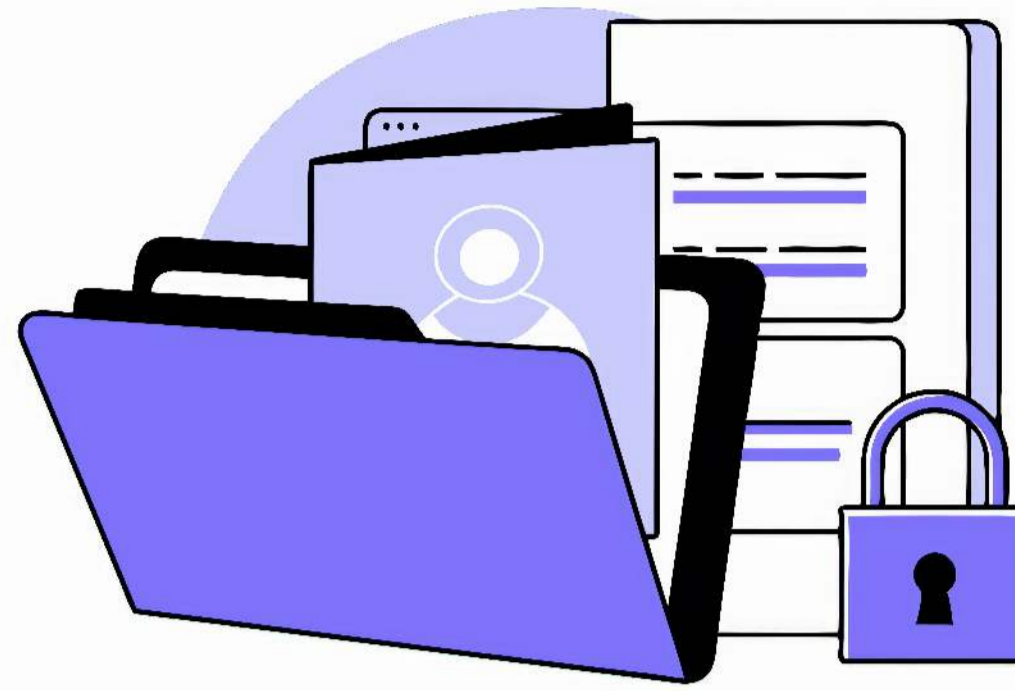




AG GRACE INC



Simplify Your CMMC Journey



Your System Security Plan: The Core of CMMC Compliance

If you're navigating CMMC Level 2 compliance, one document will make or break your assessment: the **System Security Plan (SSP)**.

Think of it as your cybersecurity blueprint — a detailed guide that explains **how your systems are configured, protected, and monitored**.

Without an SSP, your compliance efforts have no backbone. So let's walk through how to build one that's not just compliant, but clear, thorough, and audit-ready.

What is an SSP?

A System Security Plan is a **living document** that:

- Describes your IT system boundaries
- Lists implemented NIST 800-171 controls
- Details how each control is applied and maintained
- Identifies roles, responsibilities, and system components

It's **mandatory** for Level 2 under both CMMC and DFARS rules.

What to Include in Your SSP

✔ System Overview:

What system(s) are in scope? Include network diagrams, data flow, and boundaries.

✔ Environment Description:

Where is the system hosted? (On-prem, cloud, hybrid?)
What's your OS, hardware, and software stack?

✔ Control Implementation:

For **each of the 110 NIST 800-171 controls**, document:

- **What** you've done to meet it
- **How** it's implemented
- **Who** is responsible
- **Where** evidence can be found

✔ Personnel & Roles:

Identify key players (system owners, ISSO, IT leads, etc.) and their responsibilities.

✔ POA&M References:

Link unresolved items to your Plan of Action & Milestones with realistic deadlines.

Best Practices for a Rock-Solid SSP

- **Be Specific:** Vague language (e.g., "we use antivirus") is a red flag. Name tools, processes, and configurations.
- **Use Templates Carefully:** Start with one, but **customize it** to match your environment.
- **Update Frequently:** Don't treat it as "one and done." Keep it in sync with system changes.
- **Tie it to Evidence:** Mention where auditors can find proof — logs, screenshots, tickets, etc.

Warning Signs of a Weak SSP

- ✗ Using generic language copied from NIST controls
- ✗ Missing system diagrams or boundaries
- ✗ Listing controls as "TBD" or "will be implemented later"
- ✗ No named individuals responsible for controls

Helpful Resources

- [NIST 800-171A: Assessment Procedures for SSP Review](#)
- [CMMC Level 2 SSP Template \(Editable\)](#)

Next in the Series:

"What Belongs in Your POA&M: Turning Gaps Into Action" – Coming soon!

Need expert review of your SSP?

[Book a free 30-minute assessment call](#) with our CMMC consulting team or email us solutions@aggrace.com or call 240-315-6828 | www.aggrace.com

Cybersecurity Consultant | CMMC Specialist



5257 Buckeystown Pike, Suite 206, Frederick, MD 21704
Copyright © 2025 All rights reserved

No longer want to receive these emails? [unsubscribe](#)
AG Grace, Inc. www.aggrace.com