August 16, 2024

Attn: Jason Siegrist, CISO
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. Siegrist,

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 seventeen (17) 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 v2.0 requirements as the CMMC framework and program is still under development by the Cyber Accreditation Body (CyberAB) and the DoD.

At the time of development of this Readiness Assessment Report (RAR), August 5, 2024, the CMMC Assessment Standard is in development, and the Cyber Accreditation Board (CyberAB) is still developing certified Assessor training and certification. The CyberAB is also in the process of authorizing CMMC Third-Party Assessment Organizations (C3PAOs) to conduct assessments for CMMC Version 2.0 in coordination with the DoD. As such, A-LIGN cannot offer formal CMMC assessment services, authorized by the CyberAB, at this time. To facilitate the readiness assessment with CMMC Version 2.0, A-LIGN leveraged the CMMC Assessment Guide Level 1, Version 2.0, dated December 2021; NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information; and the Cybersecurity Maturity Model Certification (CMMC) Model Overview, Version 2.0, dated December 2021.

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 their planning and budgeting efforts toward a CMMC Version 2.0 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 evaluated the CMMC Level 1 controls identified in Appendix A of this memorandum 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 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 period of evaluation took place from June 2024 to August 2024, and the scope of the evaluation included interviews, review 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:

Phase 1: CMMC Level 1 Assessment	Phase 2: Final Reporting
• Interview & Data Collection • Analysis & Reporting • Deliverable: Evaluation Workbook	• Deliverable: CMMC Assessment Report • Deliverable: Attestation Letter

The results of the evaluation are documented in the Nuvolo August 2024 Readiness Assessment Report (RAR).

As of August 5, 2024, 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 December 2021.

If you have any questions about the product evaluation review the A-LIGN team performed, please contact me directly at Haomin.zhang@a-lign.com.

Sincerely,

Haomin Zhang

Haomin Zhang
Senior Manager, A-LIGN Federal Practice
Haomin.zhang@a-lign.com
(888) 702-5446 x1539

APPENDIX A: CMMC LEVEL 1 PRACTICES EVALUATED

CMMC MODEL Level 1 Version 2.0			
SECURITY PRACTICES AND MATURITY PROCESSES			
Level	**Family**	**Control ID**	**Practice**
Access Control (AC)			
1	AC	AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).
1	AC	AC.L1-3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
1	AC	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.
1	AC	AC.L1-3.1.22	Control information posted or processed on publicly accessible information systems.
Identification and Authentication (IA)			
1	IA	IA.L1-3.5.1	Identify information system users, processes acting on behalf of users or devices.
1	IA	IA.L1-3.5.2	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.L1-3.8.3	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.
Physical Protection (PE)			
1	PE	PE.L1-3.10.1	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.
1	PE	PE.L1-3.10.3	Escort visitors and monitor visitor activity.
1	PE	PE.L1-3.10.4	Maintain audit logs of physical access.
1	PE	PE.L1-3.10.5	Control and manage physical access devices.
System and Communication Protection (SC)			
1	SC	SC.L1-3.13.1	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.L1-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
System and Information Integrity (SI)			
1	SI	SI.L1-3.14.1	Identify, report and correct information and information system flaws in a timely manner.
1	SI	SI.L1-3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.
1	SI	SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.

CMMC MODEL Level 1 Version 2.0			
SECURITY PRACTICES AND MATURITY PROCESSES			
Level	**Family**	**Control ID**	**Practice**
1	SI	SI.L1-3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.