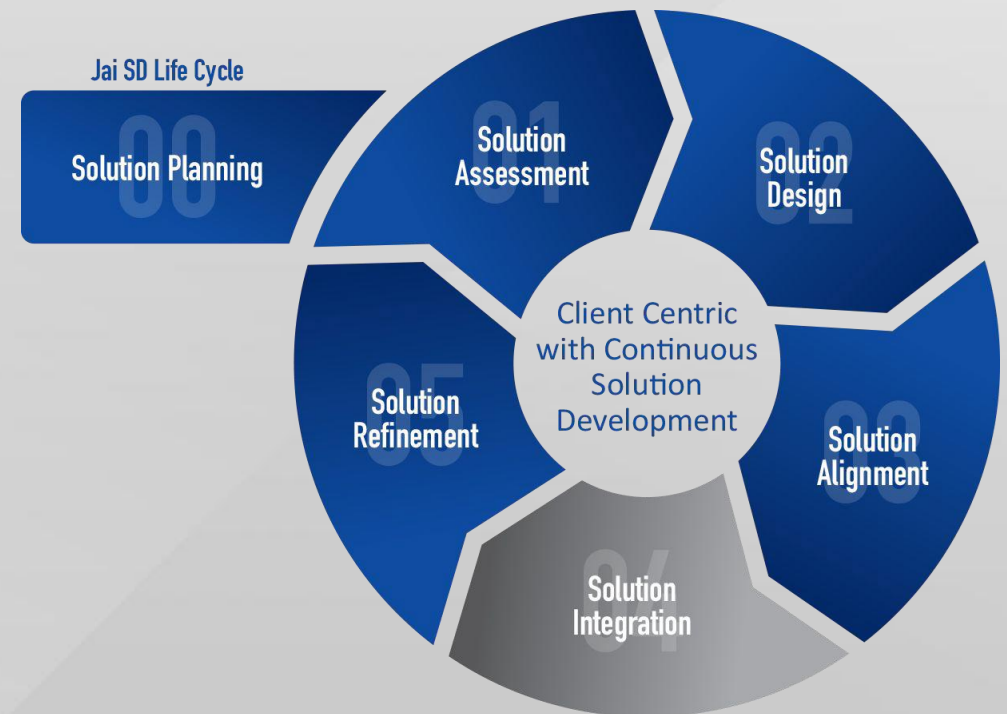




# THE JAI WORKBOOKS: OPERATIONALIZING THE JAI MODEL

**Dr. James L. Matney**

President & CTO  
Jai Solutions, LLC





# CHALLENGES THE JAI WORKBOOKS ADDRESS

## WIN STRATEGY BREAKS DOWN IN EXECUTION

BD and capture insights, client feedback, and win themes are not consistently translated into solution artifacts or proposal content

## ARTIFACTS ARE CREATED IN SILOS

BD, capture, solution, and proposal teams develop disconnected outputs, creating rework and misalignment

## SPEED PRESSURES EXPOSE PROCESS GAPS

Compressed timelines with releases of solicitation documents (e.g., Draft PWS, Draft RFP, Final RFP) demand faster artifact development without sacrificing rigor or compliance

## AI IS UNDERUTILIZED OR APPLIED INCONSISTENTLY

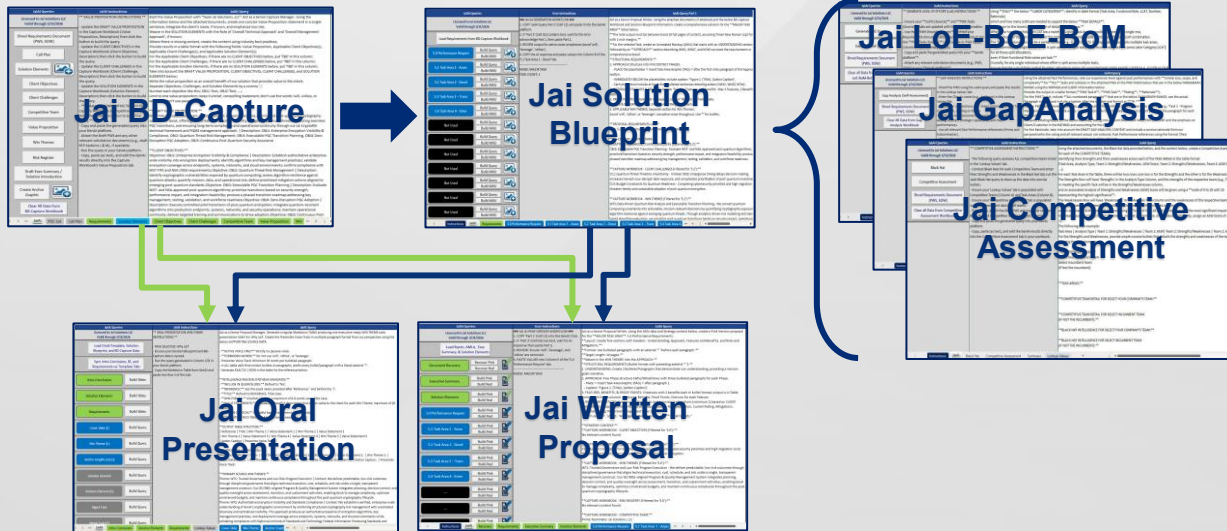
Teams lack structured, responsible ways to apply GenAI across BD, capture, solution, and proposal development



The Jai Workbooks operationalize the Jai Model—providing structured, AI-enabled tools that consistently transform strategy into compliant, proposal-ready execution.



# JAI WORKBOOKS WITH JaiAI (GenAI-ENABLED)



JaiAI-powered Jai Workbooks transform BD and Capture artifacts into fast, consistent, and winning proposal and oral deliverables.

## INTEGRATED BD-TO-PROPOSAL FLOW

Connects BD-Capture and Solution Blueprint workbooks to auto-create requirements-driven AMUs and proposal-ready content

## MODEL-DRIVEN GENAI AUTOMATION

JaiAI generates GenAI queries from Jai Model concepts, refining draft inputs into compliant Pink and Red versions with rapid recovery

## ACCELERATED, WINNING OUTPUTS

Delivers consistent, copy-paste-ready written and oral artifacts that improve speed, quality, and competitive differentiation



# JAI WORKBOOKS TRANSFORM ARTIFACTS TO WINNING PROPOSALS

**BD-CAPTURE ARTIFACTS**

- POC List
- Call Plan
- Solution Elements
- Client Objectives
- Client Challenges
- Competitive Team
- Value Proposition
- Win Themes
- Risk Register



**SOLUTION ARTIFACTS**

- Solution Strategy Poster
- Solution Blueprints
- Anchor Graphic
- Graphics ( Task, Solution, & Process )
- Bottom-Up LoE-BoM
- Competitive Assessment



**PRE-PROPOSAL ARTIFACTS**

- Solution Introduction / Executive Summary
- Annotated Mockup (AMU)
  - o Approach (with graphics)
  - o Strengths (Features, Benefits, & Proof Points)
  - o Risks & Mitigations
  - o Win Themes

WRITTEN PROPOSAL



ORALS PRESENTATION




Jai BD-Capture Workbook  
 Jai Competitive Assessment Workbook

Jai Solution Blueprint Workbook  
 Jai Gap Analysis Workbook  
 Jai Bottom-Up LoE-BoM Workbook

Jai BD-Capture Workbook  
 Jai Solution Blueprint Workbook

Jai Written Proposal Workbook  
 Jai Oral Presentation Workbook

- AMUs form the foundation of all color version drafts: written or oral presentations
- The BD, Capture, and Solution artifacts build upon each other to produce the AMU content, which is structured into **five key proposal elements**



BD-Capture and Solution arti-facts converge through Jai Workbooks, where GenAI streamlines and refines content into efficient, cohesive, and winning proposals.



# JAI BD-CAPTURE WORKBOOK

## STRUCTURED BD AND CAPTURE SPRINTS:

Drives disciplined BD/Capture sprints that define client objectives, challenges, value proposition, win themes, and solution elements

## REQUIREMENTS AND COMPETITIVE INTELLIGENCE ALIGNMENT:

Shreds the PWS while analyzing competitive teams and risks to shape winning positioning

## PROPOSAL-READY STRATEGIC OUTPUTS:

Produces solution artifacts, call plans, and a draft Executive Summary / Solution Introduction ready for downstream proposal development



Solution Element (SE: Text)	Description	Key Phases/Component/Steps	Features and Client Benefit(s) [Feature: Benefit]	Graphic Placeholder
SE1: Jai CryptoRM	Enterprise cryptography risk management framework delivering authoritative encryption visibility, quantum risk analysis, executable mitigation planning, SOC integration, and continuous improvement to protect GovA from emerging quantum threats.	1. Identify Encryption Landscape: We automate discovery across endpoints, systems, networks, and cloud; we map encryption usage to mission services and data flows to expose where cryptography protects (or fails to protect) critical data. 2. Analyze Encryption Security Posture: We assess algorithm strength and crypto hygiene against quantum and classical threats; we evaluate key management and "right-layer" encryption placement to identify systemic weaknesses. 3. Plan and Implement Mitigations: We prioritize transitions by risk, feasibility, and operational constraints; we execute phased mitigations with defined rollback and validation criteria to reduce disruption. 4. Integrate with Security Operations: We integrate crypto posture telemetry into SOC tools; we operationalize playbooks (alert → triage → contain → remediate) tied to encryption failures and misconfigurations. 5. Continuous	* Enterprise-wide encryption discovery: Full visibility across GovA's IT enterprise, * Quantum-risk prioritization: Focuses budget/time on highest exposure, * SOC-integrated workflow: Faster detection/response with fewer handoffs, * Executable mitigation roadmap: Reduces uncertainty and accelerates modernization, * Continuous improvement loop: Sustains compliance and reduces regression risk	
SE2: Teammate-1 CryptoQScan	Automated discovery and analysis capability that rapidly identifies encryption implementations, algorithms, certificates, and key management practices across on-premises and cloud environments.	1. Automated Discovery: We deploy non-intrusive, agentless collection and configuration queries; we correlate results across five regions to produce a unified crypto inventory. 2. Algorithm & Key Analysis: We evaluate algorithms, key lengths, cert chains, and protocol versions; we flag deprecated crypto, weak keys, and improper key storage/distribution. 3. Compliance Mapping: We map findings to NIST FIPS and NSA CNSA controls; we produce gap lists with implementable remediation actions and owners. 4. Risk Scoring: We score assets by exposure, data sensitivity, and mission criticality; we publish ranked remediation backlogs to drive action. 5. Continuous Refresh: We rescan on a schedule and after changes; we keep posture current and	* Agentless scanning: Minimizes operational impact and deployment friction, * Automated standards mapping: Speeds identification of compliance gaps, * Risk scoring model: Enables prioritization by mission impact, * Five-region correlation: Reduces blind spots across enterprise boundaries, * Regression detection: Prevents crypto drift after fixes	Process graphic: "CryptoQScan Pipeline" showing Inputs (CMB, network scans, cloud APIs, cert stores) → Normalize/Correlate → Analyze (algorithms/keys/protocols) → Map to FIPS/CNSA → Output (Inventory + Findings + Risk Score) feeding Dashboard + Remediation Backlog.
SE3: Integrated CryptoPosture Dashboard	Centralized, role-based dashboard providing near real-time visibility into encryption posture, quantum risk, compliance status, and POC transition progress for executives, engineers, and operators.	1. Data Aggregation: We ingest data from CryptoRM, CryptoQScan, and SOC platforms; we normalize metrics into consistent measures (coverage, strength, compliance, risk). 2. Risk Visualization: We present posture by region/system/mission service; we highlight trends, hotspots, and drift against target states. 3. Decision Support: We deliver role-based views (Exec, Security, Network, App teams); we provide "next-best-action" recommendations and prioritized backlogs. 4. SOC Integration: We align alerts and posture thresholds with SOC workflows; we connect findings to tickets/playbooks for closure tracking. 5. Continuous	* Unified visibility: Single source of truth across five regions, * Role-based views: Faster decision cycles for each stakeholder group, * Outcome KPIs: Proves progress toward compliance and PQ readiness, * Ticket/playbook linkage: Accelerates remediation closure, * Trend analytics: Predicts regression and workload before it becomes risk	Dashboard concept: A three-tier view: Top = Executive scorecards (coverage %, CNSA/FIPS compliance %, top 10 risks), Middle = heatmaps by region/system, Bottom = action queues (tickets, playbooks, roadmap milestones). Arrows from CryptoQScan/QRIE/SOC into the dashboard; feedback arrow from tickets back into posture metrics.



BD-Capture Workbook converts insight, intelligence, and strategy into proposal-ready direction that shapes winning solutions.



# JAI SOLUTION BLUEPRINT WORKBOOK



Task Area / Subtasks	Staffing (R, SCATs, Skill Levels)	Processes (Who/What/How)	Technologies (Technology Name/ Tool)	Solution Features & Benefits (Feature/ Client Benefits)	Solution Risks & Mitigations (Risk Title/ Mitigation Actions)
5.1.2 Assess Quantum Computing Risk	1. Solution Architect (Senior), Cryptography (Mid), Security Engineer (Senior), Data Analyst (Mid), Technical Writer (Mid)	1. Who: Solution Architect defines decision objectives, assessment scope, and stakeholder alignment. Cryptography (CA) defines quantum susceptibility criteria and crypt break-impact assumptions. Cybersecurity Engineer validates exposure paths and mission dependencies. Data Analyst builds risk models and prioritization logic. Technical Writer produces decision-ready outputs for stakeholders and executives.	Quantum Risk Intelligence Engine (QRIE). Analytics engine that evaluates cryptographic exposure against projected quantum threat to inform PQC transition planning. CryptSAR: Enterprise-scale cryptographic risk management framework for execution.	Quantum risk-driven prioritization. Cost-effective focus on highest-risk system/forward-looking analysis. Reduced uncertainty in quantum threat/enterprise data-driven prioritization. Smaller investment decisions.	Inconsistent crypto standards. Integration across teams. Publish quantum risk criteria and decision rules. Conduct testing scenarios, document exceptions with compensating controls/remediation backlog review. Strategic. Enterprise-to-operations review.
<b>Annotated Mockup (AMU)</b>					
<p><b>5.0 Performance Requirements UNDERSTANDING</b></p> <p>GovA requires a disciplined, fully integrated Program Management Office (PMO) to oversee contract execution, including staffing, scheduling, cost control, and performance measurement. This PMO must provide transparent, low-risk governance to support quantum-readiness initiatives under constrained budgets and compelling cybersecurity priorities (CC3). The Program Management Plan (PMP) functions as the authoritative execution guide, translating contractual requirements into actionable governance structures, technical approaches, management controls, and decision-making authorities. Without a centralized PMO and a rigorously maintained PMP, programs face fragmented oversight, delayed issue identification, and increased risk of cost and schedule overruns, jeopardizing mission objectives and PQC adoption timelines.</p> <p>The PMO establishes a mature, ISO 9001-aligned management environment through the Program &amp; Quality Management System (SE7 PQMS), integrating technical execution, organizational resources, quality assurance, and performance measurement under a single governance framework. By embedding disciplined controls and a structured five-phase lifecycle from program initiation, GovA gains predictive oversight, audit-ready documentation, and the ability to make informed, timely decisions across cost, schedule, and performance dimensions.</p> <p><b>APPROACH</b></p> <p>The PMO executes Task 5.0 through a five-phase lifecycle anchored in SE7 PQMS, providing disciplined governance, adaptive management controls, and continuous program performance measurement. Each phase integrates staff responsibilities, technical processes, and operational workflows to deliver predictable, low-risk outcomes.</p> <p>&lt; Insert Task Area Graphic (TAG) &gt;</p> <p>Figure 1. Integrated Program Management Lifecycle. Predictable, low-risk execution through structured governance, continuous performance measurement, and quality oversight.</p>					



## FOCUSED SOLUTION SPRINTS:

Orchestrates structured solution sprints to define people, processes, technologies, solution features and benefits, proof points, and risk mitigations aligned to task areas and evaluation factors

## INTEGRATED SOLUTION ARTIFACT DEVELOPMENT:

Develops comprehensive solution artifacts and weaves outputs from the BD-Capture Workbook into annotated mockups (AMUs) with embedded, proposal-ready content

## AI-ENABLED SOLUTION REFINEMENT:

Leverages the JaiAI-enabled workbook to shape and refine solution elements across task areas, while generating tailored GenAI queries that accelerate the creation of high-quality AMUs



The Jai Solution Blueprint Workbook transforms BD-Capture insight into AI-accelerated, proposal-ready solution artifacts, producing the AMU as the authoritative source document that anchors all written and oral proposal presentations.



# JAI GAP ANALYSIS WORKBOOK



Jai Solutions, LLC		Single Economic Entity		Small Business	
Experience Level: Evaluate the level of expertise in each Task Area based on the following: 4 - Substantial Expertise with Client (Multiple past performance examples within 3 years) 3 - Substantial Expertise (Multiple past performance examples within 3 years) 2 - Intermediate Expertise (At least one past performance example within 3 years) 1 - Limited Expertise (No past performance records available for this task area) 0 - No Expertise		Choose the Task Areas you are open to providing support: Yes - Ready to support and contribute to solution No - Unable to support Task Area		Strategic Capabilities and Past Performance: Furnish details about your capabilities and instances from the past three years that demonstrate your relevant experience in this Task Area	
PWS Requirement	Experience Level (0, 1, 2, 3, 4)	Support (Y/N)	Relevant Past Performance		
5.0. Performance Requirements	4	Yes	Demonstrated substantial expertise with GovA through multiple recent engagements establishing PMOs and delivering Program Management Plans. References: CryptoRM, Organization X		
5.1 Task Area 1 - Assess Encryption Security Posture	2	Yes	Extensive experience assessing enterprise encryption posture for GovA, including vulnerability analysis, compliance reviews, and quantum risk evaluations. References: CryptoRM, Organization X		
Jai Gap Analysis Summary			Jai Solutions, LLC	Teammate-1	
5.0. Performance Requirements			Small Business	Large Business	
5.1.1 Conduct Encryption Audit			4	3	
5.1.2 Assess Quantum Computing Risk			4	4	
5.1.3 Review Compliance with NIST and NSA Standards			2	4	
5.2 Task Area 2 - Develop Post-Quantum Encryption Algorithms			2	4	
5.2.1 Review Post-Quantum Encryption Algorithms			2	4	
5.2.2 Prioritize Post-Quantum Encryption Algorithms			3	4	
5.2.3 Create Transition Roadmap			3	3	
5.3 Task Area 3 - Transition to Post-Quantum Encryption with No Impact to Operations			3	3	
5.3.1 Pilot Transition of Post-Quantum Encryption Algorithms			4	3	
5.3.2 Integrate with Existing End Points, Systems, Networks, and Security Operations			4	3	
5.3.3 Provide User Training and Communication			4	3	
5.4 Task Area 4 - Enterprise Analysis Assessment			2	2	
5.4.1 Establish Monitoring Protocols			2	2	
5.4.2 Plan for Incident Response			2	3	
5.4.3 Continually Assess Encryption Security Posture			2	2	



The Jai Gap Analysis Workbook delivers a clear, evidence-based view of experience coverage and teammate strength across all task areas.

## STRUCTURED EXPERIENCE SELF-ASSESSMENT

Drives a disciplined self-assessment across all task areas to evaluate experience depth and maturity using documented past performance and Lead SA input

## TEAMMATE CAPABILITY INTEGRATION

Aggregates and normalizes teammate self-assessments to identify complementary expertise, coverage strengths, and areas where partners fill critical gaps

## GAP IDENTIFICATION AND READINESS SUMMARY

Synthesizes company and teammate results into a comprehensive, task-area-level summary that highlights expertise gaps, risk areas, and overall execution readiness



# JAI COMPETITIVE ASSESSMENT WORKBOOK



Requirement	Analysis Type	Jai Solutions LLC, Teammate-1	GDDT, Empower.AI	Leidos, TekSynap
		<b>Analysis of Strengths and Weaknesses (10 - Highest Significance)</b>		
5.1.3	Strengths	7.06 7	63.53	49.41
5.1.3	Weaknesses			
5.2	Strengths			
5.2	Weaknesses			

## STRUCTURED COMPETITIVE SELF-ASSESSMENT

Conducts disciplined self-assessments and Black Hat sessions against the top 3–5 competitive teams to evaluate relative strengths and vulnerabilities across all task areas

## ACTIONABLE COMPETITIVE INTELLIGENCE SYNTHESIS

Transforms raw Black Hat inputs into clear, meaningful competitive assessment bullets that highlight differentiators, risks, and exploitation opportunities

## QUANTIFIED STRENGTHS & WEAKNESSES ANALYSIS

Produces a comprehensive Competitive Assessment with an Analysis of Strengths and Weaknesses (ASW) score, enabling side-by-side comparison of our team versus competitors



The Jai Competitive Assessment Workbook turns Black Hat insight into a quantified, task-area-level comparison that clearly positions our team against the competition.



# JAI LOE-BOE-BOM WORKBOOK

## EARLY BOTTOM-UP COST DEVELOPMENT

Solution sprints aligned to the Solution Blueprint establishes an early, bottom-up Level of Effort (LoE) and Bill of Materials (BoM) by task area

## TASK-AREA LOE AND STAFFING ALIGNMENT

Generates detailed LoE estimates based on solution-driven staffing assumptions, supporting accurate resource allocation and apportionment across teammates

## PRICE-TO-WIN INFORMED BASIS OF ESTIMATE

Produces an AI-enabled Basis of Estimate (BoE) that supports early price validation against Price to Win, enabling timely solution and staffing adjustments to hit target pricing



PWS Task Area	Functional Role	Labor Category	LOE	Base	OY1	OY2	Teammate	Location	Clearance	Relevant Notes
5.1. Task Area 1 – Assess Encryption Security Posture	Cybersecurity Analyst	Endpoint Security Engineer (Senior)	0.00	\$9.00	0.00	0.00	Jai Solutions-LLC	Colorado		Matches task requirements; full FTEs for posture assessment
5.1. Task Area 1 – Assess Encryption Security Posture	Cryptographer	Systems Security Engineer (SME)		1.00			Teammate-1	Colorado		Lead for encryption assessment; full FTE
5.1. Task Area 1 – Assess Encryption Security Posture	Security Engineer	Systems Security Engineer (Journeyman)		2.00			Teammate-1	Colorado		Support audit and assessment; full FTEs
5.1. Task Area 1 – Assess Encryption Security Posture	Compliance Analyst	Security Compliance Specialist (Senior)		1.00			Teammate-1	Colorado		Lead compliance review; full FTE
5.1.1. Conduct Encryption Audit	Cybersecurity Analyst	Endpoint Security Engineer (Senior)		0.50			Teammate-1	Colorado		Shared FTE with 5.1.3; provides audit support
5.1.1. Conduct Encryption Audit										Shared FTE with 5.1.2; supports audit
5.1.1. Conduct Encryption Audit										Dedicated FTE for audit compliance
5.1.2. Assess Quantum Comput Risk										Shared FTE with 5.1.1; quantum risk analysis
5.1.2. Assess Quantum Comput Risk										SME support for risk assessment
5.1.3. Review Compliance with NIST and NSA Standards										Lead for compliance review
5.1.3. Review Compliance with NIST and NSA Standards										Shared FTE with 5.1.1; assists in compliance evaluation
5.2. Task Area 2 – Develop Post-Quantum Encryption Transition Plan										Lead cryptography analysis and QR algorithm planning
5.2. Task Area 2 – Develop Post-Quantum Encryption Transition Plan										Supports plan creation and integration strategy

PWS Task Area	Material/Resource Description	Quantity/# of Licenses	Vendor/Supplier	Base	OY1	OY2	Total	Relevant Notes
5.1.1 Conduct Encryption Audit	Network Auditing Tool	15	Vendor-2	\$ 100	\$ 100	\$ 100	\$ 300	Acquire licenses annually, with the understanding that assistance from Teammate-2 will not be required in the third year.
5.1.1 Conduct Encryption Audit	System Auditing Tool	15	Vendor-2	\$ 100	\$ 100	\$ 100	\$ 300	Acquire licenses annually, with the understanding that assistance from Teammate-2 will not be required in the third year.
5.1.1 Conduct Encryption Audit	Database Auditing Tool	15	Vendor-1	\$ 75	\$ 75	\$ 75	\$ 225	
5.1.1 Conduct Encryption Audit	Application Auditing Tool	15	Vendor-1	\$ 50	\$ 50	\$ 50	\$ 150	



The Jai LoE-BoE-BoM Workbook delivers early, solution-driven cost insight that aligns staffing, teammates, and pricing to Price to Win.



Task Area / Subtasks	Graphic Placeholder	Annotated Mockup (AMU)	Pink Version	Red Version
5.1 Task Area 1 - Assess Encryption Security Posture		<p>5.1 Task Area 1 – Assess Encryption Security Posture (Annotated Mockup) UNDERSTANDING</p> <p>GovA faces a rapidly evolving cryptographic risk environment driven by expanding hybrid infrastructure, distributed mission services, and accelerating post-quantum computing (PQC) timelines. Task Area 5.1 requires an enterprise-scale assessment of encryption security posture across GovA's IT enterprise, including data centers and cloud infrastructures spanning five regions. The assessment must evaluate</p>	<p>## **MAJOR TASK AREA 5.1 – Assess Encryption Security Posture**</p> <p>### **UNDERSTANDING**</p> <p>* GovA operates in a cryptographic risk environment shaped by hybrid infrastructure sprawl, geographically distributed mission services, and accelerating post-quantum computing pressures. Encryption protections span endpoints, enterprise systems, network fabrics, and cloud services across five regions, yet</p>	<p>## **TASK ID: 5.1 Task Area 1 – Assess Encryption Security Posture**</p> <p>---</p> <p>### **UNDERSTANDING**</p> <p>GovA operates within a cryptographic risk environment shaped by hybrid infrastructure sprawl, geographically distributed mission services, and accelerating post-quantum computing pressures.</p>
5.1.1 Conduct Encryption Audit		<p>Task Areas</p> <p><b>5.1 TASK AREA 1 – ASSESS ENCRYPTION SECURITY POSTURE</b></p> <p>UNDERSTANDING</p> <p>GovA operates within a cryptographic risk environment shaped by hybrid infrastructure sprawl, geographically distributed mission services, and accelerating post-quantum computing pressures. Encryption protections extend across endpoints, enterprise systems, network fabrics, and cloud services operating in five regions. However, visibility into cryptographic algorithms, key management practices, protocol dependencies, and certificate lifecycles remains fragmented across organizational and technical boundaries. Task Area 5.1 requires an enterprise-scale assessment that establishes authoritative encryption visibility, validates alignment with NIST FIPS and NSA CNSA guidance, and exposes cryptographic weaknesses that create mission degradation risk, data compromise exposure, and hardware-decryptable vulnerability. Success depends on correlating cryptography to mission services, data sensitivity, and operational impact so leadership receives a defensible, actionable risk posture rather than isolated technical findings.</p> <p>Mission goals for Task Area 5.1 focus on two inseparable outcomes: authoritative enterprise encryption visibility and actionable quantum risk management. Leadership requires a verified baseline that confirms where encryption exists, how it functions, and whether it satisfies federal standards. Engineers and operators require prioritized remediation direction grounded in mission relevance, feasibility, and budget realities. Occasional non-routine cryptographic relevant quantum computing timelines heighten these needs, rendering ad hoc assessments insufficient. Task Area 5.1 therefore establishes the foundation for informed compliance decisions, risk-based post-quantum transition planning, and sustained cryptographic governance across GovA's evolving enterprise.</p> <p>APPROACH</p> <p>We execute Task Area 5.1 through a disciplined five-phase approach that transforms fragmented cryptographic data into authoritative visibility, defensible risk scoring, and executable mitigation planning. Each phase converts technical findings into mission-relevant insight, ensuring GovA gains lasting operational value rather than a one-time assessment artifact.</p> <p>Phase 1 – Identify Encryption Landscape</p> <p>We establish authoritative enterprise-wide visibility into encryption deployments across endpoints, systems, networks, and cloud environments spanning five regions. Automated and structured discovery identifies cryptographic toolchains, algorithms, protocols, certificates, and key management practices, producing a validated baseline that eliminates blind spots and supports downstream risk analysis and compliance validation.</p>	<p>Task Areas</p> <p><b>5.1 TASK AREA 1 – ASSESS ENCRYPTION SECURITY POSTURE</b></p> <p>UNDERSTANDING</p> <p>GovA operates within a cryptographic risk environment shaped by hybrid infrastructure sprawl, geographically distributed mission services, and accelerating post-quantum computing pressures. Encryption protections span endpoints, enterprise systems, network fabrics, and cloud services across five regions, yet</p>	<p>ASK ID: 5.1.1 Conduct Encryption Audit**</p> <p>Task 5.1.1 – Conduct Encryption Audit**</p> <p>requires authoritative, enterprise-wide visibility into encryption deployments across endpoints, systems, networks, and environments spanning five regions to close long-standing gaps and achieve enterprise encryption compliance. Fragmented awareness of cryptographic algorithms, certificates, and dependencies obscures where encryption</p>
5.1.2 Assess Quantum Computing Risk		<p>Phase 2 – Analyze Encryption Security Posture</p> <p>We evaluate encryption protocols, algorithms, and key management practices against NIST FIPS and NSA CNSA guidance to identify weaknesses, deprecated configurations, and non-compliant implementations. Structured assessment criteria ensure consistent evaluation across all five</p>	<p>Our Senior Solution Architect leads kickoff working sessions with GovA stakeholders to confirm assessment scope, regional boundaries, system ownership, mission service priorities, and data sensitivity drivers. This alignment ensures discovery activities reflect operational reality and focus on events most critical to mission success. Senior Cryptographic SMEs and Senior Cybersecurity Engineers inventory encryption implementations across enterprise layers and map cryptographic dependencies to mission services and data flows, connecting raw discovery results into mission-relevant visibility that supports enterprise governance and compliance validation.</p> <ul style="list-style-type: none"> <li>Proven Application of Our Approach</li> </ul> <p>Jai CryptoM Deployment: Identified encryption supporting 12 enterprise IT services across endpoints, servers, data centers, and network infrastructures, eliminating undocumented cryptographic dependencies and establishing a validated enterprise baseline.</p>	<p>ASK ID: 5.1.2 Assess Quantum Computing Risk**</p> <p>Task 5.1.2 – Assess Quantum Computing Risk**</p> <p>faces persistent uncertainty regarding quantum threats, a condition that delays action and increases exposure to vest-now-decrypt-later attacks against long-lived sensitive data. This uncertainty creates risk not because quantum</p>

# JAI WRITTEN PROPOSAL WORKBOOK



The Jai Written Proposal Workbook transforms AMUs and capture strategy into review-ready proposals that evolve efficiently through Color Team feedback.

## AMU-DRIVEN PROPOSAL DEVELOPMENT

Leverages Annotated Mockups (AMUs), detailed solution elements, and the BD-Capture Executive Summary to generate compliant, proposal-ready Pink and Red Team drafts.

## INTEGRATED COLOR TEAM ITERATION

Incorporates Pink and Red Team review feedback to refine content, strengthen win themes, and improve clarity and evaluator alignment.

## VERSION CONTROL AND DRAFT RECOVERY

Maintains structured draft versions and enables rapid recovery and refinement of proposal content across Color Team cycles.



# JAI ORAL PRESENTATION WORKBOOK

## AMU-DRIVEN ORAL CONTENT DEVELOPMENT

Uses Annotated Mockups (AMUs) and the Solution Introduction / Executive Summary to generate oral presentation content aligned to approved solution messaging

## TEMPLATE-BASED SLIDE AUTOMATION

Leverages a Master Oral Presentation Template deck, allowing users to select task-specific slide templates that automatically populate with solution content

## CONSISTENT, EVALUATOR-FOCUSED STORYTELLING

Ensures slides are compliant, visually consistent, and tightly aligned to task areas, evaluation factors, and win themes



**Confident Post-Quantum Mission Security**

**Trusted Governance, Low-Risk Execution**  
Disciplined governance aligns cost, schedule, risk, and quality, keeping post-quantum modernization predictable and controlled across complex enterprise environments.

**Authoritative Encryption Visibility, Compliance**  
Enterprise-wide cryptographic insight creates a defensible NIST and NSA-aligned baseline while exposing true operational and mission risk concentrations.

**Data-Driven Quantum Risk Decisions**  
Quantified analysis converts quantum uncertainty into prioritized, mission-relevant actions and phased transition sequencing leaders can execute confidently.

**Zero-Disruption Post-Quantum Adoption**  
Dependency-aware deployments preserve availability, interoperability, and user productivity during cryptographic modernization across production systems.

Deliver disciplined governance, authoritative visibility, and data-driven execution that secures GovX missions throughout the post-quantum transition.

**SE1: Jai CryptoRM**

Introduction | Factor 1: Technical | Factor 2: Management | Conclusion | L-2.2, M-3.7

**Problem Statement**

- Quantum threat brings uncertainty because prioritization and knowledge exposure to harness low-decryptable data across long lead times.
- Fragmented encryption visibility across endpoints, networks, and cloud services undermines accurate risk assessment and transition planning.
- Budget pressure and competing cybersecurity demands complicate sequencing and justification of post-quantum investments.
- Deep cryptographic dependencies elevate operational risk during transition, increasing outage and interoperability concerns.
- Evolving standards and asymmetric compliance challenge sustained compliance, monitoring, and incident response effectiveness.

**Solution**

Challenges:
 

- Quantum Threat
- Fragmented Encryption Visibility
- Complex Dependencies
- Resource Constraints
- Existing Solutions

Solutions:
 

- Jai CryptoRM: Authoritative Encryption Visibility
- Task 1.2 Performance Requirements: Defensible Quantum Risk
- Task 1.3: Controlled POC Adoption
- Task 1.4: Continuous Security Assurance
- Task 1.5: Program & Quality
- Task 1.6: Incident Response

**Features/Benefits**

- Enterprise-wide discovery: Establishes authoritative encryption visibility across GovX systems and services.
- Quantum-risk prioritization: Directs resources toward highest mission and data exposure first.
- SOC-integrated workflow: Improves detection, triage, and remediation speed.
- Verifiable mitigation roadmap: Converts analysis into phased, dependency-aware transition actions.
- Continuous improvement loop: Sustains compliance and reduces regression as environments evolve.

**Proof Points**

- Jai CryptoRM implementation for Organization X identified encryption supporting twelve IT services and delivered a quantified quantum mitigation plan enabling informed POC budgeting decisions.

**Establish Authoritative Encryption Visibility And Govern A Low-Risk, Mission-Aligned Transition To Sustained Post-Quantum Cryptographic Resilience**

Jai Solutions, LLC Proprietary and Confidential | January 23, 2026 | 1

This slide anchors our entire technical approach. Jai CryptoRM provides the enterprise framework that transforms scattered cryptographic data into authoritative insight leaders trust. We expose where encryption actually protects GovX's mission data, where gaps exist, and which assets uncertainty with defensible prioritization and disciplined governance is action. We translate encryption posture and quantum exposure into executable endency-aware sequencing, defined validation criteria, and rollback planning reduce into confidence that security improvement aligns with mission realities rather than as improvement. Integrated SOC workflows, recurring posture assessments, and standards and threats evolve. GovX gains a managed, measurable, and enduring posture preserving operational continuity.

Task	Problem Statement	Key Phases/Components/Steps	Features/Benefits	Proof Points	Action Caption	Presenter Value Track
SE1: Jai CryptoRM	Quantum threat brings uncertainty because prioritization and knowledge exposure to harness low-decryptable data across long lead times. Fragmented encryption visibility across endpoints, networks, and cloud services undermines accurate risk assessment and transition planning.	Identify Encryption Landscape* Analyze Encryption Security Posture* Plan And Implement Mitigation* Integrate With Security Operations* Continuous Improvement	Enterprise-wide discovery Establishes authoritative encryption visibility across GovX systems and services* Quantum-risk prioritization Directs resources toward highest mission and data exposure first* SOC-integrated workflow: Improves detection, triage, and remediation speed.	Jai CryptoRM implementation for Organization X identified encryption supporting twelve IT services and delivered a quantified quantum mitigation plan enabling informed POC budgeting decisions	Establish Authoritative Encryption Visibility And Govern A Low-Risk, Mission-Aligned Transition To Sustained Post-Quantum Cryptographic Resilience	This slide anchors our entire technical approach. Jai CryptoRM provides the enterprise framework that transforms scattered cryptographic data into authoritative insight leaders trust. We expose where encryption actually protects GovX's mission data, where gaps exist, and which assets uncertainty with defensible prioritization and disciplined governance is action. We translate encryption posture and quantum exposure into executable endency-aware sequencing, defined validation criteria, and rollback planning reduce into confidence that security improvement aligns with mission realities rather than as improvement. Integrated SOC workflows, recurring posture assessments, and standards and threats evolve. GovX gains a managed, measurable, and enduring posture preserving operational continuity.



The Jai Oral Presentation Workbook converts AMUs and capture strategy into consistent, evaluator-focused oral presentations—automatically and at scale.

# QUESTIONS?



[James.Matney@jai-us.com](mailto:James.Matney@jai-us.com)

[Jessica.Matney@jai-us.com](mailto:Jessica.Matney@jai-us.com)

[info@jai-us.com](mailto:info@jai-us.com)

[www.jai-us.com](http://www.jai-us.com)



**INNOVATE. DISRUPT. WIN!**