University of Georgia SBDC
“The Trusted Resource for Transforming Georgia Businesses”

Mark R. Lupo, MBA, MBCP, SMP
706-542-2762
mlupo@georgiasbdc.org
https://www.linkedin.com/in/marklupo