



A-LIGN

May 18, 2026

Attn: Asparuh Vasilev, Sr. Director, IT Security & Compliance
Nuvolo Technologies Corporation
16 Mica Lane
Wellesley, MA 02110

Subject: Attestation letter regarding CMMC Level 1 compliance for the Nuvolo Connected Workplace application in the Government Cloud environment on the ServiceNow platform.

Dear Mr. Vasilev,

A-LIGN attests that the Nuvolo Connected Workplace application aligns with the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) Level 1 requirements based on the evaluation of fifteen (15) security controls applicable to developing and providing customer support for the Nuvolo Connected Workplace application (See Appendix A for the list of controls evaluated). This attestation is based upon A-LIGN's understanding of current CMMC v2.13 requirements.

To facilitate the readiness assessment with CMMC Version 2.0, A-LIGN leveraged the CMMC Assessment Guide Level 1, Version 2.13, dated September 2024; NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information; and the Cybersecurity Maturity Model Certification (CMMC) Model Overview, Version 2.13, dated September 2024.

The purpose of the CMMC Version 2.0 Level 1 Readiness Assessment was to assist with the planning and analysis phase of Nuvolo's pursuit to achieve the CMMC Level 2 certification. A-LIGN gained an understanding of Nuvolo's environment, interviewed key personnel, and inspected existing security practices to produce the following readiness assessment to assist Nuvolo International (Nuvolo) in its planning and budgeting efforts toward a CMMC Version 2.13 Level 2 certification.

Based on the CMMC readiness assessment conducted by A-LIGN, Nuvolo has established many of the required security practices. At the request of Nuvolo Technologies Corporation (Nuvolo), A-LIGN has determined that the CMMC Level 1 controls identified in Appendix A of this memorandum are applicable to Nuvolo Connected Workplace as the software developer.

These controls were evaluated for the Nuvolo Connected Workplace offering and do not include controls inherited from the ServiceNow Platform or controls that customers using the Connected Workplace application are responsible for implementing. Controls from the Security Awareness & Training, Incident Response, Personnel Security, System and Service Acquisition, and System Integrity control domains were selected for evaluation.

The evaluation period was from April 20, 2026, to April 30, 2026, and the scope included interviews, reviews of artifacts, and evidence of security controls. The evaluation approach for Nuvolo Technologies Corporation consisted of two (2) phases, as described in the figure below:



A-LIGN

Phase 1: CMMC Level 1 Assessment	Phase 2: Final Reporting
<ul style="list-style-type: none">• Interview & Data Collection• Analysis & Reporting• Deliverable: Evaluation Workbook	<ul style="list-style-type: none">• Deliverable: CMMC Assessment Report• Deliverable: Attestation Letter

The results of the evaluation are documented in the Nuvolo 2026 Readiness Assessment Report (RAR).

As of May 1, 2026, A-LIGN has validated that all controls are considered “Met” in accordance with NIST SP 800-171A and the CMMC Level 1 assessment guide, dated September 2024.

If you have any questions about the product evaluation review conducted by the A-LIGN team, please contact me directly at Mike.Gallagher@a-lign.com.

Sincerely,

Mike Gallagher
Senior Director of Federal and Advisory Services
A-LIGN, CMMC C3PAO





APPENDIX A: CMMC LEVEL 1 PRACTICES EVALUATED

CMMC MODEL Level 1 Version 2.13			
SECURITY PRACTICES AND MATURITY PROCESSES			
Level	Family	Control ID	Practice
Access Control (AC)			
1	AC	AC.L1-B.1.I	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).
1	AC	AC.L1-B.1.II	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
1	AC	AC.L1-B.1.III	Verify and control/limit connections to and use of external information systems.
1	AC	AC.L1-B.1.IV	Control information posted or processed on publicly accessible information systems.
Identification and Authentication (IA)			
1	IA	IA.L1-B.1.V	Identify information system users, processes acting on behalf of users or devices.
1	IA	IA.L1-B.1.VI	Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.
Media Protection (MP)			
1	MP	MP.L1-B.1.VII	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.
Physical Protection (PE)			
1	PE	PE.L1-B.1.VIII	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.
1	PE	PE.L1-B.1.IX	Escort visitors and monitor visitor activity; maintain audit logs of physical access; control and manage physical access devices.
System and Communication Protection (SC)			
1	SC	SC.L1-B.1.X	Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
1	SC	SC.L1-B.1.XI	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
System and Information Integrity (SI)			
1	SI	SI.L1-B.1.XII	Identify, report and correct information and information system flaws in a timely manner.
1	SI	SI.L1-B.1.XIII	Provide protection from malicious code at appropriate locations within organizational information systems.
1	SI	SI.L1-B.1.XIV	Update malicious code protection mechanisms when new releases are available.
1	SI	SI.L1-B.1.XV	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.



A-LIGN

