# Your SSP Is the Assessment

## How a C3PAO Reads Your CMMC System Security Plan

**David W. Koran**
CyberAB Registered Practitioner Advanced

---

## The Document You Did Not Know You Were Writing

If you own the CMMC program inside a defense contractor, you have probably been told that the System Security Plan is the foundation of your assessment. That is true, but it undersells the point in a way that harms contractors. The SSP is not the foundation of your assessment. The SSP is your assessment. You wrote it.

Here is what actually happens. Weeks before the assessment team arrives, the lead assessor reads your SSP. From that reading, the team builds its list of evidence requests, plans its interviews, and decides which artifacts to examine and which personnel to question. The CMMC Assessment Process is built around examining what you claimed, interviewing the people who you said do the work, and testing the mechanisms you said are in place. Every one of those activities starts from your document.

***This means the SSP functions like a restaurant menu.*** The assessment team walks in, sits down, opens the menu you handed them, and starts ordering. They do not order from some other menu. They do not invent dishes. They order what you listed, and they expect the kitchen to produce it and produce it correctly.

Everything on the menu will be ordered. That is the single most useful sentence you can hold in your head while writing or reviewing an SSP, and it reframes the entire exercise. Most program owners write the SSP as a compliance document, something to be completed and filed. Assessors read it as an offer, a set of specific claims that you have invited them to verify. The gap between those two readings is where assessments fail, and the data says they fail this way constantly. A 2025 survey of active assessors found that roughly half had delayed or declined engagements because gaps surfaced during pre-award review, and approximately eighty percent identified assumed readiness without proper validation as the primary cause. Assumed readiness is, in most cases, a menu problem. The contractor

believed the document described their environment. The assessor discovered that it described an aspiration.

What follows is how that happens, in three predictable failure modes, and what the person responsible for the program can do about each one before an assessment is ever scheduled.

## Failure Mode One: Claims That Verify as Fiction

The most common SSP failure is the implementation statement that sounds complete and is verified as fiction. It comes in three recognizable varieties.

The first is policy language masquerading as implementation language. The statement reads "the organization shall enforce multifactor authentication for all privileged accounts." Read that again as an assessor. It describes an intention, not a mechanism. It names no system, no enforcement point, no scope of accounts, no owner. When the assessor reaches this statement, the questions will be specific: show me the conditional access policy, show me the enrollment status of the privileged accounts, show me the exception list, and who approved it. A statement written in the language of policy cannot answer questions asked in the language of implementation. The word "shall" anywhere in an implementation statement is a tell. Implemented controls exist in the present tense.

The second variety is vendor boilerplate. The contractor licenses a security product, copies the vendor's description of the product's capabilities into the SSP, and considers the control addressed. The statement now describes what the product can do, not what the contractor's deployment actually does. The product supports FIPS-validated encryption. Is it configured to use it? The platform can log privileged activity. Is logging enabled, retained, and reviewed in your tenant? Assessors have read the same vendor documentation you copied. They know the difference between a capability and a configuration, and they will ask for the configuration.

The third variety is the quiet future tense, a statement describing the environment the contractor intends to have. The migration, which is 90% complete, is marked as complete. The logging program that starts next quarter gets written as operating. This is the most dangerous variety, not because assessors catch it, although they do, but because of where the SSP sits in the larger compliance structure. Your SSP supports a score submitted to the Supplier Performance Risk System, and that score is a representation to the government. The Department of Justice has now settled multiple False Claims Act cases involving defense contractors whose cybersecurity representations did not match verified implementation, including the Georgia Tech Research Corporation settlement of $875,000 in September 2025 and the MORSE Corporation settlement of $4.6 million in March 2025.

An aspirational SSP is not just an assessment risk. It is documentary evidence that the gap between the claim and reality was recorded in your own building.

The discipline that prevents all three varieties is the same. Before any implementation statement goes into the menu, the kitchen test is: can we plate this dish today, on demand, for a hostile customer? If the answer includes the words “mostly,” “by then,” or “the MSP handles that,” the statement is not ready, and the honest move is to write the control into the Plan of Action and Milestones instead. A POA&M item is a dish marked as coming soon. Assessors respect coming soon. What they do not respect, and what consumes the assessment slot you waited months for, is ordering the signature dish and watching the kitchen catch fire.

One more thing about how the verdict gets rendered, because contractors consistently misjudge it. The assessor grades the food, not the menu copy, and not how good the waitress says it is. The assessment methodology gives the team three methods: examine, interview, and test. Interview is the waitress. Examine and test are the tasting. An articulate program owner, a polished narrative, a confident walkthrough, none of it moves a determination statement if the artifact and the test do not support the claim. Assessors are trained to triangulate, and when the description and the plate disagree, the plate wins every time. Contractors preparing for assessment routinely overinvest in the waitress and underinvest in the cooking. The preparation hours that matter are the ones spent in the kitchen.

## Failure Mode Two: Documentation That Contradicts Itself

The second failure mode is internal inconsistency, and it does more damage than most program owners realize, because it costs you something before a single control is evaluated: the assessor’s default assumption about your organization.

An assessment team reading an SSP is forming two judgments at once. The explicit judgment is about the controls. The implicit judgment concerns organizational maturity, and the assessor’s leading indicator of maturity is whether your documentation is self-consistent. The SSP says CUI at rest is encrypted on the file server. The network diagram, three sections later, shows a file server the SSP never mentions. The asset inventory lists fourteen CNC machines. The scoping narrative discusses nine. The SSP neglects to show the path of CUI to and from the CNC machines. The SPRS score on file implies a posture that the implementation statements do not support. None of these is necessarily a control failure. Every one of them tells the assessor that the document set was assembled rather than authored, that different hands wrote different sections at different times, and nobody read the whole thing before printing it.

An assessment team that trusts your documentation samples. A team that does not trust your documentation digs deep. The difference between those two assessments, in time, in friction, and in outcome, is enormous, and it is decided before the team arrives, by the internal consistency of the documents you sent ahead.

The consistency check is tedious and unglamorous, which is why it gets skipped. It is also entirely within the program owner's control, which is why skipping it is inexcusable. Four documents must tell one story: the SSP narrative and implementation statements; the network and data flow diagrams; the asset inventory with its CMMC asset categorizations; and the current SPRS score with its supporting assessment. Take a day. Read all four as a stranger. Every system named in any document must appear in the inventory. Every CUI flow in the narrative must appear on a diagram. Every score component must trace to an implementation statement. Where the documents disagree, they indicate that your understanding of the environment is incomplete, which is worth knowing for reasons well beyond the assessment.

## Failure Mode Three: The SSP Nobody Has Read

The third failure mode is the SSP that is accurate, consistent, professionally written, and unknown to the people who will be interviewed against it.

This is the signature failure of the outsourced SSP. A consultant or MSP writes the document, the contractor files it, and the program owner acknowledges receipt of the deliverable. Then the assessment arrives, and the assessment process does what it is designed to do: it triangulates. The assessor examines the artifact, then interviews the person responsible for the control, and checks whether the two accounts describe the same reality. Interview validation is the assessor ordering a dish and then walking into the kitchen to ask the line cook how it is made. If the cook has never seen the recipe, it does not matter that the recipe is excellent. The dish dies at the table.

The interviews are where this failure surfaces, and it surfaces in a particular way. The IT manager is asked how the audit log review works and describes a process that differs from the one in the SSP. The machinist is asked what he does when a government drawing arrives, and describes a workflow that the data flow diagram does not show. Neither person is failing. Both are honestly describing the environment. The document is the thing that was wrong, or rather, the document was right about a hypothetical company, and nobody checked it against the real one.

The fix is not training people to recite the SSP. Assessors recognize rehearsed answers, and coached consistency reads worse than honest variation. The fix runs the other direction: the SSP must be corrected until it describes what your people actually do, and your people must

have participated enough in its drafting to recognize their own work in it. If you inherited an outsourced SSP, the single highest value exercise available to you is to walk it, statement by statement, with the person who owns each control, asking one question: Is this how it actually works? Every “well, not exactly” is an assessment finding you just bought back at zero cost.

This is also the argument for why the program owner, not the consultant, must be the final author of the SSP. Outside practitioners can structure, draft, and pressure-test it. But the document makes claims about your environment in your company’s name, and the people who must defend those claims in interviews work for you. An SSP written by someone who has never set foot in your environment can be polished. It can be true only by accident.

## Writing Statements That Survive Verification

The constructive discipline comes down to writing every implementation statement against the standard the assessor will actually use, which is not NIST SP 800-171. It is NIST SP 800-171A, the companion assessment procedures document. Each of the 110 requirements in 800-171A breaks down into specific assessment objectives and determination statements that the assessor must mark as satisfied or other than satisfied. Requirement 3.1.1 is one line in 800-171. In 800-171A, there are six determinations: authorized users are identified, processes acting on behalf of users are identified, devices are identified, and access is limited to each. An implementation statement that answers the requirement but not the determinations answers the heading but not the questions the assessor is required to ask.

A statement built to survive ordering has five properties.

1. It is written in the present tense, describing what exists.
2. It names the specific systems and mechanisms involved, the actual tenant, the actual policy name, and the actual appliance.
3. It names the role or person responsible.
4. It states where the evidence lives, the configuration export, the log location, and the review record.
5. And it answers every determination statement in 800-171A for that requirement, not just the requirement heading.

A statement with those five properties is longer and less elegant than boilerplate. It is also verifiable in the order written, which is the only elegance that matters in this document.

There is one more discipline, and it is the one program owners resist most: the scoping decision must be settled before the SSP is written, not discovered during the assessment. The asset categorization, what processes CUI, what protects the things that process CUI, what is risk managed, what is genuinely out of scope, determines which controls apply to

which systems, and therefore what the menu must cover. Manufacturing environments feel this hardest. The networked machine tools, the shared drives where government drawings become G-code, the wireless network the shop floor tablets ride on, these are the assets that scoping exercises rush past, and assessors walk straight toward. If the boundary has seams, the assessment will find them, because the assessment team will walk the entire boundary you described.

## The Shorter Honest SSP Wins

Pull the three failure modes together, and a single strategic conclusion falls out, one that runs against the instinct of nearly every contractor preparing for assessment.

The instinct is to make the SSP impressive, to claim every control as fully implemented, to present the most complete posture the words can support. The instinct is wrong because of what the document is. Every claim is an order you have invited, and every claim that fails verification costs more than the honest alternative would have. The CMMC framework permits conditional certification when the assessment scores at least 88 of 110 points and every open requirement is POA&M-eligible, with 180 days to close them. A contractor presenting 92 controls that verify cleanly, along with a credible POA&M for the eligible remainder, will have a faster, smoother assessment and a defensible certification. A contractor presenting 110 claims, of which 19 collapse under examination, will face a long, adversarial assessment, a worse outcome, and an assessor who stopped trusting the document around the third failed claim and started digging.

The shorter, honest menu also protects you in the venue that matters more than the assessment itself. The SSP, the SPRS score, and the assessment record together form a documentary trail of what your company represented to the Department of Defense and when. In an enforcement environment where the Department of Justice is demonstrably willing to pursue cybersecurity misrepresentation under the False Claims Act, the contractor whose documents honestly described a partial posture with a remediation plan is in a categorically different position from the contractor whose documents described a finished posture that did not exist. One of them has a compliance program. The other has evidence against itself.

If you are the person responsible for CMMC at your company, your work is not to produce a more impressive document. It is to produce a true one, and then to improve the kitchen until the menu you want to offer is the menu you can serve. Read your current SSP the way the assessment team will, as a list of orders you have committed to fill on demand. Walk it with the people who will sit in the interviews. Reconcile it against the diagrams, the inventory, and the score. Move every claim you cannot demonstrate on demand into the POA&M, where honesty is structurally rewarded.

*The assessment team is coming to order everything on the menu. The only question you control is whether you wrote the menu for your restaurant.*

---

*David W. Koran is a CyberAB Registered Practitioner Advanced, and the author of The CMMC Decision, Second Edition. He works with Defense Industrial Base contractors on CMMC Level 2 readiness and implementation, with a particular focus on System Security Plan development and review, and on making sure contractors understand what the requirements actually demand of their environments before an assessor does.*