AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

★★★
2026

The Plan the Assessor Reads: System Security Plans That Match the System

System & Application Security Plans (SSP): system-specific control narratives, accurate statuses and verified inheritance, written for the people who assess and sign.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary **2**

Why System Security Plans Go Stale **3**
How the Need Sounds 3
Common Triggers 3

What Changed in 2025 and 2026 **4**
FedRAMP Certification Covers the Offering, Not Your System 5
Defense Systems 5
Contractor Systems 5

What the Service Does **5**
What a Good Narrative Looks Like 6

Deliverables **8**

How an Engagement Runs **9**
What the Agency Provides 9
What Is Not Included 10

How Avalon Staffs It **10**

Pricing and How to Buy **12**

Illustration: Building the Price for a New Moderate SSP **12**

Common Pitfalls **15**

Conclusion and Next Step **15**

Appendices **16**
Appendix A: Glossary 16
Appendix B: Illustration Assumptions 16
Appendix C: References 17

Executive Summary

Every federal authorization rests on the System Security Plan. It defines the system's boundary, records its FIPS 199 categorization, inventories what sits inside the boundary, and states, control by control, how each requirement is implemented, inherited or justified as not applicable. The assessor tests against it. The Authorizing Official (AO) signs on it. When it is stale, generic or wrong, the authorization stalls, and an expiring ATO pushes the agency toward an extension memo nobody wants to sign.

Plans go stale for ordinary reasons. The ISSO who knew the system leaves, often unreplaced after the 2025 and 2026 workforce reductions. A cloud migration moves the boundary. Template narratives never described the system in the first place. And 2026 brought new FedRAMP rules, a new DoD risk construct, new OMB logging and CISA remediation policy, and a suspended CMMC phase.

This paper is written for system owners and program managers, ISSOs and ISSMs, CISO and OCIO authorization branches, and the contracting officers and CORs who buy the work. It describes Avalon Technology Services' System & Application Security Plans service, which comes in three shapes:

- **An SSP update or annual refresh** for an existing plan on a changed system, typically 3 to 5 weeks.
- **An application-level plan** for an application that rides inside an existing parent authorization boundary.
- **A new SSP for a moderate-baseline system,** delivered over a 10-week plan in the agency's template or GRC tool.

Section 9 builds the fixed price for an illustrative new moderate-baseline plan from its parts: 260 tailored controls, 35% inherited, minutes per narrative by implementation status, 12 interviews and two QA cycles. The result is about 396 hours over 10 weeks and a fixed price of $55K, with the agency's own ISSO spending about 51 hours on reviews and interviews instead of writing the plan.

The service writes and validates the plan. The system owner owns it. Assessment belongs to the agency's assessor, and the authorization decision belongs to the AO.

Why System Security Plans Go Stale

Risk	How it shows up
Authorization	Without a current, accurate plan, the assessor has nothing valid to test against and the AO has no defensible basis for a risk decision. Packages get kicked back for template language, wrong statuses or a boundary that does not match the system.
Accountability	A plan that marks a control implemented when it is not misrepresents the system to the person signing for it. An accurate plan with honest "planned" statuses and a real POA&M protects the signatories; a falsely clean one exposes them.
Audit	IG and FISMA audit cycles regularly cite missing or outdated system documentation. Each finding lands on the CISO's portfolio and the ISSO's desk.
Continuity	The plan is institutional memory. When the ISSO who maintained it leaves, its accuracy usually leaves too. Meanwhile, cloud migrations and continuous deployment change the system faster than the document.

How the Need Sounds

"Our package got kicked back." "The controls are marked implemented, but there are no narratives." "We're in eMASS, but half the fields are empty." "The AO briefing is in eight weeks and the plan isn't ready." "The boundary diagram doesn't match what's deployed." Each of these is this service.

Common Triggers

- An ATO approaching expiration on its three-year cycle, or an extension memo the AO is reluctant to sign again
- A new system, a major upgrade or a cloud migration that creates or changes a boundary
- An assessment kickback, or an IG, FISMA or GAO finding citing missing or outdated plans

- An ISSO departure that leaves an orphaned package
- Year-end O&M funds, mid-August through September, meeting any of the above

What Changed in 2025 and 2026

Date	Event	What it means for the plan
September 24, 2025	DoD announces the Cybersecurity Risk Management Construct (CSRMC)	Direction of travel for DoD; RMF, DoDI 8510.01 and eMASS remain in use, so plans are still built and maintained there
May 2026	OMB M-26-14 replaced M-21-31 with a risk-based logging model	Audit and logging (AU) narratives that cite the old maturity tiers need rewriting
June 10, 2026	CISA BOD 26-04 replaced BOD 22-01 and BOD 19-02	Flaw remediation and vulnerability narratives (SI-2, RA-5) at civilian agencies should reflect the new risk-based clocks
June 25, 2026	FedRAMP Consolidated Rules published	Cloud offerings become "FedRAMP Certified" in Classes A through D, with machine-readable, continuous evidence as the direction
July 13, 2026	CMMC Phase 2 suspended	Phase 1 self-assessment and NIST SP 800-171 obligations, including the contractor SSP, remain
June 11, 2027	New FedRAMP Rev5 submissions stop	Legacy-format cloud packages have a clock on them
December 31, 2028	FedRAMP Rev5 authorizations end	Agency plans that inherit from Rev5-authorized offerings need inheritance updated as providers move

FedRAMP Certification Covers the Offering, Not Your System

A FedRAMP Certified cloud offering is a strong source of inherited controls, but the certification covers the provider's offering only. The agency still authorizes its own system, and the plan still has to show, control by control, which parts the provider covers and which the agency implements. That means reading the provider's package and customer responsibility matrix rather than assuming the inheritance.

Defense Systems

DoD systems are still authorized under the RMF in DoDI 8510.01, with eMASS as the system of record. DoD announced CSRMC on September 24, 2025, and the continuous ATO (cATO) memo of February 2, 2022 remains the reference for continuous authorization. Both raise the bar on plan currency: a continuous authorization still rests on a living, accurate plan.

Contractor Systems

Contractors handling CUI need an SSP of their own under NIST SP 800-171 requirement 3.12.4, the basis of their self-assessment. With CMMC Phase 2 suspended since July 13, 2026, Phase 1 self-assessment and the 800-171 obligations remain. The craft is the same; the requirement set differs.

What the Service Does

The work is six activities, each done against the system as it actually is, not as an earlier plan described it.

Activity	What it covers
1. Boundary and categorization validation	Confirms the authorization boundary, the FIPS 199 impact level for each information type and the resulting baseline, and flags categorization decisions that look wrong before they shape the whole plan
2. System characterization	Mission and purpose, environment, component inventory reconciliation, network and data-flow diagrams, ports, protocols and services (PPSM format for DoD), user types and privileges, and interconnections feeding the agency's CA-3 agreements
3. Control implementation statements	For every control in the tailored baseline (roughly 150 to 350 or more), a specific statement of who performs it, what mechanism enforces it, how it works on this system and where the evidence lives, with an accurate status
4. Supporting appendices	Rules of behavior, applicable laws and regulations, digital identity determination, a separation-of-duties matrix, and pointers to companion plans
5. GRC population	Entry or import into eMASS, CSAM, Xacta, ServiceNow IRM, or an OSCAL file, wherever the agency's process lives
6. Validation	A structured walkthrough with the ISSO or ISSM and system SMEs, plus an internal assessor-lens QA review that reads each narrative the way a control assessor will

What a Good Narrative Looks Like

The difference between a plan that holds up and one that gets returned is activity 3. A template narrative restates the control. A system-specific one names the mechanism: which directory provisions accounts, who approves them, how often they are reviewed and where the records are kept. Every narrative carries one of five statuses, and each status has a rule.

Status	Rule
Implemented	Written in the present tense, describing a mechanism that exists today, with an evidence pointer
Partially implemented	States what is in place, what is missing, and the gap log entry that tracks the rest
Planned	States the intended mechanism and routes the control to the gap log for POA&M intake; never dressed up as implemented
Inherited	Names the providing system or offering and is checked against its package and customer responsibility matrix, including any shared customer portion
Not applicable	Carries a tailoring justification the AO's representative can accept

Accurate "planned" statuses are not a weakness in the plan. They are what the POA&M is for, and they protect the people who sign.

Deliverables

Deliverable	Format
System Security Plan	Word or PDF on the agency template or the NIST SP 800-18 structure; populated GRC records; or OSCAL JSON or XML where required
FIPS 199 categorization worksheet	Agency template, ready for signature
Boundary and data-flow diagrams	Visio or draw.io source plus embedded images
Inventory reconciliation	Excel or CSV, structured for reuse as CM-8 evidence
Control implementation workbook	A traceability matrix: control, status, narrative, evidence pointer
Gap log	Deficiencies found while drafting, formatted for direct POA&M intake
Maintenance guidance	A 2 to 3 page procedure for keeping the plan current under continuous monitoring

The plan satisfies the documentation requirements of NIST SP 800-53 Rev. 5 control PL-2 (System Security and Privacy Plans) and supports PL-8, PL-10 and PL-11, RA-2, CM-8, CA-3 and CA-9, and SA-9 and AC-20. In RMF terms it is the Task S-4 output that the AO or a designated representative reviews at Task S-6, updated with as-implemented detail at Task I-2 and kept current in the Monitor step.

How an Engagement Runs

Phase	Weeks	What happens
Kickoff and scoping	1	Boundary and categorization validation, artifact inventory, interview schedule, GRC account requests
Discovery	2–4	SME interviews, configuration and document review, inventory reconciliation
Drafting	3–8	Control narratives, diagrams and appendices, delivered by control family as they finish
Validation and QA	8–9	SME verification, assessor-lens QA, ISSM walkthrough, comment adjudication
Finalization and handoff	10	Final plan or GRC population, gap log, maintenance guidance

An update to an existing plan compresses to 3 to 5 weeks. A high baseline or a portfolio of systems extends roughly in line with control count and access friction.

What the Agency Provides

- System SMEs available 2 to 6 hours a week for interviews.
- Existing artifacts in week 1: the prior SSP and assessment report, inventory, diagrams and the policies the plan cites.
- GRC accounts, requested at kickoff. eMASS and CSAM accounts routinely take 2 to 4 weeks and are the most common schedule risk.
- One named decision-maker who resolves boundary questions within five business days.
- Schedule relief written into the SOW when government-furnished items slip, so delay is attributed correctly.

What Is Not Included

Included	Separate work
Documenting how controls are implemented	Implementing or remediating the controls
A gap log formatted for POA&M intake	Managing the POA&M after assessment
Pointers to the policies the plan cites	Writing those policies
Pointers to companion plans	Contingency, incident response and configuration management plans (optional add-on lines)
Assessor-lens QA of Avalon's own draft	The formal assessment (SAP, SAR, testing); never of a plan Avalon wrote
The plan the AO reviews	Authorization shepherding, AO briefings and the authorization decision

Accurate	Not accurate
A System Security Plan satisfying PL-2 and RMF Task S-4 and I-2 documentation requirements, built to a stated quality standard	"This SSP will get you your ATO"
Narratives and statuses that match observed reality	"The system is compliant with 800-53"
Acceptance criteria based on completeness and quality	Any promised assessment result or time to ATO

How Avalon Staffs It

Avalon takes one engagement at a time, unclassified only. Each engagement is staffed with named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal, and a key-personnel clause is welcome. Avalon has no past federal engagements under this service and says so before it is asked. The

offset: a small first task under the simplified acquisition threshold, fixed-price milestones so the agency never pays ahead of accepted work, and a redacted sample narrative to judge before award.

Role	Share of the engagement	Condition of the engagement
Lead SSP author	0.5 to 0.75 FTE; also the project manager	Hands-on RMF package experience and a CISSP or CGRC credential, documented in the proposal
Technical SME	0.2 to 0.3 FTE	Interviews, diagrams, inventory and GRC entry; depth in the system's platforms
Assessor-lens QA reviewer	About 0.1 FTE	Independent of the drafting; reads every narrative as an assessor would
Access	All roles	Public Trust or other investigation at the level the agency requires; DoD 8140 qualification where the role is designated
CUI handling	All roles	A documented, access-controlled environment for system documentation, agreed in writing before the first artifact is transferred

Avalon never assesses a plan it wrote and discloses any prior work on the system before award. Deliverables convey with government-purpose rights.

Pricing and How to Buy

Shape	Market-norm range
SSP update or annual refresh	$8K–$25K
Application-level plan inside an existing parent boundary	$15K–$30K
New SSP, moderate-baseline standalone system	$30K–$75K
Time and materials, senior A&A documentation labor	$115–$210 an hour, loaded

Work is offered as firm fixed price with three milestone payments: draft plan delivered, plan validated after the ISSM walkthrough, and final handoff. There is no contingency or outcome-based pricing, because pricing tied to an authorization outcome would imply a guarantee no vendor can make.

Every shape fits under the $350,000 simplified acquisition threshold, so a plan can be bought as an open-market purchase, often with year-end O&M funds. Purchases between the $15,000 micro-purchase threshold and the SAT are generally set aside for small business when two or more capable small businesses are expected to compete. Plan work inside a larger ATO or RMF task order can be subcontracted to Avalon by the prime. Avalon does not hold a GSA Schedule or a governmentwide contract today.

Illustration: Building the Price for a New Moderate SSP

The figures below are planning assumptions for one representative unclassified moderate-baseline system, not a quote and not a result from any engagement. They show how the fixed price is built so a COR can test it.

Status	Controls	Drafting minutes each	Hours
Implemented	101	45	76
Partially implemented	31	60	31
Planned	24	35	14
Inherited (verified against the provider CRM)	91	25	38
Not applicable	13	10	2
Total	260		161

Drafting minutes assume the interviews are done. Interviews are fixed at 12 in the SOW, at 2.5 lead hours each for preparation, a 90-minute session and notes. Assessor-lens QA reads every control once at 6 minutes and re-reads 30% after revisions; there are 2 ISSM review cycles.

Role	Main tasks	Hours	Share of 10 weeks
Lead SSP author	Narratives 161, interviews 30, review cycles 24, boundary, appendices, gap log, management	264	0.66 FTE
Technical SME	GRC population 35, diagrams 20, interviews 18, inventory, PPSM and interconnections	99	0.25 FTE
Assessor-lens QA	Two QA passes	34	0.08 FTE
Total		396	

At loaded rates of $140, $125 and $160 an hour, inside the market band, the labor comes to $54.7K, and the fixed price is $55K: about the middle of the $30K–$75K band for a new moderate plan. The milestones are $22,000 at the draft, $19,250 at validation and $13,750 at handoff. Each role's share sits inside the staffing model in Section 7,

and the total of about 396 hours is at the top of the 200 to 400 focused hours a moderate plan usually takes, because it includes GRC entry and two QA passes.

Filled week by week at each role's capacity, the narratives finish in week 8, the review cycles in week 9 and GRC population in week 10, so the plan fits the 10-week schedule with little slack. The agency's side is about 51 hours: interviews, two ISSO review cycles and boundary decisions. That is the answer to "our ISSO can write this": the ISSO reviews, corrects and owns the plan, without writing it.

Scenario	Hours	Fixed price	Handoff week
Base case	396	$55K	10
GRC accounts 2 weeks later than planned	396	$55K	10
GRC accounts 4 weeks later than planned	396	$55K	11
20% of controls inherited	410	$57K	10
50% of controls inherited	382	$53K	10
Boundary change: one enclave added in week 5	396 + 61	$55K + $8.5K change order	13

GRC accounts. The plan assumes accounts are usable by week 5, the long end of the routine 2 to 4 weeks. Because population is scheduled late, a further 2-week delay is absorbed. A 4-week delay moves handoff to week 11. The work does not change, so the price does not either; the SOW's schedule relief covers it.

Inheritance. At 20% inherited the plan takes about 410 hours and $57K; at 50%, about 382 hours and $53K. The share is confirmed at kickoff against the provider's package, not assumed in the proposal.

Boundary change. One added enclave or interconnection in week 5 means new diagrams, inventory and interconnection work, about 15 new controls, and rework on a fifth of the narratives already drafted: roughly 61 more hours, an $8.5K change order, and handoff in week 13. The baseline and tailoring are fixed at kickoff for exactly this

reason, and a boundary change is a written change-order trigger, not something absorbed silently.

Common Pitfalls

Pitfall	How to avoid it
"Document the control" becomes "implement the control"	Implementation is separate work with its own scope and price
The plan task absorbs policy writing	Policies and companion plans priced as optional line items
A mid-engagement boundary change doubles the control surface	Baseline and tailoring fixed at kickoff; boundary change as a change-order trigger
Finding management absorbed after delivery	POA&M management out of scope; the gap log is the handoff
Future tense on controls marked implemented	Assessor-lens QA checks tense against status on every narrative
Narratives copied across systems or from templates	Who, what, how and where for this system, or the narrative is rewritten
Inheritance claimed without reading the provider's package	Each inherited control checked against the package and customer responsibility matrix
Inventory and diagram disagree with each other or the live system	Inventory reconciliation before diagrams are finalized

Two misconceptions to correct early: the SSP is not the ATO, only one input to it; and the template is a small part of the work, while verified, system-specific narratives are the rest.

Conclusion and Next Step

An SSP describes a real system for the people who will test it and sign for it, and it earns their trust by being specific and accurate, including about what is not done yet. The rules under the plan moved a great deal in 2026, but the craft did not: confirm the

boundary, verify the inheritance, write what is actually there, and hand the gaps to the POA&M.

The natural first step is a small, fixed-price task under the simplified acquisition threshold: an update to one plan or an application-level plan inside an existing boundary, with acceptance criteria written on completeness and quality. To discuss one, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

AO
Authorizing Official: the senior official who accepts the risk of operating a system and signs the authorization decision.

CRM
Customer responsibility matrix: a provider's statement of which control parts it covers and which remain with the customer.

FIPS 199
The federal standard for categorizing information and systems by impact level.

ISSO / ISSM
Information system security officer and manager: the agency staff who maintain a system's security posture and its package.

OSCAL
NIST's Open Security Controls Assessment Language, a machine-readable format for plans and assessment data.

POA&M
Plan of action and milestones: the record of known weaknesses and how they will be fixed.

SSP
System Security Plan: the document describing a system's boundary, categorization and control implementation.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative system. None is drawn from a specific agency or a completed engagement.

Assumption	Value	Basis
Tailored controls	260 controls and enhancements	Inside the roughly 150 to 350 or more range
Inherited / not applicable	35% / 5% (20% and 50% inherited as alternates)	Planning assumption
Status mix of the rest	65% implemented, 20% partial, 15% planned	Planning assumption
Drafting minutes	45 / 60 / 35 / 25 / 10 by status	Planning assumption
Interviews	12 at 2.5 lead hours; SME attends	Fixed in the SOW
QA and review	6 min per control, 30% re-read; 2 review cycles	Planning assumption
GRC entry	8 min per control; accounts usable week 5	Government-furnished accounts
Weekly capacity	Lead 30 h, SME 12 h, QA 6 h	Staffing model in Section 7
Rates and price	$140 / $125 / $160 an hour; fixed price rounded up to the next $1,000	Inside the $115–$210 band and the $30K–$75K band

Appendix C: References

1. **National Institute of Standards and Technology**, *SP 800-18, Guide for Developing Security Plans for Federal Information Systems* https://csrc.nist.gov/pubs/sp/800/18/r1/final
2. **National Institute of Standards and Technology**, *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations* https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
3. **National Institute of Standards and Technology**, *SP 800-53B, Control Baselines for Information Systems and Organizations* https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final

4. **National Institute of Standards and Technology**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*
https://csrc.nist.gov/pubs/sp/800/37/r2/final

5. **National Institute of Standards and Technology**, *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
https://csrc.nist.gov/pubs/fips/199/final

6. **National Institute of Standards and Technology**, *SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

7. **National Institute of Standards and Technology**, *Open Security Controls Assessment Language (OSCAL)*
https://pages.nist.gov/OSCAL/

8. **Office of Management and Budget**, *Circular A-130, Managing Information as a Strategic Resource*
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

9. **FedRAMP**, *FedRAMP program site and Consolidated Rules*
https://www.fedramp.gov/

10. **Department of Defense**, *DoDI 8510.01, Risk Management Framework for DoD Systems*
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

11. **DoD Chief Information Officer**, *Cybersecurity Maturity Model Certification*
https://dodcio.defense.gov/CMMC/

12. **Centre Law & Consulting**, *Inflation Updates to FAR Thresholds: What Changed on October 1, 2025*
https://centrelawgroup.com/blog/inflation-updates-to-far-thresholds-what-changed-on-october-1-2025/