AMERIFUSIONGOVCON · FEDERAL COMPLIANCE PRACTICE

What a Defensible NIST 800-171 Package Looks Like

The complete documentation that has to sit behind a SPRS score when a prime contractor or contracting officer asks. System Security Plan, dated DoD Assessment, plan of action and milestones - what each one contains, how to score it, and how it holds up when someone reads it closely.

Josef Kamara

CPA · CISSP · CISA

15+ years in audit and risk · Former KPMG, BDO, Stryker

Table of Contents

Citations throughout this guide reference primary sources at acquisition.gov, ecfr.gov, csrc.nist.gov, and dodcio.defense.gov. Where industry practice differs from clause text - which it does for cyber incident reporting as of June 2025 - the guide flags both. This guide is current as of May 2026 and reflects the CMMC Phase 1 rollout that took effect on November 10, 2025.

SECTION 01

The gap a SPRS score does not close

A SPRS score is a number. A defensible 800-171 package is the evidence that the number is real.

The gap shows up in a specific moment. A prime contractor's compliance team sends an email. The subject line is some variation of *SPRS supporting documentation request*. The body is two paragraphs and one attachment: a request for the **System Security Plan**, the **basis of the score posted in SPRS**, and the **plan of action and milestones**. The contractor responds with a 14-page PDF that was last updated two years ago, a spreadsheet with 110 rows that nobody on the security team can explain, and a one-line note stating that the POA&M is "in progress." The prime escalates. The contracting officer is copied. The award gets paused.

None of that is hypothetical. It is what happens - and increasingly, with the November 2025 effective date of the CMMC contract clauses, what is starting to happen at scale. The DFARS 252.204-7019 clause has been in contracts since November 2020. The 7020 assessment requirement has flowed down to subcontractors for just as long. The 7021 CMMC clause now appears in new solicitations. And the supporting documentation behind every SPRS score is being asked for, by people who know what to look for.

The contractors who are getting flagged in 2026 are not the ones with low scores. They are the ones whose **documentation does not match their score**.

What "defensible" means here

A package is defensible when three things are true at once:

1. The **System Security Plan** describes the actual environment that processes Covered Defense Information (CDI) and Controlled Unclassified Information (CUI). Not an aspirational version of it. The system boundary in the plan matches the boundary the company operates.
2. The **DoD Assessment** in SPRS was scored against that plan, on a specific date, with a name attached, using the official DoD Assessment Methodology. Each of the 110 controls has a status that someone can defend if asked.
3. The **plan of action and milestones** is the bridge between the two. Every gap has a fix, an owner, and a date. The closeout date in SPRS - the date the contractor projects reaching a +110 - is a date the contractor can actually meet.

Most contractors have one of those three. Some have two. The ones with all three rarely get pulled into review. That is what this guide is for.

> BOTTOM LINE UP FRONT
>
> The SPRS score is the front door. The package is the building. If the building is empty, the score does not survive a serious request. This guide describes the three documents that fill it.

SECTION 02

What the regulation actually requires

Five clauses define the obligation. Read in order, they explain why the package has the shape it does.

DFARS 252.204-7012 - the safeguarding obligation

Clause 7012 is the underlying obligation. It requires the contractor to implement **NIST SP 800-171** on covered contractor information systems that process, store, or transmit Covered Defense Information. It also imposes the 72-hour cyber incident reporting requirement and, for cloud service providers handling CDI, a FedRAMP Moderate equivalency standard.

Two things are worth knowing about the current state of 7012. First, by Class Deviation 2024-O0013 (May 2, 2024), the operative version of 800-171 for DFARS purposes is **Revision 2** - 14 families, 110 controls. NIST has published Revision 3, but DoD has not transitioned DFARS or SPRS to it. A package built against Rev 3 today is a package out of step with the assessment basis. Second, the clause text still tells contractors to report incidents to `https://dibnet.dod.mil`. That portal was decommissioned on June 6, 2025. Reporting now goes to the DCISE Incident Collection Form at `icf.dcise.cert.org`. The clause and the operational reality are temporarily out of sync. A defensible package documents the contractor's playbook against the current DCISE process, not the literal URL in the clause.

DFARS 252.204-7019 - the prequalification notice

Clause 7019 is the gate. Before contract award, the offeror must have a **current** 800-171 DoD Assessment posted in SPRS. "Current" means not more than three years old, unless the solicitation requires sooner. If a solicitation contains 7019 and the offeror has nothing in SPRS, the offer is non-responsive.

DFARS 252.204-7020 - the assessment requirement and flow-down

Clause 7020 defines the assessments that 7019 references. It establishes three confidence levels:

LEVEL	CONDUCTED BY	CONFIDENCE	METHOD
Basic	Contractor (self)	Low	Review of the System Security Plan against the NIST SP 800-171 DoD Assessment Methodology.
Medium	Government	Medium	Basic review plus thorough document examination plus discussion with the contractor.
High	Government (DCMA DIBCAC)	High	Document examination, on-site or virtual system demonstration, verification, and discussion. Uses the assessment objectives in NIST SP 800-171A.

Clause 7020 also flows the assessment requirement to subcontractors. A prime cannot award a subcontract subject to 800-171 unless the subcontractor has a current Basic Assessment posted in SPRS. The flow-down is in paragraph (g), and primes are increasingly enforcing it before issuing purchase orders.

DFARS 252.204-7021 and 252.204-7025 - the CMMC contract clauses

The CMMC Program Rule at 32 CFR Part 170 took effect on December 16, 2024. The 48 CFR DFARS contract clauses that put CMMC into solicitations were published in final form on September 10, 2025 and took effect on **November 10, 2025**. That is Phase 1 of the rollout. The four-phase schedule is:

PHASE	EFFECTIVE	WHAT KICKS IN
Phase 1	Nov 10, 2025	Level 1 and Level 2 self-assessments at award.
Phase 2	Nov 10, 2026	Level 2 C3PAO certifications required at award for contracts handling CUI.
Phase 3	Nov 10, 2027	Level 2 certification extends to option exercises. Level 3 (DIBCAC) required at award.
Phase 4	Nov 10, 2028	Full implementation across all covered contracts.

The package this guide describes is what holds up under all of these clauses. The same three documents - SSP, assessment, POA&M - sit behind a SPRS score under 7019/7020 and behind a CMMC affirmation under 7021/7025. The bar rises with each phase. The shape of the package does not change.

The System Security Plan

The System Security Plan is the document that says, in writing, what is being protected and how. NIST SP 800-171 Rev 2 control 3.12.4 requires it. The DoD Assessment Methodology assesses against it. Every other document in the package depends on it.

The SSP is also the document where most defensible packages fall apart. The two failure modes are predictable. The first is a generic SSP - a 30-page template that describes a hypothetical environment, not the contractor's. The second is a stale SSP - a real description of an environment that existed two years ago and has since changed. Both fail the same test: the assessor asks a question, and the document does not answer it.

What the SSP must describe

A defensible SSP describes seven things. Each one has a specific purpose in the assessment.

1. The system boundary

What is in scope, what is out, and where the line runs. This includes a network diagram, a list of systems and applications that handle CUI, a list of facilities, a list of data flows that cross the boundary (including to managed service providers and cloud platforms), and the CAGE codes that cover the in-scope assets. Without a defined boundary, every other answer in the SSP is unverifiable.

2. The operating environment

Where the in-scope systems run. This typically resolves to a combination of on-premises infrastructure, an enclave (often a Microsoft 365 GCC High or AWS GovCloud tenant), and any external service providers. The environment description should match the system boundary diagram and should call out which components are subject to the FedRAMP Moderate equivalency requirement under DFARS 7012 paragraph (b)(2)(ii)(D).

3. CUI identification and marking

How the contractor identifies CUI when it arrives, marks it consistently per 32 CFR 2002.20, and removes the markings only on authorized destruction. DCMA DIBCAC routinely cites CUI identification gaps as a top finding. If the contractor cannot say what is CUI, the boundary in the SSP is built on sand.

4. Roles and responsibilities

Who is accountable for the program, who operates the controls, who makes risk decisions. Names or role titles, not "the IT team."

5. Implementation status of each of the 110 controls

For every Rev 2 control: implemented, planned to be implemented, partially implemented, not implemented, or not applicable. Each status must be defensible. "Implemented" requires evidence - a policy, a configuration, a procedure, a sample of execution. "Not applicable" requires a reason - what about the environment makes the

control inapplicable, and where in the system that exclusion holds. "Planned" requires an entry in the POA&M with a date.

6. Connections to external systems

Every interconnection that crosses the boundary. Cloud platforms, managed security service providers, EDR vendors, payroll, ERP, customer-facing portals. Each should be tied back to its own contractual security posture (FedRAMP authorization, DFARS 7012 flow-down, vendor 800-171 assessment) so the assessor can see how the contractor is relying on someone else's controls.

7. Continuous monitoring and review cadence

How and when the SSP is reviewed and updated. NIST SP 800-171 control 3.12.4 requires periodic update. Annual is the floor. After a material change to the environment is the practical trigger. A SSP that has not been updated since the day it was written is a SSP that no longer describes anything.

> COMMON FAILURE
>
> The single most common SSP defect is a system boundary that does not match how CUI actually flows through the company. A SSP that describes a tightly scoped enclave while the sales team forwards CUI to personal Gmail accounts is not a defensible plan. It is a fiction.

Format and length

NIST does not prescribe a format. DoD does not prescribe a format. The DoD Assessment Methodology assumes the SSP exists and assesses against it. In practice, a well-built SSP is between 40 and 90 pages. Anything shorter is almost always missing the implementation detail. Anything longer is almost always a template.

The structure that holds up best mirrors the 14 control families: an introduction with the system description, system boundary, and roles; then 14 sections - one per family - each describing the controls in that family with implementation detail and supporting evidence references; then appendices with the network diagram, the asset inventory, the CUI handling procedure, and the interconnection register. The POA&M is its own document, not a SSP appendix.

The dated DoD Assessment

The second document is the assessment itself. It is the document that produces the SPRS score. The clause that governs how it is conducted is the NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, dated June 24, 2020. Every Basic Assessment posted in SPRS is supposed to have been conducted against this methodology. Many were not.

How the score is built

The contractor starts at **+110** - one point per Rev 2 control, fully implemented. For each control that is not fully implemented, the methodology deducts **1, 3, or 5 points**, depending on the criticality classification in Table 1 of the Methodology. There are 42 controls weighted at 5 points, including all 17 of the FAR 52.204-21 basic safeguarding requirements. The lowest possible score is **-203**. The range is -203 to +110.

Two scoring conventions matter in practice. First, partial implementation is not a partial deduction. A control is implemented or it is not. If it is not, the full point value of the control comes off the score. The exception is a small set of controls in the Methodology that allow scaled deductions where partial implementation is meaningful - those are explicitly identified in Table 1. Treating other controls as scalable inflates scores and produces a posted number that does not survive a Medium or High Assessment. Second, controls scored as "Not Applicable" must have a documented basis in the SSP. NA is not a way to skip a control the contractor does not want to address.

What the assessment document looks like

The assessment is more than a score. The defensible version is a workbook - typically organized by the 110 controls - with the following columns:

- **Control reference.** The 800-171 Rev 2 identifier (e.g., 3.1.1, 3.13.11).
- **Status.** Implemented, partial, planned, not implemented, not applicable.
- **Score impact.** 0, -1, -3, or -5.
- **Implementation summary.** One to three sentences describing how the control is met in the contractor's environment. This is where the SSP and the assessment connect - the implementation summary should reflect the SSP language.
- **Evidence reference.** Where the supporting evidence lives. Policy ID, configuration screenshot, log sample, training record. The evidence does not need to be embedded in the workbook, but it must be retrievable.
- **Assessor.** The name of the person who scored the control.
- **Date.** The date the control was assessed.
- **POA&M reference.** If the status is partial, planned, or not implemented, the corresponding POA&M item.

An assessment document that has all eight columns, populated with substance, is a document that can be defended in front of a DIBCAC team. An assessment document with three columns - control, status, and score - cannot.

What the SPRS posting requires

SPRS itself accepts five fields per assessment: the summary level score, the date of the assessment, the scope (CAGE codes covered and a brief system description), the system security plan summary, and the projected closeout date - the date the contractor expects to reach +110. Each of those fields has a longer form behind it. The score traces to the workbook above. The date traces to who signed off. The scope traces to the SSP boundary. The closeout date traces to the POA&M. The SPRS portal entry is the visible tip of the package, not the package itself.

SPRS releases a new version periodically; the production release as of February 2026 is 4.1.3. The portal lives at sprs.csd.disa.mil. Posting requires a Cyber Vendor User role in the Procurement Integrated Enterprise Environment.

> A NOTE ON REV 3
>
> NIST SP 800-171 Revision 3 is final as of May 2024 and reorganizes the framework into 17 families and 97 requirements with 88 organization-defined parameters. DoD has issued ODP values in a memorandum dated April 2025, but Class Deviation 2024-O0013 keeps DFARS and SPRS on Revision 2. Until DoD issues a deviation rescission and SPRS accepts Rev 3-based scoring, the assessment basis for a defensible package is Rev 2.

The Plan of Action and Milestones

The POA&M is the third document. NIST SP 800-171 Rev 2 control 3.12.2 requires it: develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities. The POA&M is the bridge between the score the contractor has and the +110 the contractor is committing to reach. It is a contract with the future, signed by the present.

The POA&M is also the document where most contractors lose credibility. The two failure modes are again predictable. The first is the open-ended POA&M - every line item closes "Q4 2027" or some other date set far enough out that no one will remember to ask. The second is the closeout-on-paper POA&M - every line item shows "complete" on its planned date, regardless of whether the work was actually done. Both fail the same test: an assessor looks at the closeout dates against the in-place assessment date and sees that the math does not work.

What a defensible POA&M item contains

A POA&M item is a single row with the following fields:

FIELD	WHAT GOES IN IT
POA&M ID	A stable identifier (e.g., POAM-2026-014). The number does not change when the date does.
Control	The 800-171 Rev 2 control the item closes (e.g., 3.13.11 - employ FIPS-validated cryptography).
Deficiency description	What is missing or partial today. Specific, not generic. "FIPS-validated TLS not enforced on the legal hold archive" beats "encryption gap."
Resources required	Budget, labor, third-party. If the answer is "TBD" the item is not yet planned.
Milestones	The intermediate steps with dates. A POA&M item with one date is a wish.
Owner	Named individual accountable for closeout. Not "IT."
Target completion date	The date the deficiency is fully remediated.
Status	Open, in progress, complete, deferred.
Closeout evidence	What demonstrates the deficiency is closed. Configuration export, screenshot, policy approval, audit log.

Realistic remediation timelines

A POA&M is judged on whether its dates are believable. The following ranges are what assessors expect to see for the most common gap types - not ceilings, but defensible windows.

GAP TYPE	TYPICAL WINDOW	WHY
Policy or procedure missing or stale	30 to 60 days	Drafting, review, leadership approval, distribution.
Access control configuration (MFA, least privilege)	60 to 120 days	Tooling configuration, role review, exception cleanup.
FIPS-validated cryptography enforcement	90 to 180 days	Inventory of crypto in use, replacement of non-validated modules, verification.
Audit log retention and protection	90 to 180 days	SIEM tuning, retention policy, integrity protection, access review.
Incident response capability build	120 to 240 days	Plan, runbook, tooling, tabletop exercise, lessons learned.
FedRAMP-equivalent CSP transition	9 to 18 months	Procurement, migration, data handling change, recertification.
System-wide architecture change (boundary redesign, enclave migration)	12 to 24 months	Design, procurement, migration, validation, decommission.

Two implications fall out of this. First, the SPRS closeout date - the date the contractor projects reaching +110 - must be at least as far out as the longest open POA&M item. A closeout date of December 2026 with an enclave migration POA&M dated September 2027 is internally inconsistent. Second, when a POA&M item slips, the SPRS closeout date should be re-posted. A plan that does not move when reality moves is not a plan.

POA&Ms under CMMC

Under the CMMC Program Rule at 32 CFR Part 170, POA&Ms are permitted only on a limited subset of Level 2 requirements (those weighted 1 point in the Assessment Methodology) and only when the score meets a minimum threshold. A Conditional certification is granted when a POA&M is in place; it expires after a closeout window defined in the Program Rule. For contractors operating in Phase 1, that window matters: a Conditional that lapses without closeout costs the certification. The POA&M format above carries through. The bar for closeout evidence rises.

SECTION 06

Two anonymized case studies

The patterns in this guide are abstract until they meet a real package. The two case studies below are anonymized composites drawn from contractors I have worked with. Identifying detail is altered. The pattern is not.

Case study one - the high score that did not survive

TIER 2 SUPPLIER · AEROSPACE

Posted SPRS score	+98
Self-asserted closeout date	March 2025
Triggering event	Prime contractor compliance team requested supporting documentation following an internal audit.
What the prime found	The SSP had been written by a third-party consultant in 2022 and had not been touched since. The system boundary described an on-premises Windows domain. The contractor had migrated to Microsoft 365 GCC High in mid-2023. The 2022 SSP did not mention M365 at all. Twelve controls scored as "implemented" referenced policies that no longer existed.
What followed	Subcontract performance was paused for 47 days while the contractor rebuilt the SSP, re-ran the assessment against the actual environment, posted a corrected score of +71, and committed to a +110 closeout date 14 months out.
What changed structurally	The contractor moved SSP ownership in-house. A quarterly review cadence was established with a documented change log. The corrected SPRS score became the operational anchor.

The lesson. A high SPRS score is not a defensible position if the SSP behind it describes the wrong system. The number is not the package. The package is the package.

Case study two - the low score that held

TIER 3 SUPPLIER · MANUFACTURING

Posted SPRS score	+34
Self-asserted closeout date	August 2027
Triggering event	DCMA DIBCAC Medium Assessment as part of a contract award process.
What the assessor found	The SSP was 62 pages, written in plain language, with a current network diagram dated within 90 days of the assessment. Every control had an implementation status, an evidence reference that resolved when sampled, and a POA&M ID where applicable. The POA&M had 38 open items, each with milestones, owners, and dates that traced to the +110 closeout date. The assessor sampled 12 controls and found documentation that matched the SSP description in every case.
What followed	The Medium Assessment confirmed the +34 score within 4 points. The contract was awarded with the existing closeout date. The contractor was treated as a credible counterparty despite the low score.
What changed structurally	Nothing. The contractor had built the package the right way the first time. The assessment validated existing practice rather than creating new work.

The lesson. Defensibility is not the same as a high score. A low score with a credible package is more defensible than a high score with a fictional one. The assessor is reading for consistency, not for inflation.

SECTION 07

What primes and contracting officers actually ask for

The supporting documentation request is rarely a single email. It is a sequence. The contractor who responds well to the first email rarely receives the second. The contractor who responds badly to the first email receives every subsequent question with greater scrutiny.

Below is the pattern as it shows up in 2026. Each request is a real question that has been asked, organized in the order it tends to come.

The first request - supporting documentation

1. The current System Security Plan, including the system boundary diagram and the implementation status of all 110 controls.
2. The DoD Assessment workbook that produced the SPRS score, with assessor name, assessment date, and methodology version.
3. The Plan of Action and Milestones, including milestones, owners, and target dates for each open item.

The second request - calibration

1. How the contractor identifies CUI on receipt and how it is marked, transmitted, stored, and destroyed.
2. The list of cloud service providers in the boundary and the FedRAMP authorization or equivalency status of each.
3. The interconnection register and the basis on which each external system is trusted.
4. The cyber incident response plan, with the current reporting playbook (DCISE since June 2025, not the legacy DIBNet URL).

The third request - control sampling

Three to five controls, selected from the SSP's "implemented" list, with a request for the underlying evidence. Common samples:

- **3.1.1** - Limit system access to authorized users. Request: identity and access management policy, sample access review record, sample disabled-on-termination evidence.
- **3.1.5** - Employ the principle of least privilege. Request: privileged access matrix, sample quarterly privileged-access review.
- **3.5.3** - Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. Request: configuration export, sample of MFA-enforced login event from logs.

- **3.13.11** - Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. Request: cryptographic inventory, FIPS 140-2 or 140-3 certificate references, sample TLS configuration.
- **3.14.1** - Identify, report, and correct system flaws in a timely manner. Request: vulnerability management policy, sample patch cadence report, sample exception register.

If the SSP describes these controls as implemented and the evidence does not exist, the assessor's view of every other "implemented" control degrades. Sampling three controls is, in effect, a sampling of the SSP's overall credibility. Building a SSP that survives sampling is the single highest-leverage activity in the whole package.

> PRACTITIONER NOTE
>
> The package the contractor builds for a Medium or High Assessment is the same package that responds to a prime contractor's documentation request. Building it once, well, eliminates the second build. Most contractors build it twice - once defensively, after the prime asks, and once retroactively, after the assessor finds the gap.

ABOUT THE AUTHOR

Who wrote this and how to use it

I am Josef Kamara - a CPA, CISSP, and CISA with fifteen-plus years of audit and risk experience across **KPMG**, **BDO**, and **Stryker**. At BDO, I led both the third-party attestation practice (SOC 1, SOC 2, ISAE 3402) and the information assurance team. At Stryker, I managed the IT audit function across a regulated medical-device manufacturer with substantial federal and contract exposure. I founded **AmerifusionGovCon**, the federal contracting readiness practice at amerifusiongovcon.com, to deliver clause-level federal compliance work to defense contractors and agency program offices.

This guide is the document I would hand a defense contractor at the start of a SPRS readiness engagement. Read in order, the three documents - the SSP, the dated assessment, and the POA&M - define a defensible package. The case studies and the request patterns explain how the package gets tested in the wild. The clauses cited throughout are the regulatory floor; everything in this guide is consistent with them as of May 2026.

How to use what you have just read

1. **Audit the SSP first.** Read it against the seven elements in Section 03. If three or more are weak, the package will not hold up. The SSP is the foundation.
2. **Reconcile the assessment to the SSP.** Every "implemented" control should resolve to evidence the SSP describes. Where it does not, either the SSP is wrong or the score is.
3. **Build the POA&M with believable dates.** The closeout date in SPRS should match the longest open milestone. If it does not, fix one or the other.
4. **Repost when reality moves.** A SPRS score that has not been updated when the environment has materially changed is a posted statement that no longer matches the truth. That is the gap a prime is looking for.

- Josef Kamara
CPA · CISSP · CISA

Ready to pressure-test your package?

AmerifusionGovCon delivers SPRS readiness reviews and DFARS 7012/7019/7020/7021 documentation builds for defense contractors. Bring us the SSP, assessment, and POA&M you have today. We tell you what survives a prime's request, and what does not.

Schedule a SPRS readiness consultation →

Citations: DFARS 252.204-7012, 7019, 7020, 7021, 7025 · NIST SP 800-171 Rev 2 · NIST SP 800-171 Rev 3 (forward-looking) · DoD Assessment Methodology v1.2.1 · 32 CFR Part 170 · 32 CFR 2002.20 · Class Deviation 2024-O0013 · SPRS portal · DCMA DIBCAC.