Dr. Michael Wojcik

Protecting DoD CUI in Nonfederal Systems

Cybersecurity & Compliance

SBIR/STTR Innovation Summit

Embracing Innovation, Science, and Technology to Outpace the Threat

Approved for Public Release
21-MDA-10783 (20 Apr 21)
“For mission owners, the primary goal of DoD must be to deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded or inappropriately given way or sold.”

William Stephens, Former Director of Counterintelligence, DSS

“Adversaries will continue to use cyber operations to undermine U.S. military and commercial advantage by hacking into U.S. defense industry and commercial enterprises in pursuit of scientific, technical, and business information.”

Dan Coats (May 2017), Former Director of National Intelligence
If a contractor does not agree or is unable to comply with the terms of DFARS Clause 252.204–7012, then controlled unclassified information (CUI) shall not reside on the contractor’s information system.

DFARS Clause 252.204-7012 (Dec 2019) - Requirements

Requires the contractor/subcontractor to:

1. **Provide adequate security.** Mandates implementation of NIST SP 800-171.
2. Rapidly report cyber incidents to DIBNet (https://dibnet.dod.mil/)
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
4. Submit media/information as requested to support damage assessment activities
5. **Flow down the clause in subcontracts** for operationally critical support, or for which subcontract performance will involve covered defense information
Nonfederal Systems Cybersecurity Updates

• NIST SP 800-171 Rev.2 (updated 01/28/21)
  — Includes 5 administrative changes (characterized by author as “editorial”)
  — No other significant or material adds/deletes

• DFARS: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)
  — Interim rule published 09/29/20 and effective 11/30/20
    • Composed of historical information, cost projections associated with DoD and CMMC assessments.
    • Introduced DFARS 252.204-7019, 7020 and 7021
  — Final rule expected in Aug/Sep 2021 timeframe

• DoD Assessments
  — NIST SP 800-171 (Rev.2) assessments (aka DIBCAC assessment)
    • 110 security requirements
    • DFARS 252.204-7012, 7019, and 7020 apply to DoD assessments
    • DFARS 7012 – requires application of NIST 171 requirements and CUI protection (more info on back-up slide 7)
    • DFARS 7019 – requires assessment entry in Supplier Performance Risk System (SPRS)
    • DFARS 7020 – authorizes government to conduct onsite assessments at DIB partner facility
Interim Rule DFARS Case 2019-D041 Assessing Contractor Implementation of Cybersecurity Requirements

Purpose: Implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework

<table>
<thead>
<tr>
<th>DoD Assessment Methodology</th>
<th>Cybersecurity Maturity Model Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amendment of DFARS Subpart 204.73 Safeguarding Covered Defense Information and Cyber Incident Reporting to implement NIST SP 800-171 DoD Assessment Methodology</td>
<td>New DFARS Subpart 204.75 Cybersecurity Maturity Model Certification (CMMC)</td>
</tr>
<tr>
<td>Created new DFARS Provision 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements</td>
<td>• Created new DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirements</td>
</tr>
<tr>
<td>Created new DFARS Clause 252.204-7020 NIST SP 800-171 DoD Assessment Requirements</td>
<td>Contracting Officer is directed to</td>
</tr>
<tr>
<td>Contracting Officer is directed to</td>
<td>• Include 252.204-7021 and required CMMC level in solicitation and contract</td>
</tr>
<tr>
<td>• Include 252.204-7019 in solicitations</td>
<td>• Verify in SPRS that offeror has current CMMC certification at required level prior to award of contract, option or extension</td>
</tr>
<tr>
<td>• Include 252.204-7020 in solicitations and contracts</td>
<td>Effective:</td>
</tr>
<tr>
<td>• Verify in SPRS that offeror has current NIST SP 800-171 Assessment on record prior to award of contract, option or extension when 252.204-7012 is required</td>
<td>As stated in 204.7503</td>
</tr>
<tr>
<td>Effective: 30 November 2020</td>
<td>• 30 Nov 2020 - 30 Sep 2025, OUSD(A&amp;S) must approve use of clause 252.204-7021 [CMMC Pilots]</td>
</tr>
<tr>
<td></td>
<td>• After 1 Oct 2025, clause 252.204-7021 must be included in all applicable contracts*</td>
</tr>
</tbody>
</table>

Between 30 Nov 2020 - 30 Sep 2025, OUSD(A&S) must approve the use of clause 252.204-7021

This initial five year period is for approved CMMC Pilots only

* Interim provisions and clauses are applicable to contracts, task orders and delivery orders. Not applicable to micro-purchases or solicitations exclusively for the purchase of COTS products
The objective of the NIST SP 800-171 Compliance Assessment is to determine whether the contractor has implemented the NIST SP 800-171 security requirements.

Not intended as a value judgement about specific approaches to requirement implementation or an assessment of one solution compared to another.

- Solutions that meet the requirements are acceptable.
- Scoring methodology is designed for an objective assessment of security requirements implemented and not yet implemented.

Achievable scores range from 0 (no SSP) to 110 (all requirements met).

Scores remain a matter of record until a subsequent assessment is performed.

Scores recorded in the DoD Supplier Performance Risk System (SPRS): https://www.sprs.csd.disa.mil/
CMMC (Full Implementation Oct 2025)

- CMMC is a DoD Certification process that measures a DIB sector company’s ability to protect Federal Contract Information (FCI) and CUI
- CMMC combines various cybersecurity standards and maps these best practices and processes to maturity levels, ranging from basic cyber hygiene to highly advanced practices
- CMMC builds upon the NIST SP 800-171 security requirements
- Provides improved cybersecurity protections
- DFARS 252.204-7021 implements CMMC

<table>
<thead>
<tr>
<th>Level</th>
<th>Level Title</th>
<th># of Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Basic Cyber Hygiene</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>Intermediate Cyber Hygiene</td>
<td>72</td>
</tr>
<tr>
<td>3</td>
<td>Good Cyber Hygiene</td>
<td>130</td>
</tr>
<tr>
<td>4</td>
<td>Proactive</td>
<td>156</td>
</tr>
<tr>
<td>5</td>
<td>Advanced / Progressive</td>
<td>170</td>
</tr>
</tbody>
</table>

Approved for Public Release 21-MDA-10775 (15 Apr 21)
CMMC

• **CMMC Implementation**
  – MDA continues review of CMMC implementation requirements
  – MDA co-hosted CMMC Pathfinder/Tabletop Exercises in 2020
  – DFARS 252.204-7021 approved for use in 12 OUSD(A&S)-CMMC Pilots DoD-wide

• **NIST SP 800-172, Enhanced Security Requirements for Protecting CUI: A Supplement to NIST SP 800-171**
  – Published 02/02/21
  – Focused on protection against Advanced Persistent Threat
  – Applies to information systems associated with critical programs or high value assets
  – Expected to be the basis for many of the practices and process for CMMC Level 4/5
Backup
Questions?

MDA Strategic Cyber Council
MDACyber

Headquarters MDA
5700 18th Street, Building 245
Fort Belvoir, VA 22448-5148

571.231.8496
256.450.4477

MDACybersec-acq@mda.mil

MDAU Net
What MDA is Doing to Enhance DIB Cybersecurity

- Ensuring Contractor Compliance of FAR clause 52.204-21 and DFARS clause 252.204-7012 to safeguard Controlled Unclassified Information (CUI) on non-federal systems
- Executing joint MDA-DCMA DIB cyber assessment IAW NIST SP 800-171A
- Preparing for CMMC Implementation
  - Participating in OUSD(A&S)-CMMC Pilots
- DoDI 5200.48 and CUI Implementation
- Working with Industry Partners to promote cyber threat awareness through information sharing and collaboration
- Implementing the Information Management Control Plan (IMCP)
  - Addresses: Where is MDA CUI, and how is it protected?
- Utilizing MDA Cyber Assistance Team (CAT)
- Piloting several efforts to assist with securing MDA CUI
  - Assisting partners in the development of SSPs and Plan of Action and Milestones
- Adding Cybersecurity provisions in the Source Selection process
- Adding evaluation of Cybersecurity operations into CPARS
- Adding Software Assurance in applicable MDA contracts
- Leading DoD pathfinder working to improve overall MDA cyber hygiene
The *interim rule* took effect 30 Nov 2020 / DoD implementing a 5-year phased roll-out

**DFARS Provision 252.204-7019**
Notice of NIST SP 800-171 DoD Assessment Requirements

<table>
<thead>
<tr>
<th>Solicitation Notice: Basic Assessment Score required in SPRS for contract award</th>
</tr>
</thead>
<tbody>
<tr>
<td>A NIST SP 800-171 DoD Assessment (Basic, Medium, High) summary level score must be posted into DoD’s Suppliers Risk Performance System (SPRS) for the applicable CAGE code and Systems Security Plan</td>
</tr>
<tr>
<td>The summary level score must remain current (not older than 3 years unless a lesser time is specified) throughout the life of the contract, task or delivery order</td>
</tr>
</tbody>
</table>

**DFARS Clause 252.204-7020**
NIST SP 800-171 DoD Assessment Requirements

<table>
<thead>
<tr>
<th>Basic Assessment Score required in SPRS to be considered for contract award</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable to companies subject to DFARS clause 252.204-7012</td>
</tr>
<tr>
<td>Post award, if DoD deems a Medium or High assessment is necessary due to program sensitivity, provide DoD access to facilities, systems and personnel</td>
</tr>
<tr>
<td>Include clause in all subcontracts or other contractual instruments including subcontracts for commercial items</td>
</tr>
<tr>
<td>Confirm subcontractor compliance with SPRS reporting if receiving CUI</td>
</tr>
</tbody>
</table>

**DFARS Clause 252.204-7021**
Cybersecurity Maturity Model Certification Requirements

<table>
<thead>
<tr>
<th>Cybersecurity Maturity Model Certification Required by contract award effective 1 Oct 2025</th>
</tr>
</thead>
<tbody>
<tr>
<td>Until 1 Oct 2025, OUSD(A&amp;S) must approve clause in new acquisitions</td>
</tr>
<tr>
<td>Contractor certification level must be maintained for contract duration</td>
</tr>
<tr>
<td>Clause must be flowed down; primes must ensure subs are certified at required CMMC level prior to awarding subcontract</td>
</tr>
</tbody>
</table>

**CMMC assessments and certifications required for the applicable enterprise network or network segment where FCI or CUI will be processed, stored, or transmitted in performance of the contract**