PANDORA CLOUD
UNPACKING COMPLEXITY

SBIR Compliance Sprint Plan

A 90-day operational plan from SBIR Phase 2 award to authorized federal deployment, written for founders and technical leads, not compliance specialists

A Pandora Cloud Buyer's Resource

May 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 Sprint Plan

Most Small Business Innovation Research (SBIR) Phase 2 teams discover the compliance scope of their contract at month four or month five, when the technology is ready but the customer cannot accept the deployment. The Authorizing Official (AO) will not sign. The program office cannot approve. The team has 18 to 19 months left to rebuild in a compliant environment, complete an Authority to Operate (ATO) authorization, integrate with mission systems, and ship.

This Sprint Plan is the alternative: a 90-day operational sequence that establishes the compliance foundation in the first quarter of the contract, so the remaining 21 months are technical work on a known authorization path. It is written for Principal Investigators, founders, and technical leads, not for federal compliance specialists. Each task is concrete. Each phase ends in a verifiable milestone.

Use the 30-day phase plans to drive your weekly cadence. Use the Impact Level decision framework, the Authorizing Official engagement playbook, and the application-specific control reference to make the higher-stakes decisions early enough that they do not become rework later.

Reading time: 25 minutes to read through. 60 minutes to walk through with the team and assign owners. The sequence in months 2 and 3 rewards a second read with your contracting officer.

Why SBIR Compliance Is a Sequencing Problem

Three structural facts about the SBIR program explain why so many Phase 2 contracts stall in the final third.

1. SBIR funding pays for technical work, not compliance infrastructure. Salaries, prototype costs, customer engagement, and direct technical work all map to the contract budget. The compliant landing zone, the inheritance documentation, the application-specific control implementation, the ongoing continuous monitoring, the Authorizing Official engagement: none of these are natively budgeted. Teams that recognize the gap on day one negotiate it into the budget or build the partnership that bears the cost. Teams that discover it at month five are in a hard conversation with the customer.

2. Authorization is not a paperwork step at the end. With inheritance from a FedRAMP-authorized landing zone (the Day 1 to 30 work in this Sprint Plan), a federal Authority to Operate (ATO) is a 6 to 12 month process that runs in parallel with technical work. Standalone authorizations from cold start typically run 12 to 18 months and are not assumed in this Plan. The architecture decisions made in week one determine which path you are on. Build outside a compliant boundary and the authorization clock cannot start. Build inside one, with a partner that is FedRAMP-authorized at the right Impact Level, and the clock starts on day one.

3. The Authorizing Official is a senior decision maker, not a checklist verifier. The Authorizing Official accepts personal accountability for the risk of operating your system. They are evaluating the system, the threats, and the controls in operational terms. Teams that engage them late produce a polished package and discover the Authorizing Official has questions that take months to answer. Teams that engage them early build the package around the Authorizing Official's actual concerns and clear authorization in a single review cycle.

The Sprint Plan that follows is built around these three facts. Compliance foundation goes first, technology goes second, authorization runs in parallel with both, and the Authorizing Official is a partner from week one.

How to Use This Sprint Plan

The 90 days below are divided into three 30-day phases, each ending in a verifiable milestone. For each task, mark one of:

- Complete: the task is done and you have documentation to show it.
- In progress: the task is started but not finished.
- Not started: the task has not been opened.

Count completions at each phase gate. Use the scoring tiers at the end of this document to determine whether you are on track or need to escalate. This is a working backlog, not a compliance artifact. Re-score weekly during the sprint, then quarterly through the rest of the contract.

The Five SBIR Compliance Pitfalls That Cost Six Months

Before the plan, the antipatterns. These five mistakes show up across SBIR awards in defense, intelligence, and federal civilian agencies. Each one feels like a sensible startup decision; each one extends the delivery date by six months or more. The Sprint Plan that follows is designed to avoid them.

1. Treating the prototype environment as the production path. A team builds in a personal cloud account or a generic startup tier because it is fast and cheap. The work produces a great demo. At month four, the team plans to "just lift and shift" into a compliant environment. The lift-and-shift is a full rebuild: every Identity and Access Management (IAM) role rewritten, every secret rotated, every architectural decision re-examined under the compliance lens. Plan to deliver from a compliant environment from week one.

2. Choosing the Impact Level by reading internet posts. Teams that get this wrong default to Impact Level 2 (IL2) because it is cheaper and faster to stand up, only to discover at month five that the data they handle is Controlled Unclassified Information (CUI), which requires IL4 or higher. The remediation costs three to six months and a substantial budget hit. Confirm the Impact Level in writing with the program office and the data owner before any infrastructure decision.

3. Picking a "FedRAMP-ready" landing zone partner. The marketing language sounds similar to "FedRAMP-authorized" and the difference is significant. FedRAMP-ready means the partner is preparing for authorization but does not yet have an Authorizing Official's signature. Inheriting from a FedRAMP-ready environment is not real inheritance; the controls are not yet validated, the continuous monitoring is not in place, and the Authorizing Official will not accept the inheritance. Confirm the Federal Risk and Authorization Management Program (FedRAMP) authorization status, the Impact Level, and the agency sponsor before signing anything.

4. Underestimating the application-specific control burden. Even with strong inheritance from a compliant

landing zone, the application team owns roughly 50 to 100 application-specific controls under the National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) Revision 5. Identity provisioning, role-based access for application users, application-level logging, change control, customer notification procedures, and incident response specific to your workload. Scope this in week one, not month eight.

5. Treating the Authorizing Official as a paperwork reviewer. The Authorizing Official is a senior federal employee evaluating real risk. Teams that engage them late produce a perfect package and discover the AO has operational questions that take months to answer. Engage the Authorizing Official in days 1 to 30 and build the package around their actual concerns.

Days 1 to 30: Foundation Sprint

This phase is about decisions, not infrastructure. Most of the work happens in conversations with the program office, the partner candidates, and the Authorizing Official. The team that defers these conversations to days 31 to 60 has lost the sprint.

Goal at end of day 30

Impact Level determination signed by the program office. Compliant landing zone partner selected with confirmed FedRAMP authorization at the right level. Master Service Agreement and inheritance Letter of Attestation signed. Authorizing Official identified, with introductory meeting on the calendar.

Week 1: Mission and data scoping

- [ ] Mission Owner identified and primary point of contact established.
- [ ] Contracting Officer identified and contract scope reviewed for compliance flowdown clauses.
- [ ] Data classification request submitted to the program office, with the explicit question: at what Impact Level should this system operate?
- [ ] Data flow diagram drafted, showing what data the system ingests, processes, stores, and shares.
- [ ] Initial threat model drafted, including insider, supply chain, and adversary scenarios appropriate to the mission domain.

Week 2: Authorization path and Authorizing Official

- [ ] Authorization path selected: agency-issued ATO, Joint Authorization Board (JAB) Provisional ATO, or sponsor's pre-existing FedRAMP authorization with inheritance.
- [ ] Authorizing Official identified by name, role, and agency or program office.
- [ ] Introductory meeting requested with the Authorizing Official; agenda focused on system overview, risk posture, and the team's compliance plan.
- [ ] Authorizing Official's preferred evidence formats, communication cadence, and known concerns documented.
- [ ] Authorization timeline target negotiated with the Authorizing Official, with the 90-day foundation as the first commitment.

Week 3: Landing zone partner selection

- [ ] Three landing zone partner candidates evaluated, each with documented FedRAMP authorization status, Impact Levels supported, agency sponsor, and SBIR-specific experience.
- [ ] "FedRAMP-ready" vs "FedRAMP-authorized" status verified for each candidate; the difference is the difference between real inheritance and theoretical inheritance.
- [ ] Reference customers contacted, with explicit questions about Authorizing Official acceptance, evidence package quality, and SBIR delivery timelines.

- [ ] Cost structure negotiated: monthly subscription, inheritance scope, and exit terms documented.
- [ ] Landing zone partner selected with executive sponsor sign-off.

Week 4: Contracts and budget

- [ ] Master Service Agreement (MSA) signed with the landing zone partner.
- [ ] Letter of Attestation (LoA) for inheritance from the landing zone partner reviewed and signed.
- [ ] Compliance budget approved internally and documented in the project plan.
- [ ] Customer contracting officer notified of the compliance approach, with the contract amendment requested if compliance costs require it.
- [ ] 30-day phase gate review with executive sponsor: are decisions locked, or are blockers escalating?

Days 31 to 60: Implementation Sprint

This phase shifts from decisions to infrastructure. The pace accelerates because each week's work depends on the prior week's foundation. Teams that slipped Phase 1 enter Phase 2 with rework debt.

Goal at end of day 60

Environment provisioned in the landing zone partner's compliant cloud. Identity provider integrated. Network architecture documented and reviewed with the Authorizing Official. Application-specific control set scoped and assigned to engineering. Continuous monitoring baseline established with the platform partner.

Week 5: Environment provisioning

- [ ] Compliant cloud environment provisioned in the landing zone partner's tenant at the target Impact Level.
- [ ] Multi-account or multi-subscription structure aligned with the partner's reference architecture (typically separate dev, test, and production at minimum).
- [ ] Initial inheritance baseline confirmed: which platform controls are inherited, which are customer-responsible, which are shared.
- [ ] Cost monitoring established with budget thresholds and alerts.
- [ ] Read-only access for the Authorizing Official and the team's compliance lead documented.

Week 6: Identity and access

- [ ] Identity provider integrated with the landing zone, federated where required with the customer's identity system.
- [ ] Role-based access control (RBAC) roles defined for engineering, compliance, operations, and break-glass scenarios.
- [ ] Multi-factor authentication (MFA) enforced for all privileged and remote access, using a Federal Information Processing Standards (FIPS) 140-validated module.
- [ ] Just-in-time access procedure documented for emergency operations with audit trail.
- [ ] Initial access review conducted; standing access scoped to least privilege.

Week 7: Network and architecture

- [ ] Network architecture documented, including ingress, egress, segmentation, and east-west traffic patterns.
- [ ] Network architecture diagram reviewed with the Authorizing Official; concerns addressed before infrastructure work proceeds.
- [ ] Encryption-in-transit and encryption-at-rest configurations confirmed against the partner's inherited baseline.
- [ ] Boundary protection mechanisms documented; deny-by-default posture verified.
- [ ] Application architecture sketched against the network model; data flow inside the boundary confirmed.

Week 8: Application controls and monitoring

- [ ] Application-specific control set scoped: 50 to 100 NIST 800-53 Rev 5 controls inherited or implemented at the application layer, depending on Impact Level.
- [ ] Each application control assigned to a named owner with implementation status documented.
- [ ] Continuous monitoring baseline established: log streams, configuration scans, vulnerability scans flowing into the partner's monitoring stack.
- [ ] 60-day phase gate review with the Authorizing Official; package readiness for the days 61 to 90 evidence delivery confirmed.

Days 61 to 90: Validation Sprint

This phase shifts from infrastructure to validation. The Authorizing Official is no longer hypothetical; they are reviewing evidence. The application is no longer a prototype; it is moving into the compliant environment.

Goal at end of day 90

Application deployment begins inside the compliant boundary. Application logs flow to the centralized logging stack. First evidence delivery to the Authorizing Official scheduled. Initial authorization package draft circulating. The team can spend the rest of the contract on technical work, knowing the authorization is on a known path.

Week 9: Application deployment begins

- [ ] First application component deployed into the compliant environment, with change-management documentation captured.
- [ ] Application logging verified end-to-end: application emits events, events flow to the centralized log store, events are searchable by the compliance team.
- [ ] Application identity provisioning tested for end users.
- [ ] Backup, restore, and rollback procedures tested with documented results.
- [ ] Smoke test of the deployment process documented; the next deployment will follow the same path.

Week 10: Authorization package drafting

- [ ] System Security Plan (SSP) draft circulating, using the landing zone partner's template where provided.
- [ ] Authorization boundary diagram finalized, showing all components within the boundary and all data flows that cross it.
- [ ] First evidence delivery to the Authorizing Official scheduled; agenda focused on architecture, inherited controls, and application controls.
- [ ] Risk assessment completed and documented; identified risks tracked with mitigations or accepted with rationale.
- [ ] Plan of Action and Milestones (POA&M) opened for any control gaps that will not be closed before kickoff.

Week 11: Evidence delivery and refinement

- [ ] First Authorizing Official evidence delivery completed; questions captured and assigned.
- [ ] Feedback from the Authorizing Official incorporated into the SSP and supporting documentation.
- [ ] Continuous monitoring deliverables exercised: first monthly scan, first POA&M update, first inventory update.
- [ ] Incident response plan walked through with the team; first tabletop scheduled for month 4.
- [ ] Application development resumes at full pace, with compliance integrated into the engineering workflow.

Week 12: 90-day milestone

- [ ] 90-day phase gate review with the executive sponsor and the Authorizing Official.
- [ ] Authorization timeline confirmed: target authorization decision date is set, typically 90 to 120 days from this milestone for clean packages.
- [ ] Documentation locked into the authorization package with version control.
- [ ] Team transitions from sprint mode to sustained delivery mode; weekly compliance check-ins replace daily sprint stand-ups.
- [ ] Compliance posture is real, the package is moving, and the team is back to building technology, not infrastructure.

By the end of 90 days, the SBIR team has shifted the compliance work from an end-of-contract scramble to a parallel workstream that runs alongside technical delivery. The authorization is not finished; it is on a known path with a credible date. The remaining 18 to 21 months of the contract are technical work and incremental compliance, not a forensic compliance project.

Choosing Your Impact Level: IL2, IL4, or IL5 for SBIR

For SBIR Phase 2 teams, the Cloud Computing Security Requirements Guide (CC SRG) Impact Level determines what data the system can handle, which Authorizing Officials can sign, and which compliant landing zone partners are even available. Getting this wrong in week one is the highest-frequency source of three-to-six-month delays we see in SBIR delivery.

Impact Level 2 (IL2): Public information and non-CUI mission information. Applies to systems handling only data cleared for public release. Many SBIR Phase 1 prototypes fit IL2. Phase 2 systems that touch any procurement, personnel, technical, or operational data typically do not.

Impact Level 4 (IL4): Controlled Unclassified Information (CUI). Applies to CUI, including For Official Use Only (FOUO), Privacy Act, and Export Controlled data. Most SBIR Phase 2 systems sit at IL4. The baseline is FedRAMP Moderate plus Department of Defense (DoD)-specific overlays for boundary protection, encryption, and incident reporting.

Impact Level 5 (IL5): CUI with higher sensitivity or mission-critical or NSS data. Applies to mission-critical operational data, certain National Security Systems (NSS) workloads, and CUI with elevated handling requirements. The baseline is FedRAMP High plus DoD overlays.

How to confirm your Impact Level in week one

- Submit a written request to the program office and the data owner: "What Impact Level should this system operate at, given the data we will process?"
- Get the answer in writing, on letterhead or a signed email, with the data sensitivity rationale included.
- If the answer is ambiguous or the program office defers the question, escalate to the Mission Owner. Do not proceed with infrastructure decisions until the IL is locked.
- If the IL changes later, scope creep is the reason. Document the change and request a contract modification immediately; do not absorb the cost silently.

The Authorizing Official Engagement Playbook

The Authorizing Official is the senior federal decision-maker who accepts the risk of operating the system. The teams that move through authorization in a single review cycle treat the Authorizing Official as a partner from day one. The teams that surprise the Authorizing Official with a finished package in month nine spend the next three to six months answering questions.

Six things to ask the Authorizing Official in the first 30 days

1. What systems have you authorized at this Impact Level in the past two years, and what made those packages clean or difficult?

This is the most useful single question. The Authorizing Official will tell you exactly what they look for.

2. What evidence format do you prefer, and what is your communication cadence?

Some Authorizing Officials want live read-only access to the evidence platform; others want monthly PDF packages. The format you build for must match.

3. What known concerns do you have about systems in this mission domain?

Threats specific to the data type, the user population, the operating environment. Build the threat model around the answers.

4. Who else on your team will review the package, and at what gates?

ISSO, Independent Verification and Validation, security control assessor, agency CIO office. Each adds review time; plan accordingly.

5. What is the typical timeline from package submission to authorization decision?

Sets a credible expectation for the contract delivery date.

6. What would cause you to deny or condition the authorization?

The Authorizing Official will name specific risks. Address them in the SSP, not after the submission.

What to bring to the first meeting

- One-page system overview: what the system does, who uses it, what data it handles.
- Data flow diagram (rough draft is fine; refinement is the point of the conversation).
- Compliance plan: landing zone partner, Impact Level, target authorization timeline.
- Calendar availability for monthly check-ins through the 90-day sprint.

Cost Reality for SBIR Compliance Sprint

The compliance budget for the 90-day sprint is concrete, not theoretical. Small Business Innovation Research (SBIR) Phase 2 contracts typically run $750,000 to $2,000,000 across 24 months, depending on agency. The compliance budget is a meaningful fraction of that and should be visible in the project plan from week one. Direct cost categories below assume a fractional Chief Information Security Officer (CISO) at quarter Full-Time Equivalent (FTE) and an optional independent readiness review by a Third-Party Assessment Organization (3PAO) or qualified consultant.

Direct costs over the 90 days

Landing zone partner subscription (3 months)	$20,000 to $50,000
Compliance lead or fractional CISO (25% FTE, 90 days)	$25,000 to $60,000
Authorization package prep (SSP and evidence)	$10,000 to $30,000
Authorizing Official engagement (travel and docs)	$3,000 to $10,000
Independent readiness review by 3PAO (optional)	$8,000 to $20,000

Total 90-day compliance investment: $66,000 to $170,000.

Ongoing costs after the 90-day foundation

- Landing zone partner subscription continues at the same monthly rate through the contract.
- Compliance lead capacity drops to 10 to 20 percent FTE in steady state.
- Continuous monitoring deliverables are bundled into the landing zone subscription on most partner offerings.
- Annual reauthorization cost depends on the authorization type and the Authorizing Official's expectations.

Budget conversations with the contracting officer

The compliance scope is rarely fully budgeted in the original SBIR award. Three approaches to closing the gap:

- Negotiate compliance scope into the Phase 2 contract at award time. The cleanest path; requires raising the question during contract negotiation, before the budget is locked.
- Submit a contract modification request in days 1 to 30. Documents the compliance scope, attaches the budget, and asks for the contract adjustment. Most program offices have a path for this when the scope is justified.
- Absorb the compliance cost from operating capital. Possible for some teams, financially painful for most. Avoid if either of the first two paths is open.

What Application-Specific Controls Look Like

Inheriting from a FedRAMP-authorized landing zone does not eliminate the team's compliance work. The application layer still owns 50 to 100 NIST 800-53 Rev 5 controls, depending on Impact Level and architecture. Knowing which controls are yours in week one prevents the month-eight surprise.

Common application-layer control families

- Identity provisioning and lifecycle. Application users are not the same as cloud users; the application owns its own identity model.
- Application-level access control. Role-based access for application functions, with audit trails.
- Application logging. Events that the application emits beyond infrastructure logs, with retention matched to the authorization commitment.
- Customer notification procedures. When and how the application notifies users of system events, incidents, or required actions.
- Application change management. Pull request reviews, deployment approvals, and configuration change records specific to the application.
- Application-specific incident response. Incident scenarios that involve application logic, customer data, or business processes.
- Application supply chain. Software dependency tracking, software bill of materials, dependency scanning.

The landing zone partner provides the platform controls. The team provides everything that sits above them.

Scoring

Total possible: 12 weekly milestones across the 90-day sprint.

10 to 12 milestones	On track. The authorization is on a known path; the team is positioned to deliver technical work as the primary workstream.
7 to 9 milestones	Recoverable. Identify the slipped milestones, escalate to the executive sponsor, and rebalance the next 30 days.
Below 7 milestones	Significant slip. Escalate to the Mission Owner and the customer contracting officer. Continuing on the current path adds three to six months to the delivery date.

A team scoring 10 or higher at the day 90 milestone will deliver on time barring external events. A team scoring below 7 is fighting a compliance battle that consumes the rest of the contract.

A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business (WOSB) and an Amazon Web Services (AWS) Advanced Tier Partner with a Defense Counterintelligence and Security Agency (DCSA) Secret-level Facility Clearance and Cybersecurity Maturity Model Certification (CMMC) Level 2 self-assessment status. Our founding team holds active Secret and higher clearances. We build and operate compliant cloud landing zones at Impact Level 2, Impact Level 4, and Impact Level 5 for SBIR teams and small defense contractors.

Our Bridge platform delivers Authority to Operate inheritance at IL2, IL4, and IL5, FedRAMP-aligned continuous monitoring, and Cybersecurity Service Provider (CSSP) integration on a subscription model. For SBIR teams executing this Sprint Plan, Bridge is one path through the days 1 to 30 partner selection decision; we are happy to walk through whether it fits your contract.

If you are inside an active SBIR Phase 2 and want a second set of eyes on your 90-day plan, or if you are evaluating compliance scope as part of a Phase 2 proposal, we are happy to help.

For SBIR teams whose Phase 2 contract requires AWS GovCloud or DoD Impact Level work, the Cloud Landing Zones Guide is our 28-page tactical playbook for compliance-first multi-account architecture. This Sprint Plan presumes a landing zone exists; the Guide is the prerequisite document if you do not yet have one. Free at pandoracloud.net/cloud-landing-zones-guide.

Run your own SBIR Phase 2 or Phase 3 math at Impact Level 2, 4, and 5: pandoracloud.net/cost-calculator/. The Cost Calculator includes a Defense scenario built specifically for SBIR teams.

Need a partner for the 90-day sprint?

Schedule a free 30-minute consultation. We will walk through your contract scope and what the Sprint Plan would look like for your specific Impact Level.

pandoracloud.net/#schedule-consultation

Glossary

For readers new to SBIR compliance vocabulary, this glossary names the most common terms referenced in this Sprint Plan.

ATO (Authority to Operate)
The senior federal official's formal acceptance of the risk of operating a system. Required before a federal customer will run the application in production.

Authorizing Official (AO)
The senior federal official with authority to issue an Authority to Operate. Engaged from days 1 to 30 of this Sprint Plan.

CC SRG (Cloud Computing Security Requirements Guide)
The Department of Defense (DoD) guidance that defines Impact Levels for cloud services handling DoD data.

CMMC (Cybersecurity Maturity Model Certification)
The DoD framework for protecting Controlled Unclassified Information in non-federal systems. Increasingly required of defense subcontractors and SBIR awardees.

CUI (Controlled Unclassified Information)
Federal information that requires safeguarding but is not classified. Includes For Official Use Only (FOUO), Privacy Act, and Export Controlled data.

FedRAMP (Federal Risk and Authorization Management Program)
The federal program that standardizes security assessment, authorization, and continuous monitoring for cloud services. Landing zone partners must be FedRAMP-authorized at the right Impact Level for inheritance to work.

FedRAMP-authorized vs FedRAMP-ready
Authorized means an Authorizing Official has signed; the controls are validated and continuous monitoring is in place. Ready means the partner is preparing for authorization but does not yet have the signature. Only authorized partners support real inheritance.

Impact Level (IL)
The DoD CC SRG categorization of data sensitivity. IL2 covers public and non-CUI; IL4 covers CUI; IL5 covers CUI with higher sensitivity or NSS data.

Inheritance
The transfer of compliance posture from a FedRAMP-authorized platform to a customer deploying on it. The customer owns application-layer controls; the platform owns infrastructure-layer controls.

ISSO (Information System Security Officer)
The vendor-side compliance role that owns the day-to-day operation of the security program for the system.

JAB (Joint Authorization Board)
The board of Chief Information Officers from DoD, the Department of Homeland Security, and the General Services Administration that issues Provisional ATOs (P-ATOs) for cloud services with broad federal applicability.

NIST 800-53 Rev 5
The current revision of the NIST control catalog underlying FedRAMP and DoD authorizations. Published

September 2020.

POA&M (Plan of Action and Milestones)
Structured tracking of open compliance findings with owners and target close dates.

SBIR (Small Business Innovation Research)
The federal program that funds small business research and development with potential for commercialization. Phase 1 funds feasibility; Phase 2 funds development; Phase 3 funds commercialization.

SSP (System Security Plan)
The vendor-authored description of how the system operates, how each control is implemented, and how the operational posture maintains the controls over time. The largest single artifact in an authorization package.

Sprint Plan
The 90-day operational sequence in this document, designed to establish the compliance foundation in the first quarter of a contract so the remaining work proceeds on a known path.