Contact List:

John M. Geisler  
Deputy Director  
Michigan Aerospace Manufacturers Association  
Mobile: (248) 444-6303  
Email: john@michman.org  
Website: www.michman.org

Mark A. Montjar  
Brigadier General, US Army Retired  
President  
Arsenal of Democracy Chapter  
Association of the US Army  
Mobile: (248) 640-3472  
mmontjar@charter.net  
bgmark48@gmail.com

Vicki Selva  
Executive Director  
Michigan Defense Center  
(586) 243-6810  
selva@michigandefensecenter.org  
www.ArsenalofInnovation.com

Jess Pellegrino  
President  
Defense Cyber Solutions  
Integrated Cyber Security and Technology Services  
(586) 254-4712  
JessP@defencecybersolutions.net  
www.defencecybersolutions.net

Todd Brady  
Chief Technical Officer  
Defense Cyber Solutions  
Integrated Cyber Security and Technology Services  
(586) 254-4712  
toddB@defencecybersolutions.net  
www.defencecybersolutions.net

Cheryl Burt  
VP of Strategic & Business Development  
Defense Cyber Solutions  
Integrated Cyber Security and Technology Services  
248-760-9687  
cherylB@defencecybersolutions.net  
www.defencecybersolutions.net

Beth A. Cryderman Moss, CFCM, GWCCM  
Program Director  
Macomb Regional Procurement Technical Assistance Center  
(586) 498-4142  
cryderman-mossb@macomb.edu  
www.macomb.edu/ptac | www.ptacofmichigan.org

Vicki Selva  
Executive Director  
Michigan Defense Center  
(586) 243-6810  
selva@michigandefensecenter.org  
www.ArsenalofInnovation.com

Karen Kiewski  
Director of Client Services  
Systems X  
(586) 684-5252  
Karen.Kiewski@Systems-X.com  
www.Systems-X.com

Mike Brattain  
Account Executive  
Systems X  
(586) 884-7835  
Mike.Brattain@Systems-X.com  
www.Systems-X.com
DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT: ASSESSING CONTRACTOR IMPLEMENTATION OF CYBERSECURITY REQUIREMENTS (DFARS CASE 2019–D041)

AGENCY: DEFENSE ACQUISITION REGULATIONS SYSTEM, DEPARTMENT OF DEFENSE (DOD).

ACTION: INTERIM RULE.

November 19, 2020
WHAT IS THE INTERIM RULE CHANGE?

WHY ARE WE DOING THIS?

FOUND ON PAGE 1

“THE COUNCIL OF ECONOMIC ADVISORS ESTIMATES THAT MALICIOUS CYBER ACTIVITY COST THE U.S. ECONOMY BETWEEN $57 BILLION AND $109 BILLION IN 2016. OVER A TEN-YEAR PERIOD, THAT BURDEN WOULD EQUATE TO AN ESTIMATED $570 BILLION TO $1.09 TRILLION DOLLARS IN COSTS.”

(ACCORDING TO THE DOD, THE AVERAGE NUMBER OF BREACHES BEING INVESTIGATED BY THE DOD HAS NOT LOWERED SINCE NIST 800-171 WAS IMPLEMENTED. THIS TELLS THE DOD TOO MANY COMPANIES ARE IN THE POAM STAGE AND HAVEN’T IMPLEMENTED ALL OF THEIR 110 REQUIREMENTS. THE DOD HAS MADE IMPROVED CONTRACTOR CYBERSECURITY A VERY HIGH PRIORITY.)

November 19, 2020
WHAT ARE THE NEW CLAUSES AND WHAT DO THEY MEAN?

THE NEW DFARS PROVISION 252.204–7019 ADVISES OFFERORS REQUIRED TO IMPLEMENT THE NIST SP 800–171 STANDARDS OF THE REQUIREMENT TO HAVE A CURRENT (NOT OLDER THAN THREE YEARS) NIST SP 800–171 DOD ASSESSMENT ON RECORD IN ORDER TO BE CONSIDERED FOR AWARD. (BASIC ASSESSMENT)

THE NEW DFARS CLAUSE 252.204–7020 REQUIRES A CONTRACTOR TO PROVIDE THE GOVERNMENT WITH ACCESS TO ITS FACILITIES, SYSTEMS, AND PERSONNEL WHEN IT IS NECESSARY FOR DOD TO CONDUCT OR RENEW A HIGHER-LEVEL ASSESSMENT (MEDIUM OR HIGH). THE CLAUSE ALSO REQUIRES THE CONTRACTOR TO ENSURE THAT APPLICABLE SUBCONTRACTORS ALSO HAVE THE RESULTS OF A CURRENT ASSESSMENT POSTED IN SPRS PRIOR TO AWARDING A SUBCONTRACT OR OTHER CONTRACTUAL INSTRUMENTS.

November 19, 2020
WHAT'S THE DIFFERENCE BETWEEN BASIC, MEDIUM, AND HIGH ASSESSMENTS?

BASIC IS THE SELF-ASSESSMENT. YOU CONDUCT IT YOURSELF AND UPLOAD YOUR SCORE. MEDIUM AND HIGH MEAN THE GOVERNMENT HAS THE OPTION TO ENTER YOUR FACILITIES AND ASSESS YOUR COMPLIANCE. THE CONTRACT WILL DETERMINE IF YOU REQUIRE BASIC, MEDIUM, OR HIGH ASSESSMENT.

November 19, 2020
IS EVERY COMPANY EXPECTED TO GET A MEDIUM OR HIGH ASSESSMENT FROM THE GOVERNMENT?

FROM PAGE 6 OF THE CLAUSE:

“IT IS EXPECTED THAT THE MEDIUM AND HIGH ASSESSMENTS, ON THE OTHER HAND, WILL BE CONDUCTED ON A FINITE NUMBER OF Awardees each year BASED ON THE CAPACITY OF THE GOVERNMENT TO CONDUCT THESE ASSESSMENTS. DOD ESTIMATES THAT 200 UNIQUE ENTITIES WILL UNDERGO A MEDIUM ASSESSMENT EACH YEAR, OF WHICH 148 ARE EXPECTED TO BE SMALL ENTITIES. HIGH ASSESSMENTS ARE EXPECTED TO BE CONDUCTED ON APPROXIMATELY 110 UNIQUE ENTITIES EACH YEAR, OF WHICH 81 ARE EXPECTED TO BE SMALL ENTITIES.”
IF I DO REQUIRE A MEDIUM OR HIGH ASSESSMENT, WHAT DO I NEED TO KNOW?

FROM PAGE 8:

“(4) HIGH NIST SP 800–171 DOD ASSESSMENTS WILL BE CONDUCTED BY GOVERNMENT PERSONNEL USING NIST SP 800–171A “ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION.” (AKA ASSESSMENT OBJECTIVES)

“UNDER BOTH THE MEDIUM AND HIGH ASSESSMENT DOD ASSESSORS WILL BE REVIEWING THE CONTRACTOR’S SYSTEM SECURITY PLAN DESCRIPTION OF HOW EACH NIST SP 800–171 REQUIREMENT IS MET AND WILL IDENTIFY ANY DESCRIPTIONS THAT MAY NOT PROPERLY ADDRESS THE SECURITY REQUIREMENTS. THE CONTRACTOR PROVIDES DOD ACCESS TO ITS FACILITIES AND PERSONNEL, IF NECESSARY, AND PREPARES FOR/PARTICIPATES IN THE ASSESSMENT CONDUCTED BY THE DOD. UNDER A HIGH ASSESSMENT A CONTRACTOR WILL BE ASKED TO DEMONSTRATE THEIR SYSTEM SECURITY PLAN. DOD WILL POST THE RESULTS IN SPRS.”

November 19, 2020
CAN WE CONDUCT OUR OWN MEDIUM OR HIGH ASSESSMENT?

NO. ONLY THE GOVERNMENT CAN CONDUCT A MEDIUM OR HIGH ASSESSMENT.
WHERE DO WE GET A COPY OF THE SELF-ASSESSMENT DOCUMENT?

HTTPS://WWW.ACQ.OSD.MIL/DPAP/PDI/CYBER/DOCS/NIST%20SP%20800-171%20ASSESSMENT%20METHODOLOGY%20VERSION%201.2.1%206.24.2020.PDF
HOW DOES THE SCORING WORK?

EVERYONE STARTS WITH A SCORE OF 110 AND THEN YOU DEDUCT THE VALUE ASSIGNED TO EACH REQUIREMENT NOT IMPLEMENTED. THEY ARE VALUED AT 1, 3, OR 5 POINTS EACH. TOTAL VALUE OF REQUIREMENTS IS 313 POINTS.

BASED ON HOW MANY YOU HAVE IMPLEMENTED YOU COULD HAVE A NEGATIVE OR POSITIVE SCORE. ONCE ALL 110 REQUIREMENTS ARE IMPLEMENTED YOU WILL HAVE THE PERFECT SCORE OF 110.
**DO I GET POINTS IF I HAVE A POAM (PLAN OF ACTION AND MILESTONE) FOR A REQUIREMENT?**

NO. YOU MUST DEDUCT THE FULL VALUE OF THE POINTS AWARDED TO THAT REQUIREMENT IF IT IS NOT FULLY IMPLEMENTED. YOU GET ZERO POINTS FOR PARTIALLY IMPLEMENTED OR FOR HAVING A POAM.

IT IS A 21 PAGE DOCUMENT. FIRST 11 PAGES ARE INSTRUCTIONS. THEN, THE SCORING TEMPLATE STARTS ON PAGE 12. HERE IS AN EXAMPLE OF THE SCORING TEMPLATE:

<table>
<thead>
<tr>
<th>3.8.9</th>
<th>Protect the confidentiality of backup CUI at storage locations.</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>Screen individuals prior to authorizing access to organizational systems containing CUI.</td>
<td>3</td>
</tr>
<tr>
<td>3.9.2</td>
<td>Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.</td>
<td>5</td>
</tr>
<tr>
<td>3.1.16</td>
<td>Authorize wireless access prior to allowing such connections.</td>
<td>5</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.</td>
<td>3 to 5</td>
</tr>
</tbody>
</table>
WHERE DO WE UPLOAD OUR SCORE?

IN THE SUPPLIER PERFORMANCE RISK SYSTEM (SPRS)

HTTPS://WWW.SPRS.CSD.DISA.MIL/
CAN SCORES BE AMENDED?

YES, THERE IS AN EDIT BUTTON TO ALLOW COMPANIES TO MAKE CHANGES AS NECESSARY TO THEIR EXISTING BASIC SELF-ASSESSMENTS. ANYONE WITH THE “SPRS CYBER VENDOR USER” ROLE ASSOCIATED WITH YOUR COMPANY CAGE IS ABLE TO ENTER AND EDIT ASSESSMENT RESULTS. ONLY THE GOVERNMENT CAN AMEND THE MEDIUM OR HIGH SCORES.
WHAT DO WE HAVE TO UPLOAD?

FROM THE CLAUSE ON PAGE 7:

“TO SUBMIT THE BASIC ASSESSMENT, THE CONTRACTOR IS REQUIRED TO COMPLETE 6 FIELDS: SYSTEM SECURITY PLAN NAME (IF MORE THAN ONE SYSTEM IS INVOLVED); CAGE CODE ASSOCIATED WITH THE PLAN; A BRIEF DESCRIPTION OF THE PLAN ARCHITECTURE; DATE OF THE ASSESSMENT; TOTAL SCORE; AND THE DATE A SCORE OF 110 WILL BE ACHIEVED. ALL OF THIS DATA IS AVAILABLE FROM THE BASIC ASSESSMENT ITSELF, THE EXISTING SYSTEM SECURITY PLAN, AND THE PLANS OF ACTION. THE CONTRACTOR SELECTS THE DATE WHEN THE LAST PLAN ACTION WILL BE COMPLETE AS THE DATE WHEN A SCORE OF 110 WILL BE ACHIEVED.” (ESTIMATED TIME TO UPLOAD IS FIFTEEN MINUTES)
IS THERE ANY GUIDANCE TO HELP US WITH THIS UPLOAD?

YES. GO TO: HTTPS://WWW.SPRS.CSD.DISA.MIL/PDF/SPRS_AWARDEE.PDF.

YOU WILL SEE A COPY OF THE SUPPLIER PERFORMANCE RISK SYSTEM AWARDEE USER GUIDE
OTHER NOTES:

THE INTERIM RULE CURRENTLY REQUIRES CONTRACTING OFFICERS TO ENSURE ONLY THAT CONTRACTORS HAVE A CURRENT ASSESSMENT SCORE ON RECORD IN THE SPRS PRIOR TO AWARD. THE RULE DOES NOT SET ANY NUMERIC THRESHOLD OUT OF THE MAXIMUM SCORE OF 110 OR ESTABLISH WHAT MIGHT BE CONSIDERED A SCORE SO LOW AS TO BE UNACCEPTABLE.

IF A SOLICITATION HAS DFARS CLAUSES 252.204-7019 AND 7020, BUT NO INFORMATION ABOUT HOW THE CONTRACTING OFFICER WILL USE THE ASSESSMENT SCORE, CONTRACTORS SHOULD ASK THE CONTRACTING OFFICER WHETHER AND HOW THE ASSESSMENT WILL BE USED.
OTHER NOTES:

CONTRACTORS SHOULD ACT PROMPTLY TO CONDUCT SELF-ASSESSMENTS AND SET A TIMELINE TO ACHIEVE A PERFECT ASSESSMENT SCORE OF 110. GIVEN THE UNCERTAINTY ABOUT HOW LOWER SCORES WILL BE CONSIDERED IN THE SOURCE SELECTION PROCESS, ACHIEVING FULL COMPLIANCE MAY BE AN EXCELLENT INVESTMENT. FULL COMPLIANCE WILL BE REQUIRED FOR THE CMMC CERTIFICATION.

THIS INTERIM RULE COULD CHANGE BASED ON COMMENTS RECEIVED BY THE DOD BY NOV. 30, 2020. COMPANIES CAN SUBMIT COMMENTS WITH OPINIONS ON HOW TO CLARIFY USE OF THE NIST SP 800-171 ASSESSMENTS. COMMENTS CAN BE SUBMITTED TWO WAYS:
OTHER NOTES:


EMAIL: OSD.DFARS@MAIL.MIL. INCLUDE DFARS CASE 2019–D041 IN THE SUBJECT LINE OF THE MESSAGE.

November 19, 2020
DEFENSE CYBER SOLUTIONS
INTEGRATED CYBER SECURITY AND TECHNOLOGY SERVICES

FOR QUESTIONS, SUPPORT OR SCHEDULE A MEETING
CONTACT - CHERYL BURT- 248-760-9687
CHERYLB@DEFENSECYBERSOLUTIONS.NET
Macomb Regional PTAC

NIST/CMMC & DFARS Case 2019-D041
Resources & Support

Beth A. Cryderman Moss & Kathy Stockman
November 19, 2020
PTAC staff are trained contracting specialists that will help you obtain the most current and relevant information available, provide insight into the research process and coach you through the government contracting process, from start to finish.

- ptcsofmichigan.org
- aptac-us.org
Why is DFARS Case 2019-D041 Interim Rule Important

Role of the PTACs in the NIST/CMMC Landscape

NIST/CMMC Macomb Regional PTAC Fact Sheet
NIST/CMMC & DFARS Case 2019-D041
-Why it’s Important!

- **DFARS Case 2019-D041 Interim Rule is a stop-gap measure until CMMC can be fully implemented**

- **Contractors, beginning 1 Dec 2020, could be at risk of being negatively impacted in the evaluation process for not having a Basic Assessment uploaded to the Supplier Performance Risk System (SPRS).**

- **The good news?! Most of you are at the Basic Level which is a self-assessment of the 110 Controls contained in NIST SP 800-171.**
PTACs are connectors and provide guidance and resources in all things related to government contracting and contract administration (including NIST/CMMC). “One member from each PTAC will actually go to the A.B. (Accreditation Body) -- CMMC classes -- and get certified, so that they're ready as a resource for small businesses.” ~ Katie Arrington, CISO for Acquisition

macomb.edu/PTAC ptacsofmichigan.org aptac-us.org

PTACs are NOT CMMC assessors, auditors, or certifiers. ONLY CMMC Third-Party Assessor Organizations (C3PAOs), accredited by the CMMC Accreditation Body (AB), are authorized to assess, audit, and issue CMMC Maturity Level Certification. CMMCAB.ORG *FOOT STOMP*

ALL DoD suppliers need CMMC Certification by 2025
NIST/CMMC & DFARS Case 2019-D041 - Fact Sheet

NIST SP 800-171 Compliance & CMMC
Defense Industrial Base (DIB) Contractor & Subcontractor Factsheet

https://www.dropbox.com/sh/bqjkn9qv1h2tin8/AADv_Ff37MpCltqiUprJ2ksOa?dl=0
NIST/CMMC & DFARS Case 2019-D041 – In summary

- Don’t get a negative evaluation because your performance information does not include your NIST SP 800-171 Assessment results in SPRS

- Contact your PTAC to get guidance to work through the process

- Refer to the Macomb Regional PTAC “Fact Sheet” as a helpful resource tool
STAY COMPETITIVE IN UNCERTAIN TIMES
NIST/CMMC & DFARS Case 2019-D041 – Questions?
MDC's Cybersecurity Compliance Program

Vicki Selva – Executive Director
MDC's Cybersecurity Compliance Program

PURPOSE:

• Addresses NIST 800-171 and DFARS 252.204-7012 requirements, CMMC rollout

• Provides resources for small and medium sized Michigan companies in the defense supply chain

• Helps make compliance accessible and achievable
MDC's Cybersecurity Compliance Program

PROGRAM DEVELOPMENT:

• Formed CMMC Advisory Committee
  
  Jeff Williams—MMTC
  Cathy Fairbanks—PTAC
  Sharon Chase—US Army
  Tony Giles—NSF
  Michael Zahuranic—BAE
  Jen Tisdale—Grimm
  Sarah Tennant—MEDC
  Ashlee Breitner—UoM EGI
  Jess Pellegrino—Defense Cyber Solutions
  Ken Trumbull-Churchill—Merit
  Jeanne Schabath-Lewis—GDLS

• Conducted digital & phone surveys for NIST 800-171
  
  • Contacted 2,000 Michigan companies to assess awareness, level of compliance, and need for assistance
MDC's Cybersecurity Compliance Program

RESOURCES:
• Prequalified Vendor List
  • Set price for standardized gap analysis
  • Available by January 2021
• BTS integration with Learning Module and Vendor Page
  • Available by January 2021
What is the relationship between NIST SP 800-171 and CMMC?
The intent of the CMMC is to combine various cybersecurity control standards such as NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933 and others into one unified standard for cybersecurity. In addition to cybersecurity control standards, the CMMC will also measure the maturity of a company’s institutionalization of cybersecurity practices and processes.

How will CMMC be different from NIST SP 800-171?
CMMC will implement 5 maturity levels of cybersecurity. In addition to assessing the maturity of a company’s institutionalization of cybersecurity controls, the CMMC will also assess the company’s maturity/ institutionalization of cybersecurity practices and processes. Reference: https://www.acq.osd.mil/cmmc/faq.html

NIST SP 800-171 Compliance
Effective date: Dec. 31, 2017

Types of Information protected:
- Controlled Unclassified Information (CUI)
- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)

CMMC v1.02 Certification
Website: https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf
Effective date: Jan. 2020 (5-year roll-out)

Types of Information protected:
- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)
- Controlled Unclassified Information (CUI)

<table>
<thead>
<tr>
<th>Families (14)</th>
<th>Security Requirements Basic &amp; Derived (110)</th>
<th>Domains (17)</th>
<th>Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1: Access and Control</td>
<td>22</td>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td>3.2: Awareness and Training</td>
<td>3</td>
<td>Awareness and Training</td>
<td></td>
</tr>
<tr>
<td>3.3: Audit and Maintenance</td>
<td>9</td>
<td>Audit and Accountability</td>
<td></td>
</tr>
<tr>
<td>3.4: Audit and Accountability</td>
<td>9</td>
<td>Configuration Management</td>
<td></td>
</tr>
<tr>
<td>3.5: Identification and Authentication</td>
<td>11</td>
<td>Identification and Authentication</td>
<td></td>
</tr>
<tr>
<td>3.6: Incident Response (IRP)</td>
<td>3</td>
<td>Incident Response</td>
<td></td>
</tr>
<tr>
<td>3.7: Maintenance</td>
<td>6</td>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>3.8: Media Protection</td>
<td>9</td>
<td>Media Protection</td>
<td></td>
</tr>
<tr>
<td>3.9: Personnel Security</td>
<td>2</td>
<td>Personal Security</td>
<td></td>
</tr>
<tr>
<td>3.10: Physical Protection</td>
<td>6</td>
<td>Physical Protection</td>
<td></td>
</tr>
<tr>
<td>3.11: Risk Assessment</td>
<td>3</td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td>3.12: Security Assessment (SSP &amp; PoAM)</td>
<td>4</td>
<td>Security Assessment</td>
<td></td>
</tr>
<tr>
<td>3.13: System and Communications Protection</td>
<td>16</td>
<td>System and Communication Protection</td>
<td></td>
</tr>
<tr>
<td>3.14: System and Information Integrity</td>
<td>7</td>
<td>System and Information Integrity</td>
<td></td>
</tr>
</tbody>
</table>

Basic Security Requirements provide a high-level & fundamental security requirement for federal information based on Federal Information Processing Standards (FIPS) Publication 200 and Derived Security Requirements supplement the Basic and are taken from security controls in NIST SP 800-53. The combination of the two captures the intent to protect CUI in nonfederal systems and organizations.

A Discussion Section is found after each 110 Security Requirements & provides organizations with a better understanding of the mechanisms & procedures used to implement the Security Requirements to protect CUI. It is NOT meant to influence the solutions organizations use to satisfy the requirements. The Discussion Section information is derived from the Security Controls Discussion Sections in NIST SP 800-53.

See NIST SP 800-171:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- Pages 10 – 43 for detailed information on Families (14); and Security Requirements (110) and Discussions.

5 Maturity Levels (ML)
ML 1: Safeguard Federal Contract Information (FCI)
- Process: **Performed**
  - Requires organization perform specified practices, may or may not rely on documentation, process maturity not assessed for level 1.
- Practice: Basic Cyber Hygiene Practice
  - Corresponds to basic safeguarding requirements in 48CFR 52.204-21 (Basic safeguarding of Covered Contractor Information Systems).
ML 2: Serve as Transition step in cybersecurity maturity progression to protect CUI.

- **Process:** Documented
  - Requires organization establish and document practices and policies to guide implementation of their CMMC efforts.

- **Practice:** Intermediate Cyber Hygiene
  - Serves as a progression from Level 1 to Level 3 & consists of subset of the security requirements specified in NIST SP 800-171 as well as practices from other standards and references. Represents a transition state and a subset of the practices reference the protection of CUI.

ML 3: Protect Controlled Unclassified Information (CUI).

- **Processes:** Managed
  - Requires an organization establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. Plan may include information on missions, goals, project plans resourcing, required training and involvement of relevant stakeholders.

- **Practices:** Good Cyber Hygiene
  - Focuses on protection of CUI and encompasses all the security requirements specified in NIST SP 800-171 including additional practices for standards and references to mitigate threats.
  - DFARS 252.204-7012 (Safeguarding of Covered Defense Information and Cyber Incident Reporting specifies additional requirements beyond the NIST SP 800-171 security requirements such as incident reporting.

<table>
<thead>
<tr>
<th>Total Security Requirements for NIST SP 800-171</th>
<th>110</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Practices for CMMC ML 3 Certification (“NIST SP 800-171” 110 + 20 “Others”)</td>
<td>130</td>
</tr>
</tbody>
</table>

ML 4: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

- **Processes:** Reviewed
  - Requires an organization review and measure practices for effectiveness, take corrective action when necessary and inform higher level management of status of issues on a recurring basis.

- **Practices:** Proactive
  - Focus on protecting of CUI from APTs & encompasses a subset of the enhance security requirements from Draft NIST SP 800-171B as well as other cybersecurity best practices. Practices enhance the detection & response capabilities of an organization to address and adapt to changing tactics, techniques, and procedures (TTPs) used by APTs.


| Total Practices for CMMC ML 4 Certification | 156 |
### Steps to become NIST SP 800-171 Compliance:

- Do it yourself or hire a vendor.

1. Develop a System Security Plan (SSP)
   - See actual document page 6, pages 6 – 144.
   - Assessment Results for each 110 Security Requirements company answers:
     - Yes - a statement should be in SAR and SSP which explains how the information system implements the requirement
     - No - a statement should be in the SAR explaining why requirement not met and be included in the PoAM that describes how it will be met.
     - Partially - a statement should be in SAR why partially met and a statement in the PoAM explaining how it will be fully met and when.
     - Doesn’t Apply - a statement should be in the SAR explaining why it does not apply to company’s operational environment.
   - Alternative Approach – a statement should be in SAR and SSP fully describing the alternative approach and how it is equally effective as well as a statement that explains how the info. system implements the requirement.
   - List of Plans, Policies and Procedures you should have in place.
     See actual document page 6, pages 157 – 159.

2. Develop a System Security Plan (SSP)
   - Ref. 3.12 Security Assessment (Security Reqs 1, 3, 4)
   - SSP includes System Identification, System Environment, and Requirements (110 Security Reqs). See SSP template (this takes a few seconds to load so be patient):
   - Periodically assess the 110 Security Reqs in organizational systems to determine effectiveness.
   - Assessment includes how the 110 Security Reqs are being implemented or planned to be implemented. If it’s not applicable a rationale must be included.
   - Effective SSP’s reference policies, procedures and additional documents where detailed information can be found.

3. Develop a Plan of Action with Milestones (PoAM):
   - Ref. 3.12.2 Security Assessment (Security Req 2)
   - Describe how unimplemented Security Requirements will be met and when.
   - PoAM Template:
   - The SSP and PoAM can be combined documents or separate documents.

### ML 5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

- Process: Optimizing
- Requires organization to standardize and optimize process implementation across the organization.
- Practice: Advanced/Proactive
- Focus on protection of CUI from APTs.
  - Additional practices increase the depth and sophistication of cybersecurity capabilities
- ML 5 Domains & Practice pages 12-22:
  https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

### Total Practices for CMMC ML 5 Certification

### Steps for CMMC Certification Preparation:

- Do it yourself or hire a vendor.

1. Become NIST SP 800-171 Compliant.

2. If your goal is to get certified as CMMC Level 3:
   - Add the 7 “Other” Practices from Level 2, and the 13 “other” Practices from Level 3 for a total of 20 “Other” Practices to your SSP and PoAM.
   - Result 110 Security Requirements from NIST SP 800-171 plus the 20 “Other” Practices mentioned in CMMC equals the 130 Practices for Level 3 Certification.
   - For more information see CMMC Public Briefing slide #9:
     https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf
   - Mapping to “Other” 20 Practices. See yellow highlighted Excel Workbook tabs and cells:
     https://www.dropbox.com/s/2cgjiit8dfz6z82f5/Other%20%20Controls_CMCMCModelExcel_V1.02.xlsx?dl=0
   - Mapping Level 3 focus:

### What is the CMMC Accreditation Body (AB)?

- The AB is a non-profit, independent organization that will accredit CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors as well as establish a CMMC Marketplace that will include a list of approved C3PAOs and other information. After the CMMC Marketplace is established businesses will be able to select one of the approved C3PAOs and schedule a CMMC assessment for a specific ML: https://www.cmmcab.org/
- Ecco System Timeline:
  https://mcusercontent.com/6e7d7963b1219eb1b0fbda703/files/543677c7b865-e92fd4fa8c/Accreditation_Ecosystem.pdf

### How does your business get certified?

- C3PAO: https://www.cmmcab.org/c3pao-lp
- Assessors: https://www.cmmcab.org/assessors-lp
  - Certified Professional (CP) is authorized to participate on a team under the supervision of a Certified Assessor (CA).
  - CA is credentialed as a CA-1, CA-3 or CA-5 to conduct applicable CMMC ML Assessments.
- Registered Provider Organization (RPO): https://www.cmmcab.org/rpo
  - Deliver non-certified CMMC Consulting Services.
- Registered Practitioner (RP): https://www.cmmcab.org/registered-practitioners
  - Delivers non-certified advisory service informed by basic training on the CMMC standard.
- Note: Assessment and Consultative Services may not be delivered to the same client by the same C3PAO.
- C3PAOs and Assessors have not been identified yet therefore you can NOT get your CMMC ML Certification, but you can prepare for it.
4. Develop an Incident Response Plan (IRP):
   - Reference 3.6 Incidence Response (Security Req 3)
   - Establish operational incident-handling capability for organizational systems.
   - Track, document and report incidents internally and externally. Per DFARS 252.204-7012 an incident must be reported within 72 hours on the DoD Defense Industrial Base (DIBNet) Reporting System: https://dibnet.dod.mil/portal/intranet/
   - You do not need to apply to the DIB Cybersecurity (CS) Program, but a Medium Assurance Certificate from a DoD approved vendor is required to report a Cyber Incident. Visit here to learn more: https://public.cyber.mil/eca/.
   - It may take a couple days to get your Medium Assurance Certificate, so it is recommended you get one before you have an incident to report.
   - Test organizational incident response capability.

5. Complete a NIST SP 800-171 DoD Basic Self-Assessment and post in the Supplier Performance Risk System (SPRS) on or after Nov. 30, 2020.
   - See DFARS Interim Rule Case 2019-D041 below to learn more.

---

**Defense Federal Acquisition Regulation Supplement (DFARS) Interim Rule**
**Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)**

1. **What is the Interim Rule?**
   The interim rule amends the Defense Federal Acquisition Regulation Supplement (DFARS) to build upon the existing DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. It allows the government to evaluate federal government contractors and subcontractor’s implementation of cybersecurity requirements and enhances the protection of CUI. The NIST SP 800-171 assessment requirement consists of 3 levels Basic/Medium/High. Additionally, assessments must be posted in the Supplier Performance Risk System (SPRS). This rule is intended to serve as an interim certification process before contractors undergo a full CMMC review.
   - **Effective date:** Nov. 30, 2020 – Sept. 30, 2025
     - What happens after Oct. 1, 2025: All DoD solicitations and contracts valued at greater than the micro-purchase threshold will identify the required CMMC level and contain new DFARS clause 252.204-7021. This clause does not apply to contracts exclusively for COTS items.
   - **Exemptions:**
     - Commercial Off the Shelf (COTS) Items
     - Contracts or orders valued below the Micro-Purchase Threshold.
   - **The interim rule consists of two items:**
     - A new assessment framework which the DoD will roll out immediately (DFARS 252.204-7019-7020).
     - The new CMMC which the DoD will roll out over the next five years (DFARS 252.204-7021).
       - Solicitations will state what CMMC Maturity Level is required and Prime Contractors will need to flow this clause down to their Subcontractors and ensure they have the appropriate CMMC Maturity Level.

2. **What to look for in Contracts and Subcontract flow downs:**
   Contracting officers will implement the DoD assessment requirement by including two new DFARS clauses in all DoD solicitations, task orders, delivery orders and contracts except those solely for the acquisition of COTS items.
   - DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
     - Sets a requirement for an assessment of NIST 800-171 from Nov. 30, 2020 onward. Building off the DCMA program, it will act as the bridge to CMMC over the coming years.
     - Assessments fall into three categories:
       1) Basic (self-assessment)
         - Resulting in a “low” level of confidence in the resulting score.
         - Valid for 3 years.
       2) Medium (conducted by the Government i.e. DCMA)
         - After a contract is awarded, DoD may choose to conduct a Medium Assessment of an offer based on the criticality of the program or the sensitivity of information being handled by the contractor and DoD will post the results in SPRS.
         - Includes a review of the contractor’s Basic Assessment, a “thorough document review,” and discussions between the DoD and the contractor to obtain additional information or clarification, as needed.
         - Contractors must provide the DoD access to their facilities, systems and personnel as needed to conduct the assessment.
         - Resulting in a “medium” level of confidence in resulting score.
         - Valid for 3 years.
       3) High (conducted by the Government i.e. DCMA)
         - After a contract is awarded, DoD may choose to conduct a High Assessment of an offer based on the criticality of the program or the sensitivity of information being handled by the contractor and DoD will post the results in SPRS.
         - Consists of a Medium Assessment, plus verification, examination and demonstration of a contractor’s system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the plan.
         - Contractors must provide DoD access to their facilities, systems and personnel as needed to conduct the assessment.
         - Resulting in a “high” level of confidence in resulting score.
         - Valid for 3 years.

---

**How often does a business need to be reassessed?**
- Every 3 years.

**Specific Certification Levels will NOT be made Public.**

**For more Frequently Asked Questions on CMMC:**
https://www.acq.osd.mil/cmmc/faq.html
5. Reporting the Assessment and Rebuttals:
   - DFARS 252-204-7020 NIST SP 800-171 DoD Assessment Requirements
     - This clause has two requirements:
       1. Requires Contractors to provide access to “facilities, systems, and personnel” in order to conduct/renew higher-level assessment.
       2. Requires the Contractor to ensure subcontractors also have results of a current assessment posted in SPRS prior to awarding a subcontract or other contractual instrument such as a PO.
   - DFARS clause (252.204-7021) Cybersecurity Maturity Model
     - States inclusion of a CMMC maturity level requirement in a solicitation/contract during the time period Nov. 30, 2020 – Sept. 30, 2025 must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment and will be flowed down to Subcontractors at all tiers based on the sensitivity of the CUI flowed down to each Subcontractor.
     - Requires CMMC Certification at the time of award.
     - Awardees must maintain the required CMMC level for the duration of the contract.
     - Options may only be exercised after verifying the contractors CMMC level when CMMC is required in the contract.
     - Prime Contractor must ensure its Subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instrument such as a PO.
   - DoD intends to apply the new provision and clauses to contacts and subcontracts for the acquisition of commercial items and to acquisitions valued at or below the SAT but great than the micro-purchase threshold.
   - The provision and clauses will not be applicable to contracts or subcontracts exclusively for the acquisition of Commercial Off the Shelf (COTS) items.

3. What do Prime Contractors and Subcontractors need to do?
   Prime Contractors, subcontractors and their lower tiered subs that have or will have access to CUI need to complete a Department of Defense (DoD) NIST SP 800-171 Basic/Medium/High Assessment with respect to each system being assessed. The results of the Assessment need to be documented in SPRS on or after Nov. 30, 2020 to provide Contracting Officers with visibility into their scores, and to verify that an offeror has a current (not less than 3 years old, unless a lesser time is specified in the solicitation) NIST SP 800-171 Assessment on record prior to any contract award that involves CUI.
   - Conduct a NIST SP 800-171 DoD Basic Self-Assessment (unless a Medium/High Assessment is required)
     - NIST SP 800-171 DoD Assessment Methodology Version 1.2.1 dated June 24, 2020:
       - Documents a standard methodology that enables a strategic assessment of a contractor’s implementation of NIST SP 800-171.
       - NIST SP 800-171 DoD Assessment Scoring Template for Basic/Medium/High Assessments see Annex A, pages 12 – 20.
       - Basic Self-Assessment Results Format see Annex B, page 21.
     - Project Spectrum NIST SP 800-171 Cyber Readiness Check Self-Assessment Tool can be used to get your score by completing the on-line form (you may need to copy and paste link in Chrome): https://projectspectrum.io/#/!
     - Sign-up first to access the Cyber Readiness Check tool (copy and paste link in Chrome): https://projectspectrum.io/#/register
     - There are also 3 other Cyber Readiness Check Tools available: CMMC Level 1, 2 and 3.
   - Create an account in the Procurement Integrated Enterprise Environment (PIEE) if you don’t have one already: https://piee.eb.mil/piee-landing/
   - Enter your Basic-Self Assessment in SPRS: https://www.sprs.csd.disa.mil/
   - Data to be entered in SPRS:
     - System Security Plan Name
     - Commercial and Government Entity (CAGE) code
     - Brief description of plan architecture
     - Date of the Assessment
     - Total score
     - Date that a score of 110 will be achieved
   - Basic-Self Assessment is valid for 3 years.

4. Assessment Scoring:
   - All levels of the NIST 800-171 DoD Assessment Methodology use the same scoring system.
     - A score of 110 represents full implementation of the NIST SP 800-171 controls, regardless of the method of implementation.
     - Deductions from 110 are made for each control not implemented at the time of the assessment, with weights assigned to different controls.
     - More points are deducted for those controls deemed to have a greater impact on the overall security risk posed by the contractor’s information system.
   - The Interim Rule does not prescribe a minimum score to be eligible for award.

5. Reporting the Assessment and Rebuttals:
   - Contractors and subcontractors are responsible for reporting the results of a Basic Self-Assessment in SPRS.
   - DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (DoD will post the score in SPRS). See SPRS User's Guide: https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.
     - Upon completion of each government assessment, the Contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.
   - Takes 30 days to post scores to the SPRS, so plan ahead to avoid any potential award delays.

6. Viewing Assessment Score:
   - Authorized representatives of the offeror for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User’s Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.
   - Contracting officers shall use SPRS (https://www.sprs.csd.disa.mil/) to verify an offeror or contractor's Assessment Score.
**Take away:** How your company is postured for cybersecurity is going to affect your bottom line because those who do it right, will be in a much better competitive position.

### Additional Resources

**Procurement Technical Assistance Centers:** [https://www.aptac-us.org/](https://www.aptac-us.org/)

**PTACS of MI:** [http://www.ptacofmichigan.org/offices/](http://www.ptacofmichigan.org/offices/)

**Defense Cybersecurity Assurance Program (DCAP):** For assistance identifying **Cybersecurity resources such as vendors / potential funding opportunity** visit the Defense Cybersecurity Assurance Program (DCAP): [https://economicgrowth.umich.edu/dcap/](https://economicgrowth.umich.edu/dcap/) or contract Stephanie at: stludwig@umich.edu.

**The Michigan Manufacturing Technology Center (MMTC):** The Michigan Manufacturing Technology Center works with manufacturers to help them accelerate their business growth and sustain success into the future. We help companies analyze new and existing technology to develop a framework for secure business operations. To learn more: [https://www.the-center.org/Our-Services/Cybersecurity-Services](https://www.the-center.org/Our-Services/Cybersecurity-Services)

**Cyber Collaboration Center:** The Cyber Collaboration Center has established partnerships with industry to assist in building awareness and providing educational resources for contractors striving to meet DoD cybersecurity requirements. CCC has sponsored a series of webinars and live training events to provide training and information for prime contractors, subcontractors, and government contracting professionals. To learn more: [https://www.cybercollaborationcenter.org/](https://www.cybercollaborationcenter.org/)

**Project Spectrum:** Part of the Cyber Integrity Initiative (CI2) - and supported by the Department of Defense’s (DoD) Office of Small Business Programs (OSBP) - Project Spectrum is the definitive platform to strengthen the cybersecurity of small and medium sized businesses, as well as universities. Project Spectrum provides resources, information, training, and risk assessments to help companies and institutions improve cyber readiness and comply with DoD requirements. To learn more (you may have to copy and paste link in Chrome): [https://www.projectsp orum.io/](https://www.projectsp orum.io/)

**The Georgia Tech Procurement Assistance Center (GTPAC):** Released a cybersecurity training video along with related resource materials that provide step-by-step instructions for government contractors on how to comply with DoD's cybersecurity requirements, specifically Defense Federal Acquisition Regulation Supplement (DFARS) clause 204-73 (252.204-7012), "Safeguarding Covered Defense Information and Cyber Incident Reporting." The video and additional resource materials can be viewed at: [http://gtpac.org/cybersecurity-training-video](http://gtpac.org/cybersecurity-training-video)

**DoD Cybersecurity Fact Sheets, Presentations, Videos:** [http://dodprocurementtoolbox.com/site-pages/cybersecurity-other-resources](http://dodprocurementtoolbox.com/site-pages/cybersecurity-other-resources)

**NIST has partnered with Manufacturing Extension Program (MEP):** [https://www.nist.gov/mep/cybersecurity-resources-manufacturers](https://www.nist.gov/mep/cybersecurity-resources-manufacturers)


**The National Archives:** Video on Controlled Unclassified Information (CUI) as it relates to cybersecurity issues. [https://www.youtube.com/watch?v=zA03yDnNxm0&feature=youtu.be](https://www.youtube.com/watch?v=zA03yDnNxm0&feature=youtu.be)

**Imprimis:** Cybersecurity training videos that deals with making the case or justifying a cyber program to executives and management. There are 2 videos on this page on this topic - *Justifying a Cybersecurity Program & Cyber for Executives*. Good messages about a strong cyber program as a competitive advantage, a fiduciary responsibility, an ROI, and a way to minimize risk: [https://www.imprimis-inc.com/8-imprimis-web/36-insider-webinar-gallery](https://www.imprimis-inc.com/8-imprimis-web/36-insider-webinar-gallery).