



A-LIGN

August 16, 2024

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

Dear Mr. Siegrist,

A-LIGN attests that the Nuvolo Connected Workplace application aligns with the Federal Risk and Authorization Management Program (FedRAMP) High requirements based on the evaluation of fifty-one (51) security controls applicable to developing and providing customer support for the Nuvolo Connected Workplace application (See Appendix for the list of controls evaluated).

At the request of Nuvolo Technologies Corporation, A-LIGN FedRAMP & Assurance Services was contracted to conduct a security assessment 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 Technologies Corporation is an Independent Software Vendor (ISV) whose products are run by customers as managed packages in the IaaS environment. Once the Nuvolo Technologies Corporation package is installed in an IaaS or PaaS environment, the Nuvolo Technologies Corporation software is operated by the customer or managed service provider, and the underlying infrastructure is maintained by the IaaS provider, not by Nuvolo Technologies Corporation. Because Nuvolo Technologies Corporation 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 Technologies Corporation asked A-LIGN to evaluate whether customers with FedRAMP-compliant operations can use Connected Workplace in a manner consistent with FedRAMP requirements, notwithstanding the ineligibility of Nuvolo Technologies Corporation to be listed on its own in the FedRAMP marketplace. Most FedRAMP controls applicable to Connected Workplace customers are inherited from an IaaS provider or are the responsibility of the customer. However, A-LIGN has evaluated the FedRAMP controls identified in the Appendix of this memorandum applicable to Nuvolo Connected Workplace as the software developer.

As part of this evaluation process, the fifty-one (51) applicable FedRAMP security controls were evaluated across five (5) control domains that pertain to Nuvolo Technologies Corporation acting as an ISV deploying code via a managed package to the IaaS Government Cloud environment.



A-LIGN

These controls were evaluated for the Nuvolo Technologies Corporation Connected Workplace offering and do not include controls inherited from an IaaS provider 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. To show continued maturity and cybersecurity posture for Nuvolo Technologies Corporation, a selection of controls from the FedRAMP High baseline were included during this assessment.

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:

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

The results of the evaluation are documented in the Nuvolo Technologies Corporation August 2024 Security Assessment Report (SAR).

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

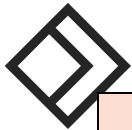




APPENDIX A: FEDRAMP HIGH PRACTICES EVALUATED

ID	Control Description	Sensitivity Level
		High
AT	Awareness and Training	
AT-2	Literacy Awareness and Training	AT-2, AT-2 (2), AT-2 (3)
AT-3	Role-Based Training	AT-3
AT-4	Training Records	AT-4
IR	Incident Response	
IR-2	Incident Response Training	IR-2, IR-2 (1), IR-2 (2)
IR-3	Incident Response Testing	IR-3, IR-3 (2)
IR-4	Incident Handling	IR-4, IR-4 (1), IR-4 (2), IR-4 (4), IR-4 (6), IR-4 (11)
IR-5	Incident Monitoring	IR-5, IR-5 (1)
IR-6	Incident Reporting	IR-6, IR-6 (1), IR-6 (3)
IR-7	Incident Response Assistance	IR-7, IR-7 (1)
IR-8	Incident Response Plan	IR-8
IR-9	Information Spillage Response	IR-9, IR-9 (2), IR-9 (3), IR-9 (4)
PS	Personnel Security	
PS-2	Position Risk Description	PS-2
PS-3	Personnel Screening	PS-3, PS-3 (3)
PS-4	Personnel Termination	PS-4, PS-4 (2)
PS-5	Personnel Transfer	PS-5
PS-6	Access Agreements	PS-6
PS-7	External Personnel Security	PS-7
PS-8	Personnel Sanctions	PS-8
PS-9	Position Descriptions	PS-9
SA	System and Service Acquisition	
SA-3	System Development Lifecycle	SA-3
SA-5	System Documentation	SA-5





A-LIGN

ID	Control Description	Sensitivity Level
		High
SA-8	Security and Privacy Engineering Principles	SA-8
SA-10	Developer Configuration Management	SA-10
SA-11	Developer Testing and Evaluation	SA-11, SA-11 (1), SA-11 (2)
SI	System and Information Integrity	
SI-2	Flaw Remediation	SI-2, SI-2 (2), SI-2 (3)
SI-3	Malicious Code Protection	SI-3
SI-10	Information Input Validation	SI-10
SI-11	Error Handling	SI-11

