POSITION PAPER SERIES

CMMC Delta 20

DISCLAIMER

The C3PAO Stakeholder Forum is an industry group of C3PAOs. The group is formed from C3PAOs and aspiring C3PAOs; it is open to all CMMC-AB Marketplace C3PAOs and confirmed C3PAO applicants. The mission is to advance the CMMC assessor and C3PAO input, participation, and consensus within the CMMC ecosystem. This include advocating for policies, sharing perspectives and working alongside the DoD, CMMC-AB, Organizations seeking certification and other stakeholders to advance the mission of CMMC, which broadly is to increase the cyber posture of the Defense Industrial Base. The C3PAO Stakeholder Forum's participation is voluntary and those individuals that participate do so of their own volition and without compensation. The views of the board and the C3PAO Stakeholder Forum are not necessarily those of each member or their respective companies. The DoD, and where delegated by the DoD to the CMMC-AB, are the ultimate authority with regard to CMMC. Any guidance contained within is not authoritative and if found in conflict with DoD guidance should be considered subordinate. We simply seek to share this guidance to help advance the conversations and drive consistency among the industry. To the extent that subsequent guidance is published by the DoD or similar authorities, this document will be revised.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

PURPOSE

To conduct an analysis of the "Delta 20" and make a recommendation for what controls should be added to the next revision of the NIST SP 800-171.

DISCUSSION

With the changes that were implemented with the release of CMMC 2.0, which resulted in the removal of the 20 CMMC-unique controls (used synonymously with practices), referred to as the Delta 20, it is our position and recommendation that 17 of those 20 controls should be added to the next NIST SP 800-171 revision, and by extension should still be implemented by DIB contractors that are pursuing a CMMC Level 2 assessment.

RECOMMENDATION

In cooperation with Chris Newborn, Cybersecurity Professor with the Defense Acquisition University, we conducted a critical analysis the Delta 20. Of the 20 controls, it is our position that three of the controls are not necessary, needed, or applicable for meeting the stated goals of CMMC 2.0. Of the remaining 17 controls, our assessment focused on if the control should still be required based on protecting CUI at the moderate confidentiality impact level.

> "The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." FIPS 199, P.2

> "With regard to federal information systems, requirements in the federal regulation for protecting CUI at the moderate confidentiality impact level will be based on applicable policies established by OMB and applicable government-wide standards and guidelines issued by NIST." NIST 800-171R, p. v

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Reference: FIPS 199, p. 6 - https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

The following table illustrates each of the Delta 20 controls, our recommendation, and the justification/reasoning for this recommendation. We reference the specific NIST SP 800-171 controls and the NFO (non-federal organization) controls.

Delta 20	Definition	Family	Recommendation	Rationale
AM.3.036	The organization establishes and maintains one or more processes or procedures for handling CUI data.	Asset Management	Yes Refer to NOTE 1	In alignment with 3.4 (CM) and NFOs (CM-1, CM-2(1), CM-2(7), CM-3(2), CM-8(5), and CM-9.
AU.2.044	Review audit logs.	Audit & Accountability	Yes Refer to NOTE 1	In alignment with 3.3 (AU) and NFO AU-1.
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.	Audit & Accountability	Yes	The security purpose for centralized collection would be to aid in protecting the integrity of the audit trail.
CA.3.162	Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.	Security Assessment	No.	Not a baseline requirement to protect CUI at the moderate confidentiality impact level.
IR.2.093	Detect and report events.	Incident Response	Yes Refer to NOTE 1	In alignment with 3.6 (IR) and NFOs IR-1 and IR-8.
IR.2.094	Analyze and triage events to support event resolution and incident declaration.	Incident Response	Yes Refer to NOTE 1	In alignment with 3.6 (IR) and NFOs IR-1 and IR-8.
IR.2.096	Develop and implement responses to declared incidents according to predefined procedures.	Incident Response	Yes Refer to NOTE 1	In alignment with 3.6 (IR) and NFOs IR-1 and IR-8.
IR.2.097	Perform root cause analysis on incidents to determine underlying causes.	Incident Response	Yes Refer to NOTE 1	In alignment with 3.6 (IR) and NFOs IR-1 and IR-8.
RE.2.137	Regularly perform and test data backups.	Recovery	Yes	Due to 2021 Security Industry Prediction Trends, this is aligned with Industry Best Practices to combat against Ransomware.
RE.3.139	Regularly perform complete, comprehensive, and resilient data backups, as organizationally defined.	Recovery	Yes	Due to 2021 Security Industry Prediction Trends, this is aligned with Industry Best Practices to combat against Ransomware.

Delta 20	Definition	Family	Recommendation	Rationale
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	Risk Management	Yes Refer to NIST 162 Handbook	In alignment with NIST 162 Handbook and Industry Best Practices to maintain a POA&M and continuous monitoring efforts of the SSP will enable leadership to determine future enhancements /implementation of the technology roadmap.
RM.3.146	Develop and implement risk mitigation plans.	Risk Management	Yes Refer to NOTE 1	In alignment with NIST 162 Handbook and Industry Best Practices to maintain a POA&M and continuous monitoring efforts of the SSP will enable leadership to determine future enhancements /implementation of the technology roadmap.
RM.3.147	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	Risk Management	Yes Refer to NOTE 1	In alignment with NIST 162 Handbook and Industry Best Practices to maintain a POA&M and continuous monitoring efforts of the SSP will enable leadership to determine future enhancements /implementation of the technology roadmap.
SA.3.169	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	Situational Awareness	No.	Not a baseline requirement to protect CUI at the moderate confidentiality impact level.
SC.2.179	Use encrypted sessions for the management of network devices.	System & Communications Protection	Yes Refer to NOTE 1	In alignment with 3.13 (SC) and NFOs SC-1, SC-7(3), SC-7(4), SC-20, SC-21, and SC-22.
SC.3.192	Implement Domain Name System (DNS) filtering services.	System & Communications Protection	Yes Refer to NOTE 1	In alignment with 3.13 (SC) and NFOs SC-1, SC-7(3), SC-7(4), SC-20, SC-21, and SC-22.

Delta 20	Definition	Family	Recommendation	Rationale
SC.3.193	Implement a policy restricting the publication of CUI on externally-owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).	System & Communications Protection	Yes Refer to NOTE 1	In alignment with 3.13 (SC) and NFOs SC-1, SC-7(3), SC-7(4), SC-20, SC-21, and SC-22.
SI.3.218	Employ spam protection mechanisms at information system access entry and exit points.	System & Information Integrity	Yes Refer to NOTE 1	In alignment with SI 3.14 and NFOs SI-1, SI-4(5), and SI-16.
SI.3.219	Implement email forgery protections.	System & Information Integrity	Yes Refer to NOTE 1	In alignment with SI 3.14 and NFOs SI-1, SI-4(5), and SI-16.
SI.3.220	Utilize sandboxing to detect or block potentially malicious email.	System & Information Integrity	Yes Refer to NOTE 1	In alignment with SI 3.14 and NFOs SI-1, SI-4(5), and SI-16.
NOTE:	The non-federal organization controls (NFO) in Appendix E of NIST SP 800-171A 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. [Source: https://www.nfo-controls.com/]			

SUPPLEMENTARY INFORMATION

Not Applicable

Document date: March 3, 2022