July 8, 2022

Attn: Jason Siegrist, CISO
Nuvolo Technologies Corporation
16 Mica Lane
Wellesley, MA 02110

Subject: Attestation letter regarding FedRAMP 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 Federal Risk and Authorization Management Program (FedRAMP) requirements based on the evaluation of sixty (60) security controls applicable to developing and providing customer support for the Nuvolo Connected Workplace application (See Appendix A for the list of controls evaluated).

At the request of Nuvolo Technologies Corporation (Nuvolo), A-LIGN FedRAMP & Assurance Services was contracted to conduct a product evaluation for the Connected Workplace application available to customers in the FedRAMP-authorized Infrastructure-as-a-Service (IaaS) environment.

The FedRAMP program was designed for Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) providers that provide multi-tenant cloud solutions to the US Federal Government. To be eligible for listing in the FedRAMP marketplace, a SaaS, PaaS, or IaaS provider must control its cloud service delivery infrastructure. Nuvolo is an Independent Software Vendor (ISV) whose products are run by customers as managed packages in the IaaS environment. Once the Nuvolo package is installed in an IaaS or PaaS environment, the Nuvolo software is operated by the customer or managed service provider, and the underlying infrastructure is maintained by the IaaS provider, not by Nuvolo. Because Nuvolo does not operate and administer the application, it has no access to the production environment in which the application is hosted (except temporary access for implementation and/or support troubleshooting), and does not provide the cloud infrastructure, it is ineligible to be authorized for listing in the FedRAMP marketplace. Nuvolo asked A-LIGN to evaluate whether customers with FedRAMP-compliant operations are able to use Connected Workplace in a manner consistent with FedRAMP requirements, notwithstanding the ineligibility of Nuvolo to be listed on its own in the FedRAMP marketplace. Most FedRAMP controls applicable to Connected Workplace customers are inherited from the ServiceNow Platform or are the responsibility of the customer. However, A-LIGN has determined that the FedRAMP controls identified in the Appendix A of this memorandum are applicable to Nuvolo Connected Workplace as the software developer.

As part of this evaluation process, the sixty (60) applicable FedRAMP security controls were evaluated across five (5) control domains that pertain to Nuvolo acting as an ISV deploying code via a managed package to the ServiceNow Government Cloud environment.

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 May 2022 to June 2022, beginning with an initial product evaluation, a remediation period, and a product re-evaluation against controls determined to be “Other than Satisfied” during the initial product evaluation. The scope of the review included interviews, a review of artifacts and evidence, and sample testing to validate the remediation of security controls initially identified by A-LIGN as not fully satisfied. The evaluation approach for Nuvolo Technologies Corporation consisted of four (4) phases, as described in the figure below:

Phase 1: Product Evaluation	Phase 2: Remediation	Phase 3: Product Re-Evaluation	Phase 4: Final Reporting
• Interview & Data Collection • Analysis & Reporting • Deliverable: Evaluation Workbook	• Remediation phase for controls not satisfied during Product Evaluation	• Interview, data collection, and testing of ‘Other than Satisfied’ controls • Deliverable: Re-Evaluation Workbook	• Deliverable: Validation Whitepaper • Deliverable: Attestation Letter

The results of the evaluation are documented in the Nuvolo Connected Workplace June 2022 Security Assessment Report (SAR).

As of October 10, 2022, A-LIGN has validated that issues identified by A-LIGN regarding any of the 60 controls evaluated as “Other than Satisfied” in the June 2022 SAR have been remediated.

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

Sincerely,

Patrick J. Morse
Senior Consultant, A-LIGN Federal Practice
patrick.morse@a-lign.com
(888) 702-5446 x746

APPENDIX A: FEDRAMP CONTROLS EVALUATED

ID	Control Description	Sensitivity Level
		Moderate
AT	**Awareness and Training**	
AT-2	Security Awareness Training	AT-2, AT-2 (2)
AT-3	Role-Based Security Training	AT-3
AT-4	Security Training Records	AT-4
IR	**Incident Response**	
IR-2	Incident Response Training	IR-2
IR-3	Incident Response Testing	IR-3 (2)
IR-4	Incident Handling	IR-4 (1)
IR-5	Incident Monitoring	IR-5
IR-6	Incident Reporting	IR-6, IR-6 (1)
IR-7	Incident Response Assistance	IR-7 (1) (2)
IR-8	Incident Response Plan	IR-8
IR-9	Information Spillage Response	IR-9 (1) (2) (3) (4)
PS	**Personnel Security**	
PS-2	Position Risk Designation	PS-2
PS-3	Personnel Screening	PS-3, PS-3 (3)
PS-4	Personnel Termination	PS-4
PS-5	Personnel Transfer	PS-5
PS-6	Access Agreements	PS-6
PS-7	Third-Party Personnel Security	PS-7
PS-8	Personnel Sanctions	PS-8
SA	**System and Services Acquisition**	
SA-3	System Development Life Cycle	SA-3
SA-5	Information System Documentation	SA-5
SA-8	Security Engineering Principles	SA-8
SA-10	Developer Configuration Management	SA-10, SA-10 (1)
SA-11	Developer Security Testing and Evaluation	SA-11, SA-11 (1) (2) (8)
SI	**System and Information Integrity**	
SI-2	Flaw Remediation	SI-2 (2) (3)
SI-3	Malicious Code Protection	SI-3 (1) (2) (7)

ID	Control Description	Sensitivity Level
		Moderate
SI-10	Information Input Validation	SI-10
SI-11	Error Handling	SI-11