



Breaking CMMC news

July 25, 2023

CMMC Rule moves to Office of
Management & Budget (OMB)

< 90-day review prior to publish
to Federal Register

<https://www.reginfo.gov/public/do/eoDetails?rrid=324614>

An official website of the United States government

 **OFFICE of INFORMATION and REGULATORY AFFAIRS**
OFFICE of MANAGEMENT and BUDGET
EXECUTIVE OFFICE OF THE PRESIDENT

Reginfo.gov

U.S. General Services Administration 

Search: Agenda Reg Review ICR

[Home](#) | [Unified Agenda](#) | [Regulatory Review](#) | [Information Collection Review](#) | [FAQs / Resources](#) | [Contact Us](#)

Pending EO 12866 Regulatory Review

RIN: [0790-AL49](#) [View EO 12866 Meetings](#)
Title: Cybersecurity Maturity Model Certification (CMMC) Program
Agency/Subagency: DOD / OS
Legal Deadline: None
International Impacts: No
Pandemic Response: No

Received Date: 07/24/2023
Stage: Proposed Rule
Section 3(f)(1) Significant: No
Affordable Care Act [Pub. L. 111-148 & 111-152]: No
Dodd-Frank Wall Street Reform and Consumer Protection Act, [Pub. L. 111-203]: No

https://www.linkedin.com/posts/robertmetzger_pentagon-cyber-certification-program-rulemaking-activity-7089616165831905280-Aafd?utm_source=share&utm_medium=member_desktop



Robert Metzger • 1st

Attorney | Procurement Law, Cyber & Supply Chain | National Security Matters | ...

18m • 

Big news. OMB has up to 90 days to complete its review, though the time could be less. Once OIRA is satisfied, and assuming that the rule is not sent back to DoD for further consideration, the Proposed Rule will be published in the Federal Register. If OIRA was to complete its review in 60 days, we could see the NPRM published before Oct. 1, 2023. The 90th day, by my count, will be October 27, 2021.

It has taken DoD much time and great effort to get the rule package to OIRA. While we in the CMMC community don't know the rule content, that the rulemaking has moved to the OIRA review stage should communicate to all concerned that CMMC is coming.

insidecybersecurity.com • 1 min read

Pentagon cyber certification program rulemaking enters formal interagency review process at OIRA >

The Pentagon's Cybersecurity Maturity Model Certification program is entering a new stage wi...

NIST SP 800-171 Rev.3

Noteworthy Feedback

<https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information/sp-800-171/comments-draft-sp-800-171-r3>

Submitted by: DOD CIO

Topic: Organization Defined Parameters (ODPs)

The use of ODPs while providing flexibility for Federal organizations that choose to establish non-standard formulations for use in their specific contracts ultimately renders the 171r3 neither a standard nor scalable. Scalability is crucial to implementation of these requirements at the contractor level. The ODP construct means that a contractor with 1 000 contracts may have 1 000 different implementations they are required to meet simultaneously many on the same enterprise network. Even if said contractor took the approach of meeting the most stringent version of each requirement they would likely need to employ fulltime staff just to track the requirements across contracts and determine which version of each requirement to meet and when to change implementations in real time as new contracts are acquired. Contractors would still run the risk of a government organization rejecting that approach and insisting on implementation of their exact ODP thus "breaking" the network with respect to other contracts. Lack of scalability is crippling the supply chain which is why Government contractors have been begging for consistency in requirements across the Federal organizations for years the ODP approach expands inconsistency and is the exact opposite of what is needed.

Given that NISTs charter is to provide Standards recommend replacing all ODPs with a standard wording. NIST may also elect to overlay that baseline by signifying which elements are most appropriately subject to enhancement by an individual Federal organization. In this way both a standard is established and flexibility is indicated should the Federal organization wish to apply it.

Submitted by: Carnegie Mellon Topic: Organization Defined Parameters (ODPs)

<p>The use of ODPs will lead to an unreasonable burden on contractors serving the federal government. Each Department/Agency could set different values for the ODPs, putting contractors in the position of having to implement multiple (and possibly mutually exclusive) variants of the same security requirement.</p> <p>In general, use of ODPs is excessive and works against standardization. NFOs seeking compliance with agency requirements will face what amounts to essentially unlimited versions of the "same" standard. During the webinar, NIST indicated that agencies could defer the ODP to the NFO which is entirely counter to good practice and standardization</p>	<p>Eliminate ODPs and provide specific baseline variables in the security requirements. Security enhancements on the baseline can be incorporated into 800-172.</p> <p>At a minimum, NIST should specify default values for most ODPs which are numeric (i.e. frequency based, number of attempts, number of characters, etc.) and give agencies the ability to customize where appropriate. Where appropriate, specific ODPs are addressed in individual comments. In no case should the ODP be entirely up to the NFO. This could lead to periodically (in r2) implementations that greatly exceed sound practice (i.e. do vulnerability scans every 5 years)</p> <p>For ODPs which reference an NFOs policy, procedures, staff roles, risks, personnel, functions, etc., it is unrealistic to assume a Federal agency can specify something that is applicable to NFOs of widely different sizes, maturity, and industries. Where appropriate, specific ODPs are addressed in individual comments but in general these assignment statements should reference the required information to be in compliance with control SSP section 3.15.1. In order to meet the objectives of SSP section 3.15.1, the NFO will need to specify organizational roles, structure, internal processes etc.</p>
--	---

Submitted by: National Institutes of Health

Topic: Organization Defined Parameters (ODPs)

<p>Has NIST has moved away from the original intent to provide industry (non-government) a plain language document to implement security controls. This major shift towards 800-53 Rev 5 is burdensome, specially with the requirement to define ODPs (pushes an independent organization to follow the govt. agency ODP which may be better fit for the agency vs the private organization); this shift aligns more so with FISMA compliance for non-federal systems. This document will have immense impact on contractors with DFARS requirements and looking for CMMC certifications. It appears NIST is converging to FISMA compliance for all.</p>	
--	--

Submitted by: DOD CIO

Topic: Organization Defined Parameters (ODPs)

The statement “For some requirements organization-defined parameters (ODP) are included. These ODPs provide additional flexibility by allowing federal organizations to specify values for the designated parameters as needed” is problematic. Clearly the organization’ should be the non-federal organization (the owner/operator of an information system NOT operated on behalf of the government but for internal business purposes) and it would be inappropriate for a USG agency to specify what parameters are assigned. But this statement says it is the USG Agency that selects the parameters. Aside from having no knowledge of the nonfederal organization’s system it is especially problematic in that different Agencies (or different elements within an Agency) would almost certainly specify different parameters for the same requirement creating unnecessary churn and a chaotic security environment if the nonfederal org has to continually accommodate differing or conflicting requirements simultaneously. It also creates unacceptable contract administration issues for the USG expected to issue some 100K contracts a year requiring compliance with NIST SP 800-171 as it is simply not possible for the USG Requiring Activities/Contracting Officers to complete the 108 ODPs in rev3 for each contract. Note also that only 35 of the 108 ODPs are simple enough (e.g. frequency of review or update) for the Agency to even attempt to specify a value – the rest require substantive knowledge of the system operation to complete which the Agency does not have. It is also noted that aside from the fill-in-the-blank’ ODP everywhere else in the requirement statement or in the Discussion’ section following each requirement whenever the term organization’ is used it clearly means the nonfederal organization – there is a complete disconnect between the use of the organization’ term in the ODP and everywhere else in the document.

Remove the ODPs from the individual requirements (and the portion of Section 2.2 discussion ODP’s) as unnecessary. The NIST SP 800-171r2 requirement statements without ODPs established the requirement for the nonfederal organization to specify the necessary parameters to implement the requirement in their SSP or associated documents – a fill-in-the-blank’ requirement statement is unnecessary. If NIST requires retention of the ODPs to align with 800-53 controls it should make clear in Section 2.2 that the ODPs are to be assigned by the nonfederal agency. If NIST is concerned that a nonfederal org may select inappropriate parameters NIST can provide in 800-171 a suggested range of acceptable values (or point to an appropriate reference). Agencies can as always review the SSP and address any concerns with the nonfederal org.

Submitted by: DOD CIO

Topic: Applicability / Scope

The applicability statement "The security requirements in this publication are only applicable to components of nonfederal systems that process store or transmit CUI or that provide protection for such components" has been (in 800-171r2) purposely misinterpreted to mean that the requirements only apply to components that actually process store or transmit CUI and the other components (e.g. servers workstations) that do not process CUI need not meet the requirements. This problem was mitigated in Section 1.1 of the recent (01-28-2021) errata version by moving the clarifying phrase "If nonfederal organizations designate specific system components for the processing storage or transmission of CUI those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain" to follow the problematic applicability statement. This clarifying phrase is absent from rev3 and so the applicability of the requirements in rev 3 will surely be misinterpreted by some to avoid fully implementing NIST SP 800-171.

Rephrase applicability statement to read "The security requirements in this publication are only applicable to nonfederal systems that process store or transmit CUI and the components within that are capable of processing storing or transmitting CUI or that provide protection for such components" and following this sentence re-insert the clarifying statement that "If nonfederal organizations designate specific system components for the processing storage or transmission of CUI those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain".

Submitted by: Carnegie Mellon Topic: Applicability / Scope

This control is redundant of 3.8.3 since the item must contain CUI. However, in the front matter :**"The requirements apply to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components."**

Change to:

Dispose of system components, documentation, or tools containing CUI or that provide protection for such components using the techniques and methods described in NISP SP 800-30

Submitted by: DOD CIO

Topic: Allowable cryptographic encryption methods

<p>3.13.11 Believe the govt will just say "FIPS-validated or NSA-approved" so why have the ODP? Regardless need to tie this requirement back to all the other requirements involving cryptography and remove from their discussions any other options so it's clear to NFOs that they need to meet this requirement everywhere it applies.</p>	<p>Assign ODP as "FIPS-validated or NSA-approved" and tie all other requirements for cryptography back to this one so when they are implemented people know one of those two solutions are required.</p>
--	--

<p>3.8.9 Cloud issue - small companies primary use cloud for backups. How do they achieve this? Link to 3.13.11 so NFOs don't accidentally fail by choosing one type of encryption here that differs from the 3.13.11 requirement. Remove alternative physical controls from the discussion - conflicts with the requirement.</p>	<p>Explain how this works with cloud backups. Link to 3.13.11 for selection of the encryption type. Remove alternative physical controls from the discussion.</p>
---	---

Submitted by: Carnegie Mellon Topic: Allowable cryptographic encryption methods

3.13.11 is expected to require either FIPS or NSA validated algorithms therefor implying that any form of encryption is acceptable is counter productive.	Either specify FIPS and NSA algorithms or reference compliance with 3.13.11
Definition requires FIPS 140-2 and excludes FIPS 140-3 validation.	Adjust definition to verified by CNVP to meet requirements of FIPS140-2 or FIPS140-3

Submitted by: DOD CIO

Topic: Independent assessments

3.12.5 What does "control" mean? Is it different from "security controls?" Are the (security) controls just all the 171 requirements? Why switch terms? Please be consistent. Does this mean to assess every requirement? If they bring in someone to assess one requirement have they met this? Need to be much more specific.

The argument for ODPs is that NIST wants to provide flexibility - this one requirement removes a HUGE part of flexibility for the govt. CMMC level 2 self-assessment would fail this that's a huge piece of flexibility the govt wants to utilize.

This requirement needs to be removed. It's not right to impose this on every company nor is there an ecosystem to support it.

We believe this excludes anyone internal to the NFO from being the "independent" assessor because they always have some level of COI when a failure could mean loss of contracts which means potentially loss of job for anyone who works in the company on the enterprise network - please be explicit regarding whether that's true or not.

Minimally you have doubled the cost of a CMMC Level 2 assessment because you have to do an independent assessment first at \$\$\$ to pass this requirement and then have a C3PAO come in and do the "real" assessment for another \$\$\$.

Use consistent terms - either requirement or control or security control.

Either reword to better explain the scope (e.g. assessment of one requirement by an independent party would meet this) and define independent (e.g. can someone inside the NFO ever meet the definition of independent) OR REMOVE.

Submitted by: Carnegie Mellon Topic: Independent assessments

<p>Understanding that this is performed as part of the RMF ATO process, it is not appropriate for all NFOs to always have third party assessments and is prohibitively expensive. And given the lack of standardization that the ODPs introduce, NFOs would require independent control assessments for every agency they contract with. Recognizing the value of third party assessments, agencies can set individual requirements for self-assessment and independent assessment</p>	<p>delete requirement</p>
--	---------------------------

Submitted by: National Institutes of Health

Topic: Independent assessments

<p>Independent Assessment This is burdensome and cost prohibitive in most cases for smaller organizations.</p>	<p>This is a burdensome requirement and removes the flexibility of self assessments, please clarify level "independence" here.</p>
---	--

Submitted by: DOD CIO

Topic: Plan of Action

3.12.2[a] Imp lies that an NFO always has a POAM that should not be required. Needs to be rewritten to allow for an org not to have a POAM and to only make one when needed - could add "as applicable".

[b] Implication is a long-term perpetual POAM which some govt orgs are not going to accept. Old R2 wording worked better. A good POAM always has an expected end date otherwise it's just a paper drill to pass an assessment without any real action. Should include a max plan length for each POAM entry of 180 days.

[a] Rewrite to allow for an org not to have a POAM.

[b] Revert to R2 wording. Or reword so as not to imply a perpetual POAM. Also set POAM limit of 180 days.

Submitted by: DOD CIO

Topic: Marking CUI

3.8.4[a] The requirement is okay for anything "known" to be CUI. But the company cannot be held accountable for CUI not marked by the govt. The requirement needs to provide companies with an out for this case - when the govt fails to mark CUI - because that is out of the NFO's control.

[b] Remove not applicable to NFOs. CUI needs to be marked - there are no exemptions.

[a] Provide an out for NFO's when the govt fails to mark CUI.

[b] Remove requirement.

Submitted by: Southern Company

Topic: Marking CUI

<p>Please add clear direction that the federal agencies are responsible to define to nonfederal organizations what data is considered CUI, per Dr Ross comments at time 7:25 of the public comments webinar. There is various interpretation by different agencies and non federal organizations on who defines what CUI is.</p>	<p>or transmitted by nonfederal organizations using nonfederal systems.⁵ "It is the responsibility of the federal agency after consulting the NARA CUI registry, to specify and notify nonfederal organizations what data is considered CUI."</p>
--	--

Submitted by: AECOM


Topic: How does Rev.3 affect CMMC?

<p>The rollout of CMMC, requiring compliance with NIST SP 800-171x seems to conflict with the completion of the NIST SP 800-171r3 timeline. How are contractors and our subcontractors expected to understand the requirements. Will CMMC define NIST SP 800-171r2 as the baseline, then change when r3 is implemented?</p>	<p>Clarify the impact of CMMC and NIST SP 800-171rs timelines.</p>
---	--

Submitted by: WinTech

Topic: External Service Providers

<p>3.9.3 External Personnel Security/3.16.3 External System Services – “external providers” “external system service” – NIST should formally define these terms in the Glossary. This is an important definition as other entities have competing definitions and will certainly impact industry going forward.</p>	<p>Formally define terms in Glossary. In order to support the confidentiality of data government agencies MUST use a standardized definition instead of being left to their own devices to come up with their own definition. Businesses don't operate in vacuums with only one agency. If one agency defines an MSP differently than another this actually does the goal of confidentiality of data disservice.</p>
<p>Requiring external personnel especially cloud services to comply with an SMB's security policies and procedures as well as monitoring that compliance is unrealistic.</p>	<p>Redefine this requirement to differentiate the types of roles that would be required for these vs just stating a external providers. Requiring this does not contribute towards the goal of supporting confidentiality of data.</p>
<p>3.16.3 External System Services (reference to ODP) – ODPs define controls – Customer could require compliance with a variety of competing regulations. The intent to lower risk could actually introduce more risk by reducing the amount of vendors available willing and compliant.</p>	<p>Clarify which tiers are responsible for meeting. Define ESP MSP CSP (recognizing they are not all equal and perform different roles in the environment). Not defining these increases risk of confidentiality of data because companies will be defined differently across different projects and partnerships.</p>



Summary created by
Amira Armond, CMMC
Provisional Assessor &
Provisional Instructor &
CCA, CISSP, CISA



Resilient IT