

## SAMPLE

### CMMC 2.0 Evidence Builder

The opening of CMMC-SSP-Template.docx, one of 7 files in the kit. <https://solasai.net/products/cmmc-evidence-builder/>

#### System Security Plan

NIST SP 800-171 Rev 2 / CMMC Level 2. Template for [Organization Name], [System Name]

**Product:** CMMC 2.0 Evidence Builder, System Security Plan template, version 3.0, 19 October 2026.

**Classification:** Purchaser use only. Customize before use. Mark the completed plan CUI if it describes a system that handles CUI. **Built by:** Solas AI. Written by an Information System Security Manager at a DoD contractor, CISSP and CISM. solasai.net

| Version | Date   | Author | Change       |
|---------|--------|--------|--------------|
| [1.0]   | [date] | [name] | Initial plan |
|         |        |        |              |

#### How to use this plan

1. Complete Sections 1 to 4 first. The system boundary in 2.2 decides what every statement in Section 5 has to cover. A narrow, well-defined enclave is easier to defend than the whole company network.
2. Work through Section 5 one family at a time. Every requirement has a short table (points, POA&M eligibility, status, owner, date), an implementation statement written as a worked example with [bracketed placeholders], the assessment objectives an assessor will test, and the evidence to attach. Replace every bracket. Delete anything that does not describe your system; an assessor reads a statement that mentions a tool you do not run as a finding.
3. Set the status of each requirement honestly. "Implemented" means every assessment objective is met and the evidence exists today. Anything less is "Partially implemented" or "Planned", and both score as NOT MET except for 3.5.3 and 3.13.11, which have a built-in 3-point partial.
4. Score the plan in the SPRS Scoring Workbook that ships with this kit. The workbook applies the 32 CFR 170.24 point values and the 170.21 Conditional-status rules. Submit the score to SPRS under DFARS 252.204-7019 and 7020.
5. Put every NOT MET item in the POA&M Tracker with an owner and a date. Six requirements can never be on a Conditional-status POA&M (3.1.20, 3.1.22, 3.10.3, 3.10.4, 3.10.5, 3.12.4), and

nothing above one point can be, apart from 3.13.11 at three points.

6. Review the plan at least annually and after any significant change, record the revision in the table above, and have it signed in Section 8.

The assessment objectives are paraphrased from NIST SP 800-171A (June 2018) so that each statement can be checked against what an assessor will determine. The point values follow 32 CFR 170.24 and the NIST SP 800-171 DoD Assessment Methodology, version 1.2.1.

## System Security Plan

This SSP documents how [Organization Name] protects Controlled Unclassified Information (CUI) in accordance with NIST SP 800-171 Rev 2 and CMMC Level 2 requirements.

### 1. System Identification

| Field                       | Value                                                         |
|-----------------------------|---------------------------------------------------------------|
| <b>System Name</b>          | <i>[System name]</i>                                          |
| <b>System Owner</b>         | <i>[Name, Title]</i>                                          |
| <b>Security Contact</b>     | <i>[Name, Title, Email, Phone]</i>                            |
| <b>System Location</b>      | <i>[Physical location and/or cloud provider/region]</i>       |
| <b>System Status</b>        | <i>[Operational / Under Development / Under Modification]</i> |
| <b>Authorization Date</b>   | <i>[Date system was authorized to operate]</i>                |
| <b>Last Assessment Date</b> | <i>[Date of most recent NIST 800-171 assessment]</i>          |
| <b>SPRS Score</b>           | <i>[Current score]</i>                                        |

### 2. System Description

#### 2.1 System Purpose

*[Describe the system's purpose and the business functions it supports. What does it do and why does it exist?]*

#### 2.2 System Boundaries

*[Define what is inside and outside the system boundary. List all components: servers, databases, applications, network devices, endpoints, and cloud services that process, store, or transmit CUI.]*

#### 2.3 System Architecture

*[Describe the system architecture. Include a network diagram showing system boundaries, data flows, and connections to external systems. Reference an attached architecture diagram.]*

## 2.4 System Interconnections

*[List all connections to external systems, including: system name, organization, connection type, data exchanged, and authorization status.]*

## 3. CUI Information Types

The following types of CUI are processed, stored, or transmitted by this system:

| <b>CUI Category</b>           | <b>CUI Marking</b>   | <b>Source</b>             | <b>Handling Caveat</b>         |
|-------------------------------|----------------------|---------------------------|--------------------------------|
| <i>[e.g., Technical Data]</i> | <i>[CUI//SP-CTI]</i> | <i>[Contract/Program]</i> | <i>[e.g., ITAR controlled]</i> |
|                               |                      |                           |                                |
|                               |                      |                           |                                |

## 4. System Users

| <b>User Role</b>              | <b>Access Level</b>          | <b>Count</b> | <b>Authorization</b>      |
|-------------------------------|------------------------------|--------------|---------------------------|
| <i>[System Administrator]</i> | <i>[Full administrative]</i> | <i>[#]</i>   | <i>[ISSM approval]</i>    |
| <i>[Standard User]</i>        | <i>[Read/write CUI]</i>      | <i>[#]</i>   | <i>[Manager approval]</i> |
| <i>[Read-only User]</i>       | <i>[Read CUI only]</i>       | <i>[#]</i>   | <i>[Manager approval]</i> |
|                               |                              |              |                           |

## 5. Security Requirement Implementation

All 110 NIST SP 800-171 Rev 2 requirements follow, grouped by family. The family summary table is for the executive reader; the per-requirement entries are the plan.

| <b>Family</b>                         | <b>Requirements</b> | <b>Points available</b> | <b>Implemented</b> | <b>Partially</b> | <b>Planned</b> | <b>N/A</b> |
|---------------------------------------|---------------------|-------------------------|--------------------|------------------|----------------|------------|
| 3.1 Access Control                    | 22                  | 54                      |                    |                  |                |            |
| 3.2 Awareness and Training            | 3                   | 11                      |                    |                  |                |            |
| 3.3 Audit and Accountability          | 9                   | 19                      |                    |                  |                |            |
| 3.4 Configuration Management          | 9                   | 33                      |                    |                  |                |            |
| 3.5 Identification and Authentication | 11                  | 27                      |                    |                  |                |            |
| 3.6 Incident Response                 | 3                   | 11                      |                    |                  |                |            |
| 3.7 Maintenance                       | 6                   | 18                      |                    |                  |                |            |

| Family                                    | Requirements | Points available | Implemented | Partially | Planned | N/A |
|-------------------------------------------|--------------|------------------|-------------|-----------|---------|-----|
| 3.8 Media Protection                      | 9            | 23               |             |           |         |     |
| 3.9 Personnel Security                    | 2            | 8                |             |           |         |     |
| 3.10 Physical Protection                  | 6            | 14               |             |           |         |     |
| 3.11 Risk Assessment                      | 3            | 9                |             |           |         |     |
| 3.12 Security Assessment                  | 4            | 13               |             |           |         |     |
| 3.13 System and Communications Protection | 16           | 42               |             |           |         |     |
| 3.14 System and Information Integrity     | 7            | 31               |             |           |         |     |
| <b>Total</b>                              | <b>110</b>   | <b>313</b>       |             |           |         |     |

The 109 scored requirements total 313 points, so the lowest possible SPRS score is -203.

Requirement 3.12.4, this plan, carries no point value: Annex A of the DoD Assessment Methodology marks it NA because without a system security plan the assessment cannot be completed.

A requirement may be marked Not applicable only when the system has no component to which it could apply. Annex A names five such cases where points are not subtracted: 3.1.12 and 3.1.13 where remote access is not permitted, 3.1.16 and 3.1.17 where wireless access is not permitted, and 3.1.18 where connection of mobile devices is not permitted. Any other N/A is the assessor's call. Every N/A must be justified in Appendix A, and an N/A the assessor rejects scores as NOT MET.

### 3.1 Access Control (22 requirements)

Access control is where most small contractors lose SPRS points, and where assessors spend the most interview time. Every statement below names a system of record (the identity provider, the firewall, the mobile device manager) because the assessor will ask to see that system, not the policy.

The sample ends here. The full document runs about 25,166 words; the kit holds 7 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/cmmc-evidence-builder/>, 14-day refund for any reason.