



A-LIGN




Nuvolo Technologies Corporation


CYBERSECURITY  
MATURITY MODEL  
CERTIFICATION (CMMC)  
LEVEL 1 READINESS  
ASSESSMENT REPORT

Version 1.1  
August 8, 2022

## Prepared by

Identification of Organization that Prepared this Document		
	<b>Organization Name</b>	A-LIGN, Inc (A-LIGN)
	<b>Street Address</b>	400 N Ashley Drive
	<b>Suite/Room/Building</b>	Suite 1325
	<b>City, State Zip</b>	Tampa, FL 33602

## Prepared for

Identification of IT Services Provider		
	<b>Organization Name</b>	Nuvolo Technologies Corporation (Nuvolo)
	<b>Street Address</b>	16 Mica Lane
	<b>Suite/Room/Building</b>	N/A
	<b>City, State ZIP</b>	Wellesley, MA 02110

## Revision History

Date	Description	Version of RAR	Author
6/3/2022	Initial Draft Readiness Assessment Report	1.0	A-LIGN
8/8/2022	Initial Draft Readiness Assessment Report	1.1	A-LIGN

## TABLE OF CONTENTS

<b>SECTION 1 - EXECUTIVE SUMMARY.....</b>	<b>1</b>
<b>SECTION 2 - DOCUMENT AND CONTROL ANALYSIS.....</b>	<b>4</b>
Company Overview and Introduction.....	5
Scope and Requirements .....	5
CMMC Domain Organization and Structure.....	5
Assessment Procedures and Security Documentation.....	6
Readiness Assessment Methodology .....	9
<b>SECTION 3 - READINESS ASSESSMENT RESULTS .....</b>	<b>10</b>
Controls Analysis Summary.....	11
Conclusion & Recommendations.....	11

## SECTION 1 - EXECUTIVE SUMMARY

The protection of Controlled Unclassified Information (CUI) resident in non-federal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations. Executive Order 13556 established a governmentwide Controlled Unclassified Information (CUI) program to standardize the executive branch handles unclassified information that requires protection. 32 CFR part 2002, *Controlled Unclassified Information*, is the CUI Program for implementation regulations. Only federal information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or government-wide policy may be designated as CUI.

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), in conjunction with the Defense Industrial Base (DIB), Department of Defense (DoD) stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry has developed the Cybersecurity Maturity Model Certification (CMMC). The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to provide for the protection of CUI that resides on partner networks.

Prior to the start of this readiness assessment, the Department of Defense and CMMC Accreditation Body announced CMMC Version 2.0 which changes the scope and levels related to CMMC certification. A-LIGN focused the readiness assessment on the 110 security practices to be in scope for CMMC Version 2.0 Level 2 (which replaces CMMC Version 2.0 Level 3) while using the CMMC Version 2.0 Assessment Guide for Level 3 to interpret the security practice objectives for the assessment.

The CMMC framework is organized into multiple domains mapped across three levels. CMMC level descriptions, requirements, and mapping take into account multiple considerations including regulations, type and sensitivity of information, threats, cost, implementation complexity, diversity within the DIB sector, assessment implications, and other factors. The CMMC level required of an organization is specified by the DoD in Requests for Information (RFIs) and Requests for Proposals (RFPs).

The CMMC Model Version 2.0 characterizes the following levels:

- **Level 1**
  - Foundational (FCI)
  - This level encompasses the basic safeguarding requirement for FCI
- **Level 2**
  - Advanced (CUI)
  - Encompasses the security requirements for CUI
  - Requires an organization to also meet the security practices defined for Level 1
- **Level 3**
  - Expert (CUI)
  - Still being refined and is expected to include practices based on NIST SP 800-172
  - Requires an organization to also meet security practices defined for Level 1 and Level 2

The practices in CMMC Model Version 2.0 are largely derived from NIST Special Publication 800-171 Revision 2 (“NIST 800-171”), *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. CMMC Level 3 (from Version 2.0) will also include security practices derived from NIST Special Publication 800-172 (“NIST 800-172”), dated February 2021, *Enhanced Security Requirements for Protecting Controlled Unclassified Information*, a supplement to NIST 800-171.

Source for CMMC Practices Per Level

Level	Security Practices	Source
1	17	NIST 800-171
2	110	NIST 800-171
3	110+	NIST 800-171 & NIST 800-172

**CMMC Focus Topics**

- **System Security Plan (SSP):** CMMC requires that Federal agencies and contractors develop a formal system security plan which documents the types and methods of security control implementations utilized within the authorization boundary
- **Information Security Practices:** CMMC Level 3 (now to be known as CMMC Level 2 in Version 2.0) requires organizations to implement all CMMC security practices for Level 2 as well as security practices required for Level 1. CMMC practices span the people, processes, and technologies within the authorization boundary of the CUI environment

At the time of development of this Readiness Assessment Report (RAR), June 3, 2022 the CMMC Assessment Standard is in development and the CMMC Accreditation Board (CMMC-AB) has not formally certified Assessors or CMMC Third-Party Assessment Organizations (C3PAOs) to conduct assessments for CMMC Version 2.0 on behalf of CMMC-AB. As such, A-LIGN cannot offer formal CMMC assessment services, authorized by the CMMC-AB, at this time. To facilitate the readiness assessment with CMMC Version 2.0, A-LIGN leveraged the *CMMC Assessment Guide Level 2, 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 3 Readiness Assessment was to assist with the planning and analysis phase of Nuvolo’s pursuit to achieve the CMMC Level 3 certification. Based on the announcement of CMMC Version 2.0, the readiness assessment focused on the security practices for the new CMMC Level 2 in Version 2.0. 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.

A CMMC Version 2.0 Level 2 (formerly CMMC Version 1.02 Level 3) certification takes time to achieve. The project requires operational and resource commitment from all stakeholders, including management, to achieve a successful alignment with the CMMC requirements. It also requires a significant ongoing commitment to continuous monitoring activities conducted following the completion of a certification assessment.

Based on the CMMC readiness assessment conducted by A-LIGN, Nuvolo has established many of the required security practices. Nuvolo likely requires a moderate level of effort to address findings from this readiness assessment in preparation for a CMMC Version 2.0 Level 2 certification assessment. The findings from this readiness assessment are detailed in Section 3.

## SECTION 2 - DOCUMENT AND CONTROL ANALYSIS



## Company Overview and Introduction

Nuvolo is an Independent Software Vendor (ISV), that provides the Nuvolo Connected Workplace solution to the ServiceNow platform. Nuvolo Connected Workplace is a single cloud-based solution that is natively built on ServiceNow, which extends the ServiceNow platform and automates enterprise-wide processes for capturing data across all business areas. Nuvolo Connected Workplace provides an automated solution for data gathering in operational technology security, operational maintenance, project management, real estate management, and operational sustainability. Nuvolo manages the Connected Workplace solution entirely on Microsoft Azure.

## Scope and Requirements

The scope of the assessment was a controlled environment including the people, processes, and technology used to receive, process, analyze, and store CUI-related information. Nuvolo supports their information technology environment at their software development location at 16 Mica Lane, Wellesley, MA where they manage all security practices. The Nuvolo corporate-wide policies, procedures, and infrastructure were used as a conceptual scope for the purposes of this project.

## CMMC Domain Organization and Structure

The CMMC Level 1, Version 2.0 model identifies 6 domains that align with the appropriate security requirement families in NIST 800-171. Assessment procedures are grouped by the CMMC domain to help ensure assessments are complete and consistent. The new CMMC Level 1 (Version 2.0) contains a total of 17 security practices organized into these 6 domains.

- Access Control (AC)
- Identification and Authentication (IA)
- Media Protection (MP)
- Physical Protection (PE)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

## Assessment Procedures and Security Documentation

The CMMC Version 2.0 Level 1 Assessment Guide used for this readiness assessment contains assessment procedures consisting of an assessment objective for each security practice and objects that can be used to conduct the assessment. The assessment objectives include a determination statement related to each security practice.

During the assessment, assessment objects are evaluated based on the assessment objectives to determine how security practices and maturity processes are implemented. Objects can include specifications, mechanisms, activities, and individuals. Specifications are document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system. Mechanisms are the specific hardware, software, or firmware safeguards employed within a system. Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic). Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.

<b>CMMC MODEL Level 1 Version 2.0</b>			
<b>SECURITY PRACTICES AND MATURITY PROCESSES</b>			
<b>Level</b>	<b>Family</b>	<b>Control ID</b>	<b>Practice</b>
<b>Access Control (AC)</b>			
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.
3	AU	AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.
<b>Identification and Authentication (IA)</b>			
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.
<b>Media Protection (MP)</b>			
1	MP	MP.L1-3.8.3	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.
<b>Physical Protection (PE)</b>			
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.
<b>System and Communication Protection (SC)</b>			
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.
<b>System and Information Integrity (SI)</b>			
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.

<b>CMMC MODEL Level 1 Version 2.0</b>			
<b>SECURITY PRACTICES AND MATURITY PROCESSES</b>			
<b>Level</b>	<b>Family</b>	<b>Control ID</b>	<b>Practice</b>
1	SI	SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.
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.

In the table above, are the security practices and maturity processes that were tested during the assessment, as per Level 1 CMMC assessment Version 2.0.

## Readiness Assessment Methodology

A-LIGN performed the readiness assessment from 5/9/2022 through 6/3/2022 to determine Nuvolo compliance with their policies and procedures and to confirm Nuvolo implemented the security practices in accordance with published security practice objectives. Interviews with Nuvolo personnel and inspection of documented evidence such as policies, procedures, and system configuration settings were the primary methods of testing used during the assessment. Testing procedures followed the guidance in the table below.

Method	Definition
Interview	The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.
Examine	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.
Test	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

The following individuals were interviewed during the assessment.

Name	Title	Department
Jason Siegrist	Chief Information Security Officer (CISO)	Security
Asparuh Vasilev	Security & IT Operations Director	Security & IT Operations
Omar Fernandez	Compliance Director	Compliance
Joseph Thanickal	Lead Auditor	Compliance
Jonelle Lotts	Security Analyst	IT Security
Subin Valiyaprambath	Security Analyst	IT Security

## **SECTION 3 - READINESS ASSESSMENT RESULTS**

## Controls Analysis Summary

CMMC Version 2.0 Level 1 requires 17 security practices (organized in the 6 CMMC domains) to be implemented by Nuvolo. These practices include policies and procedures, processes, and technical controls. In order to understand the level of effort required for Nuvolo to prepare for a CMMC Version 2.0 Level 1 certification assessment, A-LIGN reviewed all 17 security practices.

A-LIGN identified a total of two (2) areas for improvement by Nuvolo: zero (0) high-impact, zero (0) moderate-impact, and two (2) low-impact areas. The Readiness Assessment Recommendations are summarized in the Risk Exposure Table (RET) embedded below.



## Conclusion & Recommendations

CMMC is an enterprise-wide model that requires significant resource commitment from organizations to achieve certification. Based on the work performed by A-LIGN and the information provided by Nuvolo, A-LIGN outlined recommendations that will allow Nuvolo to initiate the project activities to prepare for a CMMC Version 2.0 Level 2 certification. The purpose of these recommendations is to allow Nuvolo to assess the budgetary and resource requirements to develop an implementation process.

To achieve CMMC Version 2.0 Level 2 certification, Nuvolo should monitor and review CMMC Version 2.0 requirements as details and guidance are published (<https://www.acq.osd.mil/cmmc/index.html>). This should include NIST special publications <http://csrc.nist.gov/publications/PubsSPs.html> and the Computer Security Resource Center website <http://csrc.nist.gov/>.

- **Control Implementation** - Implementation of CMMC security practices is required to achieve CMMC certification. Currently, Nuvolo has implemented 56 of the 61 security practices defined for CMMC Version 2.0 Level 1. The 5 findings related to 5 CMMC security practices are documented in the Risk Exposure Table (RET) embedded in this report
- **Ongoing Commitment** - Upon achieving CMMC certification, Nuvolo will enter the continuous monitoring phase. The level of effort required to maintain CMMC certification is similar to the effort required to achieve certification. Although continuous monitoring occurs throughout the year, Nuvolo's management should be aware of the commitment made to ongoing cost and resource allocations required to maintain certification. At the time this Readiness Assessment Report was created, continuous monitoring activities and re-certification requirements have not been detailed by the CMMC Accreditation Body (CMMC-AB). Nuvolo should refer to the [CMMC-AB website](#) for additional information as the new CMMC model is rolled out
- **CUI Identification** - Nuvolo should work closely with each government client to identify and document where Nuvolo will collect, develop, receive, transmit, use, or store CUI for the performance of the contract. That data will then be used to determine the scope of the assessment and be subject to the controls outlined in the CMMC Version 2.0 Level 2 requirements