

IPS CMMC SERVICES

Protecting the DoD supply chain through certified implementation

Implementation Service

Organizations who have supported the DoD over several years often feel confident that their past implementation of the self-attested NIST 800-171 controls will guarantee them a certification under CMMC. THIS IS A FALSE SENSE OF SECURITY THAT COULD COST YOU A CONTRACT.

There are nuances of CMMC assessments that go deeper than the NIST 800-171. **Certified Registered Practitioners** have been trained to ensure organizations have what is needed to pass an assessment THE FIRST TIME.

Assessment Service

As of March 2023 only organizations part of the Joint Surveillance Voluntary Program are authorized to conduct or receive CMMC Assessments. But organizations not in this group still need to take action. There are very limited C3PAO's to conduct assessments and organizations need to get on the schedule now so you are not behind once rule making is complete. IPS is a C3PAO candidate and we are scheduling for 2023-2024 assessments NOW!



SUPPORTING THE DIB

WHY WE SERVE:

Protecting the thousands of organizations that support our DoD is the #1 priority of IPS. Securing each network node that transmits and stores sensitive data is paramount to our national security.

IPS CMMC SERVICES

Protecting the DoD supply chain through certified implementation

REPORT CMMC 2.0 Level 1 Self-Assessment Report

Contents

- EXECUTIVE SUMMARY1
- SELF-ASSESSMENT INFORMATION 1
- CMMC 2.0 SELF-ASSESSMENT TEAM 2
- SELF-ASSESSMENT OBJECTIVE, APPROACH, AND METHODOLOGY3
- SELF-ASSESSMENT OBJECTIVE 3
- SELF-ASSESSMENT APPROACH 3
- SELF-ASSESSMENT METHODOLOGY 5
- SELF-ASSESSMENT SCOPE7
- PERIODICITY OF SELF-ASSESSMENT8
- SELF-ASSESSMENT FINDINGS AND SELF-ASSESSMENT SCORE9
- DOMAIN 1: ACCESS CONTROL (AC) 11
- DOMAIN 5: IDENTIFICATION AND AUTHENTICATION (IA) 16
- DOMAIN 8: MEDIA PROTECTION (MP) 18
- DOMAIN 10: PHYSICAL PROTECTION (PE) 19
- DOMAIN 13: SYSTEM AND COMMUNICATIONS PROTECTION (SC) 23
- DOMAIN 14: SYSTEM AND INFORMATION INTEGRITY (SI) 25
- PLANS OF ACTION & MILESTONES (POA&MS)29
- APPENDIX A: CMMC DOCUMENT MANAGEMENT32
- CMMC SYSTEM SECURITY PLAN 32
- CMMC POLICY 33
- CMMC PROCEDURES 36
- CMMC EVIDENCE 38
- CMMC SUPPORTING EVIDENCE SCREENSHOT 40
- APPENDIX B: CMMC PHASE 1 INTAKE FORM

HOW TO GET STARTED

Before any commitment is made, we do a pre-assessment. This ensures your system is well defined and the a detailed contract is created.

CMMC Approach

- Identify and document the current cybersecurity practices and processes against CMMC.
- Perform gap analysis and be proactive and plan for enhancements in practices and processes.
- Assess where your organization is with respect to process maturity for each of the CMMC domains.

Validation Event	Score	Core Questions
Determine and Confirm Assessment Outputs	Fully	Did the plan ID the require outputs of the assessment
Develop Assessment Plan	Fully	
Identify Allowable Tailoring of Assessment Method	Partially	Was the level of tailoring identified in the plan?
Develop OE Collection Approach	Fully	Was the approach - timing method, roles, etc., ID'd in plan?
Select Assessment Team Members (ATMS), if Applicable	Fully	Were the Assessment Me CPs, CAs, or RPs?
Identify Resources and Schedule	Fully	Were the Assessment inte data collection, and finding schedule recorded in the p
Identify and Manage Conflicts of Interest (COI)	Fully	
Identify and Manage Conflic (COI)		

DETAILED SCORE

Contact Information

For more information contact:
 Dr. Celeste Chamberlain, CISSP
 cmmc@ips314.com

This ensures we meet your organizations needs where you are with a road map to where you want to be.