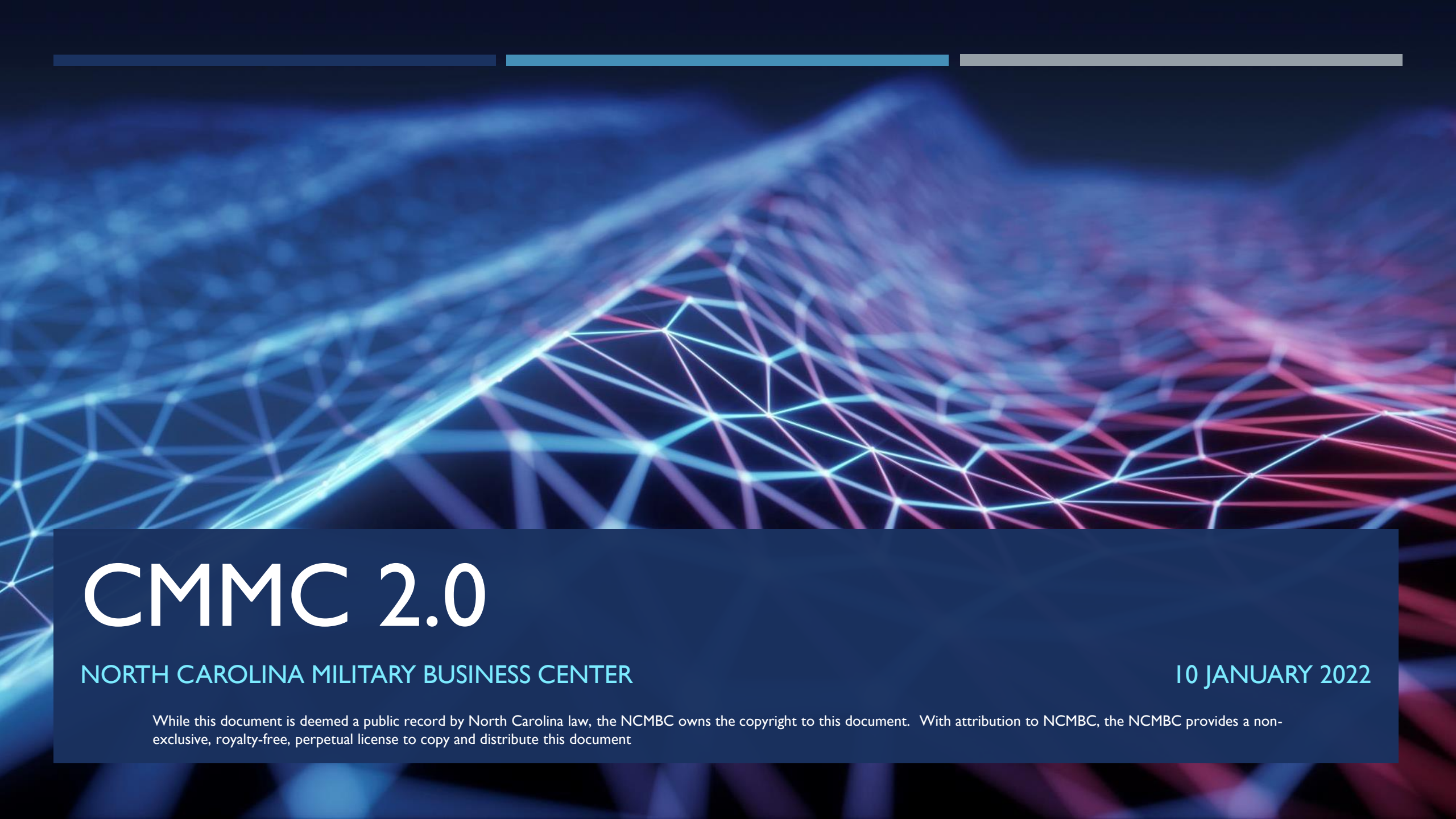


CMMC 2.0

NORTH CAROLINA MILITARY BUSINESS CENTER

10 JANUARY 2022

CMMC 2.0 - BACKGROUND

On November 4th of 2021, the Department of Defense released the CMMC 2.0 model. CMMC 1.0 was part of the DFARS Interim Rule (DFARS clause 252.204-7021) that became effective November 30, 2020.

Why the model was changed:

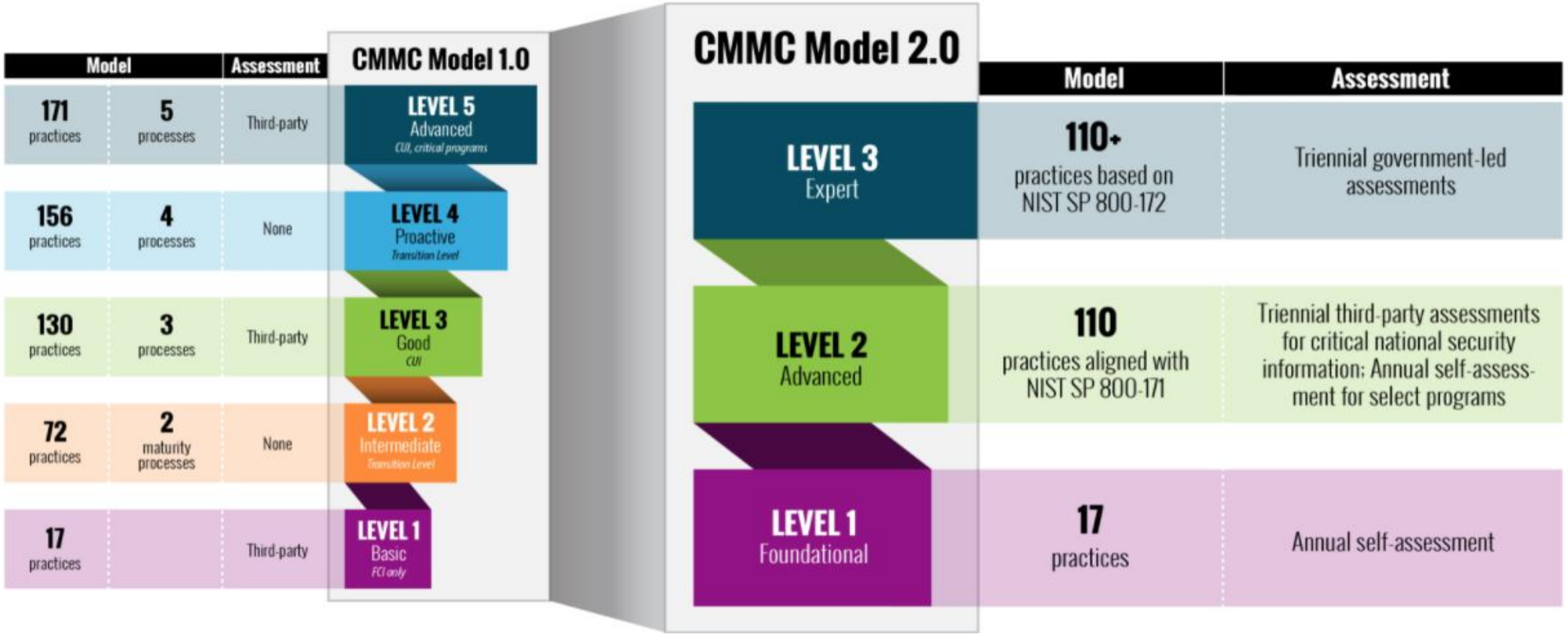
- Industry push-back over the cost of implementation.
- The DoD wanted to align its cyber requirements with NIST standards since other federal agencies use NIST.
- The CMMC – unique standards would separate the DoD from other agencies

CMMC 2.0 – WHAT CHANGED?

Overall changes from CMMC 1.0

- Process maturity practices eliminated – or were they?
- 20 additional controls in CMMC 1.02 Level 3 were removed
- Streamlined from 5 levels down to 3 levels. Levels 2 and 4 were eliminated (not really – they were combined into the new CMMC Levels 2 and 3).
- Plans of Action and Milestones (POAMS) are allowed, but with restrictions.
- Waivers are allowed under certain circumstances.
- Self-assessments allowed for Level 1 and a subset of Level 2.
- Participating in CMMC 2.0 is voluntary until rule-making is completed in 9 – 24 months. The CMMC-AB is considering incentivizing companies that want to get assessed prior to implementation
- Pilot program suspended – CMMC will be in 100% of contracts when approved - after rule-making process. Could be as early as 2023.

CMMC 2.0 - MODEL



CMMC 2.0 – WHAT CHANGED? LEVEL 1

CMMC 2.0 - Level 1 (Foundational)

- Same 17 controls derived from FAR 52.204-21
- Protects FCI
- No 3rd party assessments – contractors will perform a self-assessment using the DoD Assessment Methodology (DoD AM) and upload their score to SPRS. *Senior official must affirm the score*. (Remember the DOJ recently rolled out its Civil Cyber Fraud Initiative)
- Yearly self-assessment

CMMC 2.0 – WHAT CHANGED? LEVEL 1

CMMC 2.0 - Level 1 (Foundational)

Impact

- Contractors don't have to pay for a 3rd party assessment every three years
- Supply chain not illuminated – can't weed out back actors ($30M contract just awarded to Convergent Solutions to illuminate the supply chain)
- C3PAOs and assessors saw 60% of their market disappear

CMMC 2.0 – WHAT CHANGED? LEVEL 2

CMMC Level 2 (Advanced)

- Combination of CMMC Levels 2 and 3 from original model.
- Protects CUI
- Assessments – Level 2 was split into 2 groups:
  - "Non-prioritized" acquisitions will not require contractors to undergo a 3rd party independent assessment. Self-assessments to the 110 controls in NIST SP 800-171 using the DoD AM must be performed, scores uploaded to SPRS, and *senior official must affirm the score. Yearly self-assessments*.
  - "Prioritized" acquisitions will require contractors to undergo an independent assessment by a C3PAO every 3 years.

CMMC 2.0 – WHAT CHANGED? LEVEL 2

CMMC Level 2 (Advanced)

- Eliminated the 20 additional controls (Delta 20). We are back to the 110 controls in NIST SP 800-171; however, many of the 'Delta 20' are referenced in other controls and are therefore implied.
- Removed process maturity – not really – Non-Federal Controls controls still in place

CMMC 2.0 – WHAT CHANGED? LEVEL 2

CMMC Level 2 (Advanced)

- POAMs allowed
  - Limited number of POAMs
  - Must have a minimum score to have POAMs
  - No POAMs on the 42 controls with a DoDAM value of 5 (most expensive and difficult to implement)
  - POAMs are time-limited – most likely 180 days
- Waivers of CMMC requirements allowed under certain circumstances

CMMC 2.0 – WHAT CHANGED? – LEVEL 2

CMMC Level 2 (Advanced)

Impact

- Some percentage of contractors that touch CUI will not have to pay for a 3rd party assessment (Savings of at least $50k)
- Contractors are potentially at a greater risk of charges being filed using the False Claims Act since 3rd party verification of their system no longer required. (DOJ Civil Cyber Initiative)
- C3PAOs and assessors saw more of their market disappear
- Having a POAM in place means you haven't implemented a control, which creates a vulnerability. Could have a negative impact on national security.

CMMC 2.0 – WHAT CHANGED? LEVEL 2

CMMC Level 2 (Advanced)

Impact

- Eliminating the Delta 20 controls below makes no sense. An organizations highest risk is its people, so why eliminate the controls that help keep employees from getting emails that contain malware?
  - SI.3.218 - Employ spam protection mechanisms at information system access entry and exit points.
  - SI.3.219 - Implement email forgery protections.
  - SI.3.220 - Utilize sandboxing to detect or block potentially malicious email.

CMMC 2.0 – WHAT CHANGED? LEVEL 2

CMMC Level 2 (Advanced)

Impact

- Eliminating the Delta 20 controls
  - AM.3.036 – Define procedures for the handling of CUI data
  - IR.2.093 - Detect and report events.
  - IR.2.094 - Analyze and triage events to support event resolution and incident declaration.
  - IR.2.096 - Develop and implement responses to declared incidents according to pre-defined procedures.
  - IR.2.097- Perform root cause analysis on incidents to determine underlying causes

CMMC 2.0 – WHAT CHANGED? – LEVEL 2

CMMC Level 2 (Advanced)

Impact

- RE.2.137 - Regularly perform and test data backups.
- RE.3.139 - Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.
- RM.3.144 - Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.
- RM.3.146 - Develop and implement risk mitigation plans.
- RM.3.147 - Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.

CMMC 2.0 – WHAT CHANGED? LEVEL 2

CMMC Level 2 (Advanced)

Impact

- SA.3.169 - Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
- SC.3.193 - Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).

CMMC 2.0 – WHAT CHANGED? LEVEL 3

CMMC 2.0 Level 3 (Expert)

- Combination of Levels 4 and 5
- Designed to protect CUI from Advanced Persistent Threats
- 110 cybersecurity controls from NIST SP 800-171 plus controls from NIST SP 800-172
- No maturity processes (still must implement the NFO controls)
- Allows for Plan of Action & Milestones (POAMs) – limited number of POAMs, may not have POAMs for 42 practices with NIST value of 5, must have a minimum score to have POAMs, POAMs will be time-limited
- Assessments
  - Government-led assessments every 3 years (probably DIBCAC)
- Waivers of CMMC requirements allowed under certain limited circumstances

CMMC 2.0 – BACK TO WHERE WE STARTED

Until the rule-making process is completed and the new CMMC model is approved, (9 – 24 months) we are back to where we started.

- **2017 - DFARS 252.204-7012** – Safeguarding Covered Defense Information and Cyber Incident Reporting; allowed self-attestation to the 110 controls in the NIST SP 800-171 framework; protects Controlled Unclassified Information (CUI) plus flow-down requirements, rapid reporting of cyber incidents (72 hours), submission of malicious software to the DoD, media preservation/protection, cloud service provider must meet FedRAMP moderate baseline; Plan of Action and Milestones (POAMs) allowed for unimplemented controls.
- **DFARS 252.204-7019** – required a self-assessment (Basic) to the 110 controls in NIST SP 800-171 using the DoD Assessment Methodology (DoDAM) every 3 years, and scores to be uploaded to the Supplier Performance Risk System (SPRS). Did not replace DFARS 252.204-7012
- **DFARS 252.204-7020** – requires contractors to allow the DoD to perform Medium or High assessments. DFARS 252.204-7012 still in effect.

DFARS CLAUSES – NIST ASSESSMENTS

What most of us didn't know about NIST SP 800-171: supposed to use the assessment objectives in 800-171A when performing self-assessments.

PUBLICATIONS

SP 800-171 Rev. 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Date Published: February 2020 (includes updates as of January 28, 2021)

Supersedes: SP 800-171 Rev. 2 (02/21/2020)

Planning Note (3/9/2021):

*NIST SP 800-171, Revision 2 issued on 1/28/2021 is an errata update. It is consistent with NIST procedures and criteria for errata updates, whereby a new copy of a final publication is issued to include corrections that **do not alter** existing or introduce new technical information or requirements. Such corrections are intended to remove ambiguity and improve interpretation of the work, and may also be used to improve readability or presentation (e.g., formatting, grammar, spelling).*

Specifically in SP 800-171, Revision 2, an existing paragraph was moved to an earlier section to emphasize existing relevant supplemental guidance about the applicability of the security requirements. The changes in the applicability paragraph are editorial in nature and do not impact the publication's scope or implementation, nor introduce new technical information.

DOCUMENTATION

Publication:
SP 800-171 Rev. 2 (DOI)
Local Download

Supplemental Material:
CUI Plan of Action template (word)
CUI SSP template **[see Planning Note] (word)
Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 (xls)

Other Parts of this Publication:
SP 800-171A

DFARS CLAUSES – NIST ASSESSMENTS

3.1 ACCESS CONTROL

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.1[a]	*authorized users are identified.*
	3.1.1[b]	*processes acting on behalf of authorized users are identified.*
	3.1.1[c]	*devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d]	*system access is limited to authorized users.*
	3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f]	*system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].	

Implementation of a control means that *all assessment objectives must are met.* If any of the objectives are not met, the value of the control from the DoDAM must be deducted from 110.

NIST SP 800-171 NON-FEDERAL CONTROLS

What most of didn't know about NIST SP 800-171

- The non-federal organization controls (NFO) in Appendix E are "*expected to be routinely satisfied by non-federal organizations without specification.*" In this context, the term "without specification" means that NIST approaches these NFO requirements as basic expectations that do not need a detailed description, since they are fundamental components of any organization's security program. An organization cannot legitimately implement a security program without **policies and procedures**, which are requirements that the NFO controls address as "basic expectations" for an organization to have. Without the NFO controls (e.g., foundational policies & governance), it is not feasible for an organization to have appropriate evidence of due care and due diligence to withstand external scrutiny in an audit. [https://www.nfo-controls.com/]

- What that means: CMMC 2.0 still includes policies/procedures – they were not removed.

CMMC 2.0 – OTHER CONSIDERATIONS

NIST SP 800-171 framework potential changes

- 800-171 r2 was written before the new Executive Order on Cybersecurity was released, before new threats such as ransomware emerged, and before COVID brought additional risks associated with remote work. It is likely that the 20 controls that were removed from CMMC 1.0 will be added to NIST SP 800-171.
- The current framework doesn't work well with manufacturing systems and operational technology.

CMMC 2.0 – OTHER CONSIDERATIONS

DOJ Civil Cyber Fraud Initiative – will use DOJ's civil enforcement mechanisms, namely the False Claims Act, to pursue government contractors and federal grant recipients that "knowingly provide deficient cybersecurity products or services, knowingly misrepresent their cybersecurity practices or protocols, or knowingly violate obligations to monitor and report cybersecurity incidents and breaches." DOJ will not limit enforcement to entities; *individuals also can be held accountable for cybersecurity-related fraud* (*remember, someone from senior management must affirm the NIST score that is uploaded to SPRS when CMMC 2.0 is implemented).* Under the False Claims Act, penalties for such violations could be substantial, including treble damages.

Recommendations:

- Perform a *thorough* self-assessment using the assessment objectives.
- If an employee has a cybersecurity concern, address it and don't retaliate. Several large contractors have been fined millions dollars for retaliation against whistleblowers.

CMMC 2.0 – OTHER CONSIDERATIONS

Good CUI news from the National Archives CUI blog on the response to the Intelligence and National Security Alliance report on the CUI program:

- Streamline CUI Registry to reduce the number of CUI categories.
- Transition more CUI categories from Specified to Basic.
- Adding more information to CUI Registry entries.
- Prioritize a FAR clause for CUI. Will "create a common mechanism to communicate which information contractors create for and receive from the Federal Government must be protected, how to protect it, and who it can be shared with. Contractors and Government officials will know the place in any solicitation or contract to find this information. It will also increase the clarity of the existing requirements, while the continued implementation of CUI further reduces the complexity and vagueness that existed pre-CUI."

CMMC 2.0 – OTHER CONSIDERATIONS

Accounting

The DFARS Interim Rule specifically delineated the expected costs of implementing the new DFARS clauses. The DoD is assuming that since DFARS 252.204-7012 has been in contracts since 2016, the only non-recurring costs that should be considered allowable are the costs for the additional requirements.

Example: *In accordance with NIST SP 800-171, a contractor should already be aware of the security requirements they have not yet implemented and have documented plans of action for those requirements; therefore, the burden associated with conducting a self-assessment is the time burden associated with calculating the score. DoD estimates that the burden to calculate the Basic Assessment score is thirty minutes per entity at a journeyman-level-2 rate of pay (0.50 hour * $99.08/hour = $49.54/assessment).*

So, implementing CMMC 2.0 Levels 1 and 2 should only cost $49.54 each year for self-assessments.

CMMC 2.0 – WHAT TO DO?

- Continue with your compliance program – don't wait for the rule-making process to be completed. *The requirements in FAR 52.204-21and DFARS 252.204-7012, 7019 and 7020 have not gone away.The DOJ Civil Cyber Fraud Initiative is applicable NOW.*
- Review your current contracts/solicitations to determine which cybersecurity FAR/DFARS clauses are referenced.
- If DFARS 252.204-7012 is in your contract AND you touch CUI, by virtue of accepting the contract you are self-attesting that you have implemented the 110 controls in NIST SP 800-171 or have POAMs in place for the unimplemented controls.
- If DFARS 252.204-7019 is in a solicitation AND you touch CUI, you must do a self-assessment to the 110 controls in NIST SP 800-171 using the DoD AM and upload your score to SPRS ASAP. *Do a **thorough** self-assessment using the assessment objectives in NIST SP 800-171A and implement the NFO controls.*

CMMC 2.0 – WHAT TO DO?

- If DFARS 252.204-7020 is in your contract AND you touch CUI, you may be assessed by the DoD – Medium or High assessment.
- Implement the 20 controls that were taken out of CMMC 1.0 anyway.
- Keep good records on how much you're spending on compliance. Now that we're back to NIST SP 800-171, it's doubtful the DoD will let you roll any non-recurring costs associated with compliance into your OH rates.
- Download CMMC Level 2 in a Box from cyberNC.us website.
- Get help from the NCMBC. rodgersl@ncmbc.us

CMMC 2.0

NORTH CAROLINA MILITARY BUSINESS CENTER

30 NOV 2021