The Mission App Builder Guide

From SBIR Award to Authorized Deployment in 90 Days

A Pandora Cloud Guide

April 2026

Pandora Cloud LLC
Women-Owned Small Business (WOSB) | AWS Advanced Partner
GSA MAS: 47QTCA24D00D3 | CAGE: 9JSG7 | UEI: R36GQ3N4XT63
Secret Facility Clearance | pandoracloud.net

About This Guide

This guide is written for Small Business Innovation Research (SBIR) companies in Phase I, Phase II, or transitioning to Phase III, plus emerging defense primes and small defense contractors building applications that will run in a Department of Defense (DoD) or federal civilian agency cloud. If you are sitting on a contract or grant, you have a delivery milestone, and the words "Authorization to Operate (ATO)" have started showing up in your customer's email signatures, this is for you.

If you are a venture-funded commercial SaaS company exploring the federal market, parts of this guide will translate. The IL2/IL4/IL5 framing, the inheritance map, and the conversation cheat sheets are useful regardless of how you got into the federal market. The 90-day plan assumes the contract structure typical of SBIR and small defense awards.

This guide assumes you already have an application or a clear application concept. It does not teach you how to build software; it tells you how to put the software you build into a cloud environment that can be authorized to run mission data without consuming the rest of your contract budget.

Reading time: 30 minutes. Save it, print it, share it with your CTO and program manager. The decisions in this guide compound; the cost of making them late is much higher than the cost of making them now.

What's In This Guide

Section 1: The 90-Day Path vs. the 18-Month Path

Every mission application has the same fork in the road, and most teams take the wrong branch by accident.

The wrong branch looks like this. Phase II award lands. The engineering team gets to work on the application. Six months in, the customer asks where the system will run. The team starts a separate workstream to stand up infrastructure. The infrastructure work lengthens. Authorization paperwork starts. The infrastructure work lengthens again. By month twelve, the application is feature-complete and waiting on an environment that is not yet authorized. By month sixteen, the funding is mostly gone and the deployment milestone has slipped twice. By month eighteen, the contract is at risk, the team has spent most of its budget on infrastructure and compliance, and the application that was supposed to deliver capability is sitting in a development environment that the customer cannot use.

We have walked into this engagement, in some form, more times than we can count. The team that started behind on infrastructure stays behind on infrastructure. The cost of catching up is a quarter to a half of an SBIR Phase II budget, and the timeline cost is six to nine months of slip.

The right branch looks like this. Award lands. The first decision the team makes is the cloud environment, before a single line of application code is written. The team chooses a pre-authorized landing zone at the right Impact Level for the contract, signs the inheritance documentation, and stands the environment up in two to three weeks. From day one, every architectural decision the application team makes happens inside a known compliance boundary, with a known set of inherited controls, and with a Plan of Action and Milestones (POA&M) template already started for the controls they own. By month three, the application is deployed in an authorized environment. By month six, the customer is using it.

This is not a difference in technical talent. The teams that take the second branch are not better engineers. They are working against a different decision tree, and the difference between that decision tree and the default one is the difference between a delivered mission capability and a stalled SBIR pursuit.

The rest of this guide is the decision tree.

The numbers behind the fork

A standalone Authority to Operate for a government cloud environment typically runs $400,000 to $500,000 and takes 12 to 18 months. Inheriting from a pre-authorized landing zone reduces that to roughly three months of deployment time and shifts the cost from one-time ATO buildout to predictable monthly operating cost. For a Phase II SBIR award in the $1.2M to $1.7M range, that is the difference between delivering a capability and delivering paperwork.

Section 2: Pick Your Impact Level

The first decision after award is not what cloud provider to use. It is what Impact Level your application requires. Every other infrastructure decision flows from this one, and getting it wrong in either direction costs you time and money you do not have.

Impact Level (IL) is the Department of Defense's data sensitivity classification for cloud services, defined in the DoD Cloud Computing Security Requirements Guide (CC SRG). It tells you which cloud regions and services are authorized to host your application's data, and which security controls the platform underneath you needs to satisfy. There are six Impact Levels, but for SBIR companies and small defense contractors, only three are practical destinations.

IL2: Publicly releasable information. Your application handles content that could legally be posted on a public website. Examples: marketing analytics, public-facing dashboards, unclassified research summaries, training content. IL2 environments run in commercial cloud regions (AWS GovCloud is not required) and use the FedRAMP Moderate control baseline. Lowest cost, fastest to deploy, but cannot accept Controlled Unclassified Information (CUI).

IL4: Controlled Unclassified Information (CUI). This is the most common requirement for SBIR Phase II and Phase III mission applications. CUI includes a wide range of categories: export-controlled data, sensitive personally identifiable information, certain procurement data, technical data with distribution limitations, and most sensor or telemetry data with operational relevance. IL4 environments require AWS GovCloud (US) or equivalent isolated regions, FedRAMP High control baseline, and US-citizen-only operational personnel. Run rate is two to three times an equivalent IL2 deployment.

IL5: Higher-sensitivity CUI and mission-critical systems. IL5 adds dedicated infrastructure isolation on top of IL4. Required when your data is mission-critical CUI (think targeting data, weapons system telemetry, intelligence community products), when the data classification guide explicitly mandates IL5, or when the contract clause references DFARS 252.239-7010 with IL5 specification. IL5 environments are a strict superset of IL4 and cost meaningfully more to operate.

(IL6 is for classified Secret-level data and runs on dedicated SIPRNet-connected enclaves. If you need IL6, your contracting structure looks very different from typical SBIR work and this guide is not the right starting point.)

The five questions that determine your Impact Level

Before you can shop for infrastructure, you need a defensible answer to these five questions in writing, signed off by your customer or contracting officer.

1. What categories of data will your application process or store? Map every data type to the National Archives CUI Registry (archives.gov/cui). If any category lives in the registry, you are at IL4 minimum. If your data is publicly releasable, you may be at IL2.

2. Has your customer issued a Data Classification Guide? If yes, it tells you exactly what Impact Level applies. If no, your customer's Mission Owner needs to provide one before you scope the environment. Asking for it is not insulting; it is professional.

3. Does your contract reference DFARS 252.239-7010, Cloud Computing Services? If yes, the DFARS clause typically maps to IL4 or IL5 depending on the data. Read the clause carefully and confirm the level with your customer.

4. Will your application connect to other DoD or federal systems? Connections to Mission Owner systems often inherit those systems' classification. If you connect to an IL5 system, your application's environment likely needs to be IL5 even if your own data is technically IL4.

5. Is your application's failure considered mission-critical? Mission criticality is a separate axis from data sensitivity. An IL4 dataset hosted in a system whose unavailability would degrade an operational mission is often elevated to IL5 by the Authorizing Official's discretion.

The two traps we see most often

Over-specifying to IL5 when IL4 is sufficient. Teams hear "defense contract" and assume IL5. The cost difference between IL4 and IL5 over a 24-month Phase II contract can run $300,000 to $500,000 in additional infrastructure run rate. Many SBIR teams over-specify because nobody on the team has read the CC SRG and the customer never volunteered the actual classification. If you cannot point to a Data Classification Guide or a contract clause that mandates IL5, you are probably at IL4.

Under-specifying to IL2 when CUI is in scope. This is the more dangerous mistake. Teams want to move fast, choose IL2 because the environment is cheaper to stand up, and start deploying. Six months in, the customer asks for evidence that CUI is being handled per DFARS, and the team discovers their commercial cloud region is non-compliant. The retrofit involves a full migration to GovCloud, redoing every Identity and Access Management policy, and starting the inheritance and authorization process from zero. Cost: typically $200,000 and three to six months. If there is any chance your data is CUI, scope to IL4.

A one-page decision tree

Print this and bring it to your kickoff meeting.

- Q1. Is your data publicly releasable? YES to Q2; NO to Q3.
- Q2. Does your customer require IL2-authorized infrastructure for an operational reason? YES: IL2. NO: confirm with contracting officer; commercial cloud may be acceptable for non-DoD pilots.
- Q3. Does your data fall into a CUI category in the National Archives CUI Registry? YES: IL4 minimum, continue to Q4. NO: confirm with contracting officer; you may still be at IL4 if connected to DoD systems.
- Q4. Does any of the following apply? Data Classification Guide explicitly mandates IL5; contract references DFARS 252.239-7010 with IL5; application connects to an IL5 Mission Owner system; failure of your application would degrade operational mission. YES to any: IL5. NO to all: IL4.

If you cannot get to a confident answer, escalate to your contracting officer in writing before week two. Working in the wrong Impact Level is the single most expensive infrastructure mistake an SBIR team can make.

Section 3: The Three-Path Infrastructure Decision

Once you know your Impact Level, you face three real options for delivering it. Most teams default to one without realizing the others exist; that default is what creates the 18-month timeline.

Path A: Build your own ATO

You stand up your own cloud environment from scratch (typically AWS GovCloud or Azure Government), implement every NIST 800-53 control yourself, author your own System Security Plan (SSP), negotiate directly with the Authorizing Official, and carry the entire compliance burden as part of your engineering organization.

- Timeline: 12 to 18 months from kickoff to authorization.
- Cost: $400,000 to $500,000 in one-time ATO buildout, plus $15,000 to $40,000 per month in ongoing run rate after authorization.
- Team requirement: At least one full-time security engineer with NIST 800-53 fluency, plus access to a third-party assessor and a body-of-evidence platform.
- When it makes sense: Unusual technical requirements no commercial landing zone supports, or a multi-year program where the long timeline is acceptable. For most SBIR Phase II awards, this path is mathematically incompatible with the contract budget.

Path B: Inherit from a pre-authorized landing zone

You deploy your application into a cloud environment that has already been authorized at your Impact Level. The platform owner has implemented and is continuously monitoring the bulk of NIST 800-53 controls; you inherit those controls via a documented inheritance agreement. You author an SSP that covers only your application-specific controls and references the platform's SSP for the rest.

- Timeline: Two to three weeks to environment provisioning. Eight to twelve weeks to your application's own authorization. Total: roughly three months.
- Cost: No one-time ATO buildout. Monthly run rate that bundles infrastructure, compliance operations, and continuous monitoring. For a typical IL4 Phase II application, $8,000 to $20,000 per month.
- Team requirement: Your engineering team plus a designated compliance liaison (typically part-time).
- When it makes sense: For nearly every SBIR Phase II company, every emerging defense prime under 50 employees, and every team that needs to deliver application capability before the contract ends.

Path C: Hybrid

You inherit most controls from a pre-authorized landing zone but maintain a small set of custom controls for application-specific reasons (typically because of a hardware integration, a non-standard data flow, or a regulatory overlay that the platform does not cover).

- Timeline: Four to six months. Faster than Path A; slower than Path B.
- Cost: Inheritance run rate plus the cost of your custom-control workstream. Often 30 to 50 percent more expensive than pure inheritance.
- When it makes sense: Rare, but real. Edge devices that connect via non-standard protocols, applications spanning IL4/IL5 boundaries, or applications with regulatory overlays outside the standard FedRAMP-DoD

overlay (for example, ITAR data with specific export-control handling).

The three-question scoring rubric

Walk these three questions before you commit to a path.

1. Is delivering application capability inside the contract timeline a hard requirement? If yes, Path A is high-risk.
2. Does your team have a full-time security engineer with NIST 800-53 fluency available for 12+ months? If no, Path A is unrealistic.
3. Does your architecture include hardware, regulatory overlays, or cross-IL boundaries that no commercial landing zone supports? If yes, Path C may be necessary.

If your answers point to Path B and you are choosing Path A by inertia, that is the moment to stop and re-decide.

When not to inherit

Inheritance is the right path for nearly every SBIR mission application, but it is not a universal answer. Inherit only if:

- The platform you are inheriting from has a current, valid Authority to Operate at your Impact Level.
- The platform owner can produce their SSP excerpt and continuous monitoring evidence under non-disclosure agreement (NDA).
- The inheritance boundary is documented in writing before you sign.
- The platform commits to notifying you of any control changes that affect your inheritance.

If a vendor cannot produce these, they are not really offering inheritance; they are selling you marketing. Walk away and find a partner who treats inheritance as an operational practice, not a sales pitch.

Section 4: Your First 90 Days

The decisions in Sections 2 and 3 turn into a week-by-week execution plan. This is the version we use with our own clients. Adapt the deliverables to your specific contract, but keep the cadence; the sequencing is what makes the 90-day timeline work.

Days 1 to 15: scope lock and partner selection

Goal at end of week 2: You know your Impact Level, you have selected a compliant landing zone partner, and you have signed inheritance documentation.

Week 1 deliverables. Impact Level determination signed by your Mission Owner or contracting officer. Application architecture diagram with documented compliance boundary. List of every data category your application will process, mapped to the CUI Registry. Initial connection requirements to other federal or DoD systems.

Week 2 deliverables. Vendor evaluation across at least three compliant landing zone partners. Signed Master Service Agreement (MSA) with selected partner. Inheritance Letter of Attestation from partner referencing their current ATO. Named Authorizing Official (AO) and Mission Owner identified, with introductory meeting scheduled.

Days 16 to 45: environment provisioning and identity baseline

Goal at end of week 6: Your environment is provisioned, your team has access, your identity baseline is locked, and your initial logging is operational.

Weeks 3 to 4 deliverables. Cloud environment provisioned at correct Impact Level. Multi-account structure stood up with separate development, staging, and production boundaries. Identity provider integrated with multi-factor authentication enforced. Just-in-time access policies for privileged operations. Initial network architecture deployed.

Weeks 5 to 6 deliverables. Logging baseline configured (CloudTrail or equivalent, application logging into the centralized log aggregation, retention set to match framework requirements). Initial set of inherited controls validated and documented in your SSP draft. First monthly continuous monitoring report received. Initial POA&M template populated with your application-specific controls.

Days 46 to 75: application deployment and security testing

Goal at end of week 11: Your application is deployed into the authorized environment, your application-specific controls are implemented and tested, and your security assessment package is in draft.

Weeks 7 to 9 deliverables. Application deployed into staging, then production, with deployment automation that captures audit trails. Application-specific access controls implemented. Application logging integrated with platform logging. Vulnerability scanning baseline established. Initial penetration test scoped.

Weeks 10 to 11 deliverables. Penetration test executed and findings remediated or accepted. SSP draft complete (your application-specific controls plus reference to platform SSP). Body of Evidence assembled. POA&M reviewed and prioritized.

Days 76 to 90: authorization package and customer hand-off

Goal at end of week 13: Your application is authorized, your customer is using it, and your continuous monitoring rhythm is operational.

Weeks 12 to 13 deliverables. Authorization package submitted to AO. AO review and questions addressed. Authorization granted (Authority to Operate or interim Authority to Test). Customer demo and hand-off. Continuous monitoring rhythm established (monthly evidence reviews, quarterly POA&M updates, semi-annual control re-validation).

Printable weekly milestone tracker

Print this page and put it on the wall. Every Friday, mark which milestones are complete and which are at risk. The teams who hit 90 days are the ones who notice slip in week 4, not week 11.

- Week 1: IL determination signed.
- Week 2: Partner selected, MSA signed, inheritance letter received.
- Week 3: Environment provisioned.
- Week 4: Multi-account structure live, identity provider integrated.
- Week 5: Just-in-time access enforced, network architecture deployed.
- Week 6: Logging baseline operational.
- Week 7: Application in staging.
- Week 8: Application in production.
- Week 9: Application logging integrated, vulnerability baseline set.
- Week 10: Penetration test scoped and underway.
- Week 11: Pen test findings remediated, SSP draft complete.
- Week 12: Authorization package submitted.
- Week 13: Authorization granted, customer hand-off complete.

If you slip a week, do not catch up by adding people. Catch up by reducing scope of the application's first authorized version. Get authorized on a smaller capability and add to it under continuous monitoring; the AO would much rather see a smaller, well-controlled capability than a larger one that misses the milestone.

Section 5: Ten Pitfalls We See in SBIR Mission App Pursuits

Failure modes drawn from real engagements. None of these are hypothetical. Each one has cost a real team weeks or months. Each is preventable.

1. Application-first sequencing.

What it looks like: Award lands; the engineering team starts building features. Infrastructure is "the next thing on the list." Six months in, infrastructure becomes the critical path.

What it costs: Six to nine months of contract slip; a quarter to a half of contract budget redirected to compliance work that should have been amortized.

How to avoid it: Make the infrastructure decision your first decision, even if the application architecture is not finalized.

2. Choosing a cloud provider before knowing your Impact Level.

What it looks like: "We are an AWS shop, so we will deploy in AWS." Six weeks in, the contract clarifies it requires IL4, and the team is in commercial AWS instead of GovCloud.

What it costs: Full migration to GovCloud, three to six months and $200,000.

How to avoid it: Confirm your Impact Level before selecting a region or partner. The provider name is not the decision; the Impact Level is.

3. SSP as deliverable instead of system of record.

What it looks like: SSP is written for the original assessment, then never updated. Six months later the architecture has evolved and the SSP is fiction.

What it costs: When the AO or assessor compares the SSP to the running environment, they find divergence and flag it. Rework adds two to six weeks per finding.

How to avoid it: Treat the SSP like code: every architecture change goes through SSP review; the SSP is pinned to a versioned location; changes go through pull-request review.

4. Underestimating continuous monitoring overhead.

What it looks like: Team thinks ATO is the milestone. Once authorized, they go back to focusing on the application. Continuous monitoring quietly degrades over six months.

What it costs: When the next continuous monitoring review hits, the AO finds drift, threatens authorization, and the team scrambles for two months to recover.

How to avoid it: Treat continuous monitoring as an operating condition, not a project. Designate one named owner, allocate two to four hours per week, integrate the rhythm into your engineering meetings.

5. Inheritance boundary not negotiated up front.

What it looks like: Team signs with a landing zone partner without a clear inheritance boundary in writing. Six weeks in, the partner says a control the team thought was inherited is actually the customer's responsibility.

What it costs: Surprise control implementation work, often during the authorization package phase when the timeline is most stressed.

How to avoid it: Require the partner to produce a written inheritance matrix that names every control as platform-inherited, customer-owned, or hybrid before signing. Section 6 of this guide is a template.

6. Waiting for the AO to define requirements.

What it looks like: Team treats the AO as a customer who will tell them what to do. Weeks pass without movement because the AO is not driving the process.

What it costs: Calendar slippage that compounds. The AO is reactive by design; if you do not bring an opinion, you wait.

How to avoid it: Bring a draft authorization plan to your first AO meeting. Ask the AO to react to it, not to invent it. The AO's job is to evaluate; yours is to propose.

7. Same identity system across dev and prod.

What it looks like: Single Identity Provider tenant for all environments. Developers have permissions in production "just in case." Service accounts share credentials across environments.

What it costs: Privileged access findings during assessment. Failed least-privilege validation. Six to twelve weeks of identity work to fix.

How to avoid it: Separate identity tenants or, at minimum, separate role assignments for development versus production. No standing access to production. Every privileged action requires just-in-time elevation with audit trail.

8. Application logging incompatible with platform logging.

What it looks like: Application emits logs to its own destination. Platform's logging cannot ingest them. Auditor cannot see the full picture.

What it costs: Logging gap finding. Re-architecture of logging pipelines, two to four weeks.

How to avoid it: Standardize on the platform's logging pipeline before the first line of production code. Confirm application events, security events, and infrastructure events all land in the same searchable, retained log store.

9. POA&M ignored until assessment.

What it looks like: POA&M is opened during the SSP draft, populated with three placeholder items, and never touched again until the assessor asks.

What it costs: Late discovery of unaddressed control gaps. Last-minute remediation that delays the authorization decision.

How to avoid it: Treat the POA&M as a working document, not a deliverable. Review it monthly. Close items quickly. New gaps get added the day they are identified.

10. Architecture drift from the documented boundary.

What it looks like: Application starts inside the documented compliance boundary. Over time, integrations are added and the boundary documentation does not catch up. Six months later, sensitive data is flowing across an undocumented boundary.

What it costs: Worst-case finding category. AOs treat undocumented boundaries as evidence of broader process failure. Recovery takes a full re-assessment, often months.

How to avoid it: Treat every integration change as a boundary review, with the boundary diagram and the SSP updated before the integration ships. No exceptions.

Section 6: The Inheritance Map

The inheritance map is the single most important document in your authorization package. It tells the Authorizing Official, in one page, exactly which controls the platform is responsible for and which controls your application owns. When the boundary is clear and the platform's controls are well-documented, your authorization process becomes dramatically simpler.

This section provides a representative 25-row map across the most common NIST 800-53 Rev 5 control families. The full 200+ row inheritance map ships as a separate downloadable companion artifact, pre-filled with platform responsibilities and blank in the application column for you to complete.

Sample inheritance map (representative, not exhaustive)

Legend: P = platform responsibility (full); A = application responsibility (full); P/A = shared responsibility.

Control	Name	Owner	Notes
AC-2	Account Management	P/A	Platform manages identity provider; application configures application-level roles
AC-3	Access Enforcement	P/A	Platform enforces network and IAM; application enforces business logic access
AC-6	Least Privilege	P/A	Platform sets baseline; application minimizes its own permission set
AC-17	Remote Access	P	VPN, bastion, and remote access flow are platform-owned
AU-2	Audit Events	P/A	Platform captures infrastructure events; application emits events to platform pipeline
AU-3	Content of Audit Records	A	Application is responsible for application-event content
AU-9	Protection of Audit Information	P	Platform secures and retains audit logs
AU-12	Audit Generation	P/A	Platform generates infrastructure logs; application generates application logs
CM-2	Baseline Configuration	P/A	Platform maintains environment baseline; application maintains its own
CM-7	Least Functionality	P/A	Platform enables service surface; application restricts to needed services
CP-9	System Backup	P/A	Platform handles infrastructure backups; application handles data-level backups
IA-2	Identification and Authentication	P/A	Platform provides authentication; application enforces application-level identity
IA-5	Authenticator Management	P	Password, MFA, and credential lifecycle are platform-owned
IR-4	Incident Handling	P/A	Coordinated through platform's CSSP
RA-5	Vulnerability Monitoring	P/A	Platform scans infrastructure; application scans code and dependencies
SA-11	Developer Testing and Evaluation	A	Application owns its own SDLC testing

Control	Name	Owner	Notes
SC-7	Boundary Protection	P	Platform manages all boundary protection
SC-8	Transmission Confidentiality	P/A	Platform enforces TLS for infrastructure; application for app-to-app
SC-13	Cryptographic Protection	P/A	Platform provides FIPS 140-2 modules; application uses them
SC-28	Protection of Information at Rest	P/A	Platform provides encryption at rest; application configures keys
SI-2	Flaw Remediation	P/A	Platform patches infrastructure; application patches code and libraries
SI-4	System Monitoring	P/A	Platform runs continuous monitoring; application emits monitoring data
SI-7	Software Integrity	P/A	Platform validates infrastructure; application validates deployment artifacts
CA-7	Continuous Monitoring	P/A	Platform's program is the spine; application contributes data
PL-2	System Security Plan	P/A	Platform provides SSP excerpt; application authors application-specific SSP

How to use this map

In your kickoff meeting with the platform partner:

1. Walk every control row together. Confirm the platform's responsibility column.
2. For shared rows, agree on the boundary in writing: "Platform configures X; application configures Y."
3. Sign the map as an attachment to your inheritance Letter of Attestation.
4. Reference the map in your SSP wherever you cite an inherited control.
5. Re-validate the map every six months. Platform changes happen; your inheritance assumptions need to stay accurate.

The full XLSX (200+ rows) maps every NIST 800-53 Rev 5 control to a representative compliant landing zone. Use it as your starting point; expect to mark up about 25 to 40 rows where your application's specifics differ from the default.

Section 7: Authorizing Official Conversation Cheat Sheet

The Authorizing Official is the single person whose decision determines whether your application reaches the customer. Most SBIR teams meet their AO once, fumble through the conversation, and then wonder why their authorization timeline is slipping. The teams that move fast walk into AO meetings sounding like operators, not students.

This section is the cheat sheet.

Eight questions to ask the AO before kickoff

1. What is your standard authorization model: full Authority to Operate, Authority to Test, or continuous Authority to Operate?
2. What is your typical timeline from authorization package submission to decision?
3. Do you have a preferred or recommended platform partner for systems of our type?
4. Are there specific control overlays beyond the NIST 800-53 Rev 5 baseline that you require?
5. What is your continuous monitoring expectation post-authorization (cadence, evidence, reporting)?
6. Have you authorized similar systems? If so, what were the most common findings?
7. Do you require a specific Body of Evidence platform, or are we free to choose?
8. What is the preferred channel for ongoing communication: scheduled reviews, email cadence, shared workspace?

The point of these questions is not to extract requirements; it is to signal that you understand the AO's job and are operating in their world.

Five phrases that signal you have your act together

Use these naturally; do not memorize a script. Each one tells the AO that you have done the work.

- "We are inheriting the bulk of our controls from [platform name], and we have the inheritance Letter of Attestation in our package."
- "Our Plan of Action and Milestones is reviewed monthly; here is the current state."
- "Our continuous monitoring evidence flows automatically from the platform; happy to walk through a live dashboard."
- "We have a named compliance owner with allocated time for the program; that role does not change post-authorization."
- "We followed your continuous-ATO model, so the package is structured for ongoing assessment, not a point-in-time approval."

Three things to never say

"We will figure that out post-ATO." This signals that authorization is your milestone, not your operating condition. AOs hear this as a future finding.

"That control is the platform's responsibility, so we did not document it." Inheritance does not exempt you from documenting; you reference the platform's control language in your SSP, not omit it.

"We can move faster if you give us a list of what you need." This signals that you are waiting for the AO to drive. Bring proposals; do not extract requirements.

Sample script: the "what is your security posture" cold question

Most AO conversations include a moment where the AO asks, in some form, "tell me about your security posture." Have a 90-second answer ready. Here is a template:

Security posture script (template)

We are running on a compliant landing zone authorized at [Impact Level], inheriting the platform's NIST 800-53 Rev 5 control implementation. Our application owns [N] application-specific controls, primarily in [areas]. Continuous monitoring is automated through the platform; our team reviews monthly. Our Body of Evidence is in [platform], available for your review at any time. The boundary between platform-inherited and application-owned controls is documented in our inheritance map, attached to the package.

Practice this. The first AO meeting is not a place to think out loud.

Section 8: Vendor Selection Criteria

Not every "compliant" cloud partner is offering the same thing. Some are reselling commercial cloud with a compliance dashboard. Some are operating real authorized landing zones with continuous monitoring. The difference shows up in your authorization timeline.

Twelve questions to ask any cloud partner before signing

1. What is your current Authority to Operate, and at what Impact Level? (Ask for the authorization letter.)
2. When was your last continuous monitoring review, and what did it find?
3. Can you produce your System Security Plan excerpt under NDA?
4. What is your inheritance boundary? (Get this in writing as a control-by-control matrix.)
5. What is your Cybersecurity Service Provider (CSSP) integration?
6. What is your incident response coordination model?
7. What is the change management process for control updates?
8. What is your Plan of Action and Milestones cadence?
9. What is your tenancy isolation model?
10. What logging is provided by default, what retention applies, and where does it live?
11. What is your billing structure? (Bundle vs a la carte vs consumption; multi-year predictability.)
12. Who is your reference customer in our Impact Level and industry?

Red flags

- "We are FedRAMP authorized" with no further detail. Ask which Impact Level and which authorization scope.
- Vendor cannot produce a current SSP excerpt or refuses under NDA.
- Vendor's body of evidence platform is internal-only and not available to customers.
- Vendor's continuous monitoring is described as "we run the standard tools" without naming them.
- Vendor's inheritance boundary is "everything" or "trust us" without a control-by-control matrix.
- Vendor cannot name a customer at your Impact Level for reference.
- Vendor's documentation is older than six months at the time of your evaluation.

Green flags

- Vendor offers an inheritance Letter of Attestation referencing a current ATO, before you ask.
- Vendor's CSSP integration is named and the relationship is established.
- Vendor produces a sample monthly continuous monitoring report under NDA.
- Vendor's named compliance lead can talk fluently about specific NIST 800-53 controls in their environment.
- Vendor offers a two-week proof of concept in a sandboxed environment so you can validate before signing.
- Vendor's reference customer at your Impact Level is willing to take a 30-minute call.

Scoring rubric

Rank each vendor on the twelve questions above. Score 0 (no clear answer) to 3 (strong, documented answer). Total possible: 36 points.

- 30+ points: strong partner; proceed to MSA.

- 24 to 29 points: viable partner; clarify gaps before signing.
- Below 24 points: not a real inheritance partner; keep looking.

The cost of choosing the wrong partner is higher than the cost of any due diligence cycle. The right partner saves you four to six months and several hundred thousand dollars; the wrong one costs you the same in remediation.

Section 9: Worked Example, "Acme Sensor SBIR Phase II"

This example is composite; it is drawn from real engagements, with details adjusted. The team, the contract, and the timeline are representative of teams we work with in our defense and SBIR practice.

The team

Acme Sensor is a 7-engineer Phase II SBIR company with a $1.5M, 24-month contract from a DoD program office. Their application is an edge-sensor data ingestion and analytics platform: sensors deployed in the field stream telemetry to a cloud backend, where the application performs analytics and presents dashboards to the program office. Data is CUI under the Controlled Technical Information (CTI) category. The contract references DFARS 252.239-7010 and specifies IL4.

The wrong-branch plan (months 1 to 4)

Acme's CTO has prior commercial cloud experience and an instinct that says infrastructure is the easy part. The team's initial plan:

- Months 1 to 2: Build the application MVP in commercial AWS.
- Months 3 to 6: Demo to the program office, gather feedback, iterate.
- Months 7 to 12: "Move to GovCloud" and pursue the ATO.
- Months 13 to 18: Authorize and deploy.
- Months 19 to 24: Operations and Phase III preparation.

Acme spent the first four months executing this plan. The MVP came together on schedule. The program office demo went well. Then the program office's contracting officer asked when the system would be available in a CUI-authorized environment for live data, and the team began to learn what GovCloud actually meant.

The pivot at month 4

A consultant Acme brought in for the GovCloud move surfaced the actual cost: $400,000 to $500,000 in ATO buildout, 12 to 18 months for authorization. The contract had 20 months remaining, $1.1M of budget left, and a delivery milestone at month 18 that the team had committed to.

Acme had three options: continue the standalone ATO path (risk: contract slip and budget exhaustion before delivery); pivot to inheriting from a compliant landing zone (risk: rework on the application to fit the new environment); or drop the live-data milestone and deliver only the demo capability (risk: program office relationship damaged; Phase III at risk).

The team chose the pivot. They evaluated three landing zone partners (using the rubric in Section 8), selected one, signed an inheritance MSA in week 17 of the contract, and provisioned the IL4 environment in week 19.

The execution timeline (months 5 to 9)

Month	Acme's focus	Platform partner's focus
5	Vendor evaluation, partner selection, MSA signing	Initial partner conversations, inheritance scope

Month	Acme's focus	Platform partner's focus
6	Environment provisioning, identity baseline, application port to GovCloud	Environment provisioning, inheritance Letter of Attestation
7	Application deployment to staging then production; logging integration	Continuous monitoring baseline, monthly evidence delivery
8	Penetration testing, SSP draft, POA&M population	Pen test coordination, inheritance map review
9	Authorization package submission, AO review and Q&A	Body of Evidence delivery to AO

By the end of month 9 (week 36 of the contract), Acme's application was deployed in an authorized IL4 environment and accepting live CUI data from the program office. From the pivot at month 4 to authorized deployment was approximately five months.

The cost comparison

Item	Standalone ATO	Inheritance
Initial ATO buildout	$450,000	$0
Cloud infrastructure (24 months)	$360,000	(in run rate)
Compliance staff (1 FTE x 18 months)	$225,000	$45,000 (partial)
Third-party assessor	$120,000	$40,000
Body of evidence platform	$48,000	(included)
Inheritance run rate (24 months at $14K/mo)	n/a	$336,000
Total over 24 months	$1,203,000	$421,000

Acme's pivot saved approximately $782,000 over the contract's 24 months. More importantly, it delivered the live-data capability to the program office at month 9 instead of month 18, which became the basis for the Phase III conversation.

Five lessons from this engagement

1. The wrong-branch plan was not a bad plan; it was a familiar plan. The CTO's instincts were calibrated to commercial cloud. They were not wrong; they were not transferable.
2. The pivot was painful but cheap relative to the alternative. Three weeks of partner evaluation and rework saved nine months and $782K.
3. The application port to GovCloud was less work than expected. Most of the application's code was unchanged; the work was in identity, networking, and logging integration.
4. The program office's reaction to the pivot was positive. When the team showed up with a credible inheritance plan and a five-month timeline, the program office trusted the path. AOs respond to credible operators.
5. Continuous monitoring became part of the team's normal operating cadence. Two hours per week, owned by the same engineer who handled deployment automation. Compliance stopped being a project and became an operating condition.

If your team is in month 4 of a similar pursuit and the math is starting to feel like Acme's, the pivot is the right call. The window to make it stays open longer than most teams realize.

Section 10: Resources, References, Next Steps

Authoritative references

- National Institute of Standards and Technology (NIST) 800-53 Rev 5: the control catalog. csrc.nist.gov
- DoD Cloud Computing Security Requirements Guide (CC SRG): the source of truth for Impact Level definitions and DoD cloud requirements. Available through the DoD Cyber Exchange.
- FedRAMP Marketplace: the public list of FedRAMP-authorized cloud services. marketplace.fedramp.gov
- National Archives Controlled Unclassified Information (CUI) Registry: the authoritative list of CUI categories. archives.gov/cui
- DFARS 252.239-7010: Cloud Computing Services contract clause. Read the version current to your contract.

Pandora Cloud Bridge

Bridge is Pandora Cloud's compliant landing zone for SBIR companies, emerging defense primes, and small defense contractors. Authorized at IL2, IL4, and IL5. Built specifically for teams whose mission is the application, not the infrastructure. Inheritance is a documented operational practice, not a marketing pitch. Continuous monitoring is automated and visible to your team in real time. CSSP integration is included by default.

If your team is in the decision window described in this guide, we are happy to walk you through what Bridge would look like for your application before you commit to a partner.

Free 30-minute consultation

No sales pitch; we will look at your contract, your Impact Level question, your timeline, and your current infrastructure plan, and tell you honestly what we would do in your position.

The earlier you make the infrastructure decision, the more of your contract budget stays available for the application itself. That is the entire thesis of this guide and the entire point of the work we do.

Stop trading mission velocity for compliance paperwork.

Schedule a free 30-minute consultation: **pandoracloud.net/#schedule-consultation**

Appendix A: Glossary

ATO (Authority to Operate / Authorization to Operate)
Formal authorization by a federal agency that allows a system to process its data. Granted by an Authorizing Official based on a security assessment.

Authorizing Official (AO)
Federal employee with authority to grant or deny ATO for a system. Typically a senior official in the customer agency.

Body of Evidence (BoE)
The collection of documents, configurations, test results, and monitoring data that demonstrate a system's compliance posture.

cATO (continuous Authority to Operate)
Authorization model in which the system is continuously assessed and authorized through ongoing evidence rather than a periodic re-test.

CC SRG (Cloud Computing Security Requirements Guide)
DoD document defining Impact Levels and cloud-specific security requirements.

CMMC (Cybersecurity Maturity Model Certification)
DoD certification framework for defense contractors handling Federal Contract Information (FCI) and CUI.

CSSP (Cybersecurity Service Provider)
Organization providing continuous cybersecurity services for a DoD system.

CUI (Controlled Unclassified Information)
Unclassified information that requires safeguarding under federal law or policy. Defined in the National Archives CUI Registry.

DFARS (Defense Federal Acquisition Regulation Supplement)
Set of regulations governing DoD contracting. Several DFARS clauses cover cloud, cybersecurity, and CUI handling.

FedRAMP (Federal Risk and Authorization Management Program)
Federal program standardizing security assessment, authorization, and continuous monitoring for cloud services.

IAM (Identity and Access Management)
The system that determines who can access what in a cloud environment. Most-cited finding category in defense ATO assessments.

IL (Impact Level)
DoD's data sensitivity classification for cloud services. IL2, IL4, IL5, and IL6 are the practical levels for most government cloud workloads.

Inheritance
The practice of relying on a platform's authorized controls rather than implementing your own. Documented in an inheritance Letter of Attestation and a control-by-control inheritance map.

Mission Owner

The federal organization or program office that owns the mission the system supports. Often distinct from the AO.

NIST 800-53
The control catalog for federal information systems. Rev 5 is the current version.

NSS (National Security System)
A federal information system that meets specific national security criteria.

POA&M (Plan of Action and Milestones)
Working document tracking known security gaps, planned remediation, and target dates.

SBIR (Small Business Innovation Research)
Federal program funding small business research and development, structured in three phases.

SSP (System Security Plan)
Document describing how a system implements NIST 800-53 controls. Should be a current system of record, not a one-time deliverable.