**Response to Request for Quote**

Rapid Technology Services (RTS) – Volume I

**Solicitation #:** 15JPSS25O00000041

**Solicitation Due Date:** 04/04/2025 12:00 PM EDT

# Prepared by Offeror:

**Primary Vendor:** Canopy One Solutions Inc – SBA 8(a) Certified Small Business
**Subcontractor:** Stealth Solutions Inc – SBA 8(a) Certified Small Business
4229 Lafayette Ctr Dr Ste 1625, Chantilly, VA 20151
**CAGE:** 73W91 | **DUNS#:** 065545545 | **UEI:** KVMCAAMAAAH7
**EIN/TIN#:** 27-1556206 **GSA MAS Contract#** 47QTCA22D009E
**URL:** http://www.canopyone.com
**Point of Contact:** Gopal Bethi
**E:** gopal@canopyone.com | **O:** 703-867-7172

# Prepared For:
U.S. Department of Justice
**RFP Point of Contact:**
DeChanta S. Vaughan
**Email**: DeChanta.S.Vaughan@usdoj.gov

## TABLE OF CONTENTS

1. **EXECUTIVE SUMMARY**

**Team Canopy (Prime: Canopy One Solutions Inc, Sub: Stealth Solutions Inc)**, led by Canopy One Solutions Inc., is proud to present a highly qualified and mission-aligned partnership with Stealth Solutions Inc., an SBA-certified 8(a) small business and a recognized provider of innovative technology and management services. Together, we bring a complementary blend of expertise in cloud technologies, low-code/no-code platforms, AI/ML, and digital modernization. This strategic partnership enhances our ability to rapidly respond to DOJ's mission needs with agility, technical depth, and small business engagement. As an integrated team, Team Canopy is fully committed to delivering scalable, secure, and forward-looking solutions that enable DOJ's components to achieve their modernization objectives under the Rapid Technology Services (RTS) BPA. Furthermore, we acknowledge that we have reviewed all the RFP documents, amendments, and the Q&A released by the agency.

**Our Understanding of the RFP**

Canopy One understands that the U.S. Department of Justice (DOJ) seeks to establish a Rapid Technology Services (RTS) Blanket Purchase Agreement (BPA) to provide agile, flexible, and secure IT services supporting the full Systems Development Life Cycle (SDLC). The RTS BPA is designed to enable DOJ components to modernize legacy systems, adopt emerging technologies, leverage cloud-native solutions, and implement low-code/no-code platforms — all while ensuring robust cybersecurity and compliance with federal mandates.

The BPA encompasses a wide range of services, including solution design and architecture, system engineering and development, operations and maintenance (O&M), cybersecurity, cloud services, program and risk management, records and document management, and end-user support and training. These services will be delivered with strict adherence to applicable federal security, privacy, and accessibility standards, including FedRAMP, FISMA, NIST RMF, and Section 508. Canopy One brings proven experience and expertise across a broad spectrum of technologies, platforms, and mission-critical domains. We are well-equipped to effectively support DOJ's objectives under this BPA by delivering innovative, scalable, and cost-effective solutions tailored to the Department's diverse and evolving mission needs

We recognize that each BPA Call will require a responsive and flexible approach, with the ability to quickly assemble specialized teams capable of delivering high-quality results that align with DOJ's operational priorities and evolving technology landscape.

**Challenges**

Canopy One recognizes the scale and complexity of the RTS BPA, and the unique challenges associated with meeting DOJ's mission-critical objectives. Key challenges include:

- **Balancing Rapid Delivery with Complex Compliance Requirements**
  - Delivering technology solutions using Agile, DevSecOps, and rapid application development approaches while ensuring compliance with stringent federal mandates — including FedRAMP, FISMA, NIST RMF, and Section 508 accessibility — requires mature governance, continuous monitoring, and highly skilled resources.
- **Diverse Technology Landscape and Legacy Modernization**

  - o DOJ's existing IT landscape spans modern cloud-native applications and legacy systems. Successfully integrating new technologies while maintaining interoperability, performance, and security across this spectrum presents significant complexity.
- **Operationalizing Emerging Technologies**
  - o Effectively adopting and operationalizing AI/ML, big data analytics, low-code/no-code platforms, and cloud-native architectures requires balancing innovation with risk management, ethical AI principles, and robust data governance.
- **Scalability Across DOJ's diverse Mission Footprint**
  - o Supporting DOJ's wide-ranging mission areas demands a flexible, scalable staffing and management approach capable of responding to multiple simultaneous BPA Calls without compromising quality.

## Key Success Factors

Team Canopy identifies the following as essential for successful execution:

- **Process Delivery and Certified Delivery Excellence:** CMMI Level 3 (Development and Services), ISO 27000, 20000, and 9001 certified—ensuring disciplined quality, security, and IT service management across projects.
- **Comprehensive Technical Coverage**
  - o Deep expertise across a wide range of technologies, platforms, and domains enabling us to tailor solutions to DOJ's needs — from cloud services, DevSecOps, and AI/ML to data analytics, low-code/no-code platforms, and cybersecurity.
- **Domain Knowledge**
  - o Past performance in systems supporting case management, litigation, financial management, infrastructure, and identity management.
- **Agile, Scalable, and Proactive Program Management**
  - o Certified PMP/Agile managers ensuring risk mitigation, stakeholder communication, and quality-driven delivery.
- **Strong Focus on Security and Accessibility**
  - o Embedded security practices, 508 remediation, and continuous improvement frameworks aligned with DOJ policies.

## Value Proposition

Team Canopy offers DOJ a proven, reliable partner positioned to deliver the RTS objectives with the following value:

- **Mission-Aligned Innovation:** Deep understanding of DOJ's operational needs, offering scalable, forward-looking solutions that incorporate AI, Cloud, Big Data, and Low-Code/No-Code platforms for faster mission outcomes.
- **End-to-End Service Delivery:** Comprehensive support across application development, operations & maintenance, cloud migration, cybersecurity, and data transformation, ensuring minimal disruption and maximum mission impact.
- **Certified Quality and Security:** Industry-recognized certifications guaranteeing risk-aware, compliant, and high-quality execution throughout the project lifecycle.
- **Rapid Response and Adaptability:** Agile resource mobilization to meet BPA Call demands quickly, supported by a deep bench of skilled professionals ready to serve DOJ's evolving needs.
- **Proven Federal Performance:** Demonstrated success delivering complex IT services to federal agencies, reducing costs, improving performance, and ensuring compliance.

## 2. TECHNICAL APPROACH

Team Canopy is committed to delivering scalable, secure, and future-ready IT architecture that aligns with the Department of Justice's (DOJ) enterprise objectives and mission-critical needs. Our approach is designed to modernize DOJ's IT infrastructure, optimize business processes, and ensure compliance with federal security and regulatory standards.
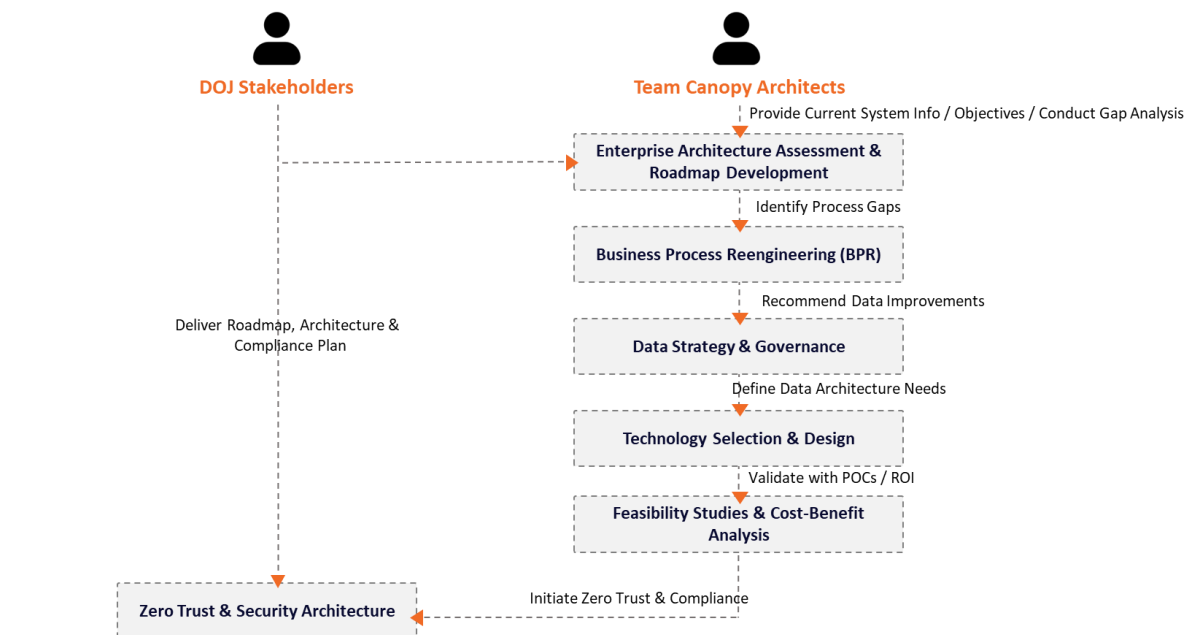
By leveraging the Federal Enterprise Architecture Framework (FEAF) as the foundation, Canopy One will implement a structured and standardized enterprise IT environment that enhances operational efficiency, data-driven decision-making, and system agility. Our cloud-first, AI-driven, and automation-enabled strategy will help DOJ streamline IT investments, reduce costs, and improve service delivery across its various components.

With a strong foundation in federal IT modernization, digital transformation, and emerging technologies, Canopy One will drive DOJ's transition toward a highly efficient, automated, and resilient IT ecosystem that can adapt to evolving technology landscapes and mission requirements. The following sections outline Team Canopy's technical approach to Planning & Solution Architecture, ensuring a seamless transformation that meets DOJ's current and future needs.

### 2.1 Planning & Solution Architecture

Effective planning and solution architecture form the foundation of any successful IT modernization initiative. For the DOJ's Rapid Technology Services (RTS) BPA, Canopy One recognizes that planning is not just about technology alignment but about ensuring that every IT investment is strategic, scalable, secure, and mission aligned.

Our approach focuses on delivering flexible, future-ready architectures that allow DOJ to rapidly adapt to changing mission needs, integrate emerging technologies such as AI/ML and cloud, and maintain compliance with federal security and regulatory standards. Leveraging our extensive federal experience, Canopy One will ensure that DOJ's IT ecosystem is agile, interoperable, and optimized for performance and cost efficiency.



**DOJ Stakeholders** — **Team Canopy Architects**

Provide Current System Info / Objectives / Conduct Gap Analysis

Enterprise Architecture Assessment & Roadmap Development

Identify Process Gaps

Business Process Reengineering (BPR)

Recommend Data Improvements

Data Strategy & Governance

Define Data Architecture Needs

Technology Selection & Design

Validate with POCs / ROI

Feasibility Studies & Cost-Benefit Analysis

Deliver Roadmap, Architecture & Compliance Plan

Initiate Zero Trust & Compliance

Zero Trust & Security Architecture

## Our Approach

- **Enterprise Architecture Assessment & Roadmap Development**
  - Conduct a comprehensive gap analysis of DOJ's current IT assets guided by the Federal Enterprise Architecture Framework (FEAF), including Performance (PRM), Business (BRM), Applications (ARM), Infrastructure (IRM), and Security (SRM) domains.
  - Aligning IT systems and capabilities with DOJ's strategic mission priorities, ensuring interoperability, eliminating redundancy, and supporting cross-component collaboration.
  - Develop a phased modernization roadmap addressing system enhancements, integration strategies, and legacy system decommissioning, ensuring alignment with DOJ's operational timelines and change management processes.
- **Business Process Reengineering (BPR)**
  - Analyze DOJ's business workflows, identifying inefficiencies, bottlenecks, and automation opportunities using **Lean Six Sigma methodologies**.
  - Propose and design process improvements, leveraging low-code/no-code platforms (as appropriate) to streamline workflows, reduce manual intervention, and enhance agility.
  - Explore intelligent automation opportunities, such as AI-enabled document processing, case triage, and predictive task routing to enhance mission delivery efficiency.
- **Data Strategy and Governance**
  - Design a robust **Data Reference Model (DRM)** to enable data sharing, standardization, and analytics readiness across DOJ.
  - Recommend scalable **data lake/data warehouse architectures** to support both structured and unstructured data, enabling real-time insights and advanced analytics.
  - Establish DOJ-wide **data governance policies** covering data quality, security, privacy, access controls, and lifecycle management, aligned with federal guidelines.
- **Technology Selection and Design**
  - Assess and recommend technology solutions based on DOJ's mission needs and evolving technology landscape, covering AI/ML, IoT, data platforms, cloud, and enterprise systems.
  - Ensure architectural designs enable seamless integration between modern platforms and legacy systems while embedding DevSecOps practices for secure development and operations.
  - Emphasize open APIs, microservices architecture, and containerized design patterns for scalability, agility, and interoperability—enabling DOJ to adapt quickly to new mission requirements or technology shifts.
- **Feasibility Studies & Cost-Benefit Analysis**
  - Perform Total Cost of Ownership (TCO) and Return on Investment (ROI) analysis for cloud migrations, AI/ML adoption, and emerging technologies using industry-standard models and decision matrices.
  - Validate technology decisions through rapid Proof of Concepts (PoCs), sandbox environments, and pilot programs to test integrations, performance benchmarks, and user adoption prior to full-scale implementation.
  - Develop investment optimization strategies to prioritize high-value initiatives that align with DOJ's strategic goals, minimize operational disruption, and reduce long-term technical debt.
- **Zero Trust and Security Architecture Integration**

- Integrate Zero Trust security principles from the initial planning stages, embedding identity verification, least privilege access, and micro-segmentation across all architectural layers.
- Ensure all solutions comply with FedRAMP, NIST, FISMA, and Section 508 standards by embedding automated compliance checks into CI/CD pipelines and applying security-as-code principles to infrastructure and application layers.
- Align planning with DOJ's cybersecurity roadmap to support continuous monitoring, security incident response readiness, and auditability across all deployed solutions.

**Key Success Factors:**
- **Alignment with DOJ Mission Objectives:** Every architectural plan is designed to align with DOJ's diverse operational objectives and mission needs, supporting critical systems and programs across its components
- **Agile and Scalable Planning:** Our iterative and agile architectural planning enables DOJ to accommodate rapid changes in priorities or technologies.
- **Cross-Domain Expertise:** Canopy One's experience across AI/ML, Big Data, IoT, Cloud, and DevSecOps ensures DOJ's architecture is future-proof and capable of integrating emerging technologies.

**Value Proposition:**
- **Mission-Driven Architectural Framework:** Canopy One delivers architecture that supports DOJ's entire digital ecosystem, breaking down silos between components.
- **Cost Optimization:** Our structured approach to TCO/ROI ensures maximum value from each IT investment.
- **Risk Mitigation:** Early embedding of security, compliance, and feasibility analysis reduces future rework and mitigates risks.

### 2.2 Program Management Office (PMO) Support

Effective program management is essential to the successful execution of the DOJ's Rapid Technology Services (RTS) BPA. Canopy One understands that overseeing concurrent and diverse task orders within this BPA requires disciplined governance, real-time monitoring, risk management, and consistent stakeholder engagement. Our Program Management Office (PMO) is designed to function as the centralized control hub, ensuring the delivery of services aligns with DOJ's objectives, performance expectations, and compliance requirements.

Our approach emphasizes adaptability and scalability, enabling the PMO to tailor support based on the complexity and size of each BPA Call while maintaining oversight across technical execution, resource alignment, risk management, and reporting.

**Approach:**
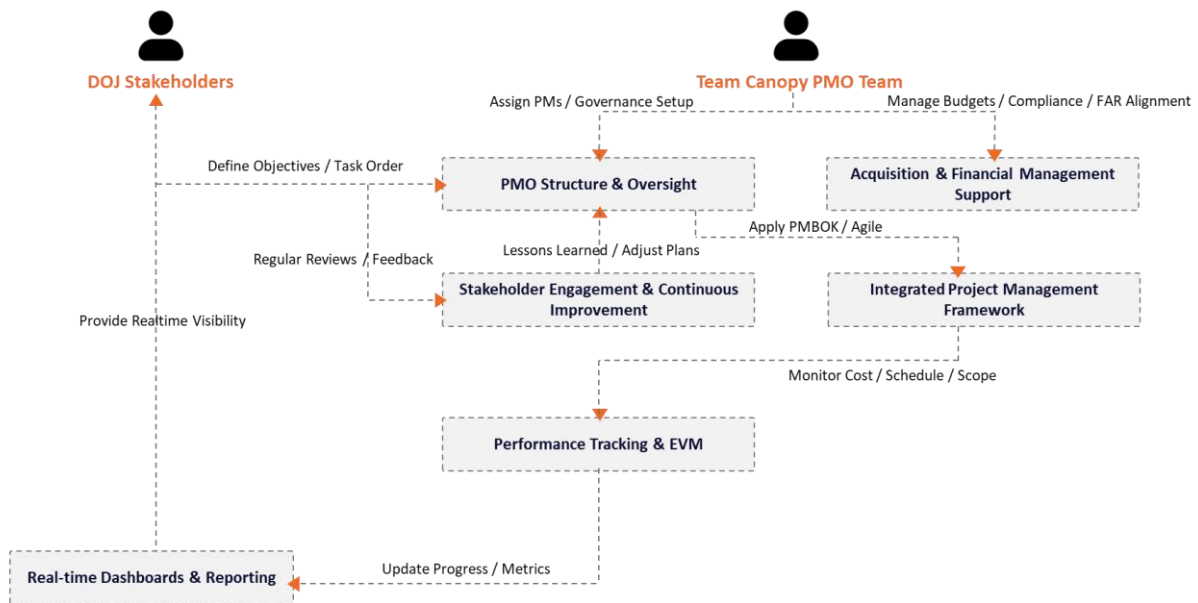
- **PMO Structure and Oversight**
  - Establish a dedicated PMO team with experienced, certified Program and Project Managers responsible for overall program governance, task order tracking, and communication with DOJ stakeholders.
  - Tailor PMO support based on the size, scope, and complexity of each BPA Call to ensure agile resource allocation and responsive oversight throughout the task order lifecycle.
- **Integrated Project Management Framework**
  - Apply a hybrid management methodology that combines PMBOK best practices for structured project controls with Agile delivery principles to support iterative, flexible execution where appropriate.
  - Utilize the PMBOK's standard phases—Initiation, Planning, Execution, Monitoring & Controlling, and Closure—to maintain control over cost, schedule, and deliverables.
- **Performance Tracking and Earned Value Management (EVM)**
  - Implement Earned Value Management (EVM) to monitor project performance against planned cost, schedule, and scope baselines.
  - Track key EVM metrics such as Planned Value (PV), Earned Value (EV), and Actual Cost (AC) to quickly detect variances and apply corrective measures.
  - Integrate performance metrics into dashboards for visibility and transparency.
- **Reporting, Dashboards, and Communication**
  - Provide real-time dashboards and reporting tools to keep DOJ informed of program and task order status, resource utilization, and potential risks.
  - Dashboards may include earned value charts, milestone tracking, and key performance indicators, using tools like Microsoft Project, JIRA, or equivalent systems as examples.
  - Maintain risk registers, issue logs, and change management records, enabling early detection of risks or deviations from scope and timely mitigation actions.
- **Stakeholder Engagement and Continuous Improvement**
  - Facilitate regular status reviews and program briefings to maintain alignment with DOJ expectations and provide progress updates.

- Conduct after-action reviews and continuous improvement workshops to capture lessons learned and enhance future performance across task orders.
- **Acquisition and Financial Management Support**
  - Align program management activities with Federal Acquisition Lifecycle Framework (FALF) principles and ensure compliance with federal acquisition regulations and DOJ policies, where applicable.
  - Provide support in monitoring task order budgets, resource utilization, and financial performance, applying techniques such as activity-based costing (ABC) models where appropriate for transparency.

**Key Success Factors:**
- Deployment of experienced Program Managers and Agile practitioners with a strong background in federal program oversight.
- Use of real-time metrics and dashboards to enable data-driven decision-making and performance monitoring.
- Scalable PMO structure allowing efficient resource allocation and rapid adjustment to evolving BPA Call demands.

**Value Proposition:**
- Disciplined oversight and governance minimize rework, delivery delays, and cost overruns.
- Improved visibility and accountability across all BPA Calls through structured reporting and risk tracking.
- Alignment with federal acquisition best practices, enabling transparency, auditability, and effective program execution.

## 2.3 System Engineering & Development

System Engineering and Development under RTS BPA demand an approach that delivers rapid, secure, scalable, and adaptable solutions while accommodating DOJ's evolving mission requirements. Canopy One recognizes the importance of balancing Agile delivery, system interoperability, security, and integration with legacy environments.

Our approach is rooted in modern software engineering, with strong governance, iterative development cycles, and a focus on building modular, reusable, and scalable systems. We emphasize architectures that are cloud-ready, security-compliant, and flexible enough to support future needs such as AI, big data analytics, and IoT integration—all while maintaining operational continuity.
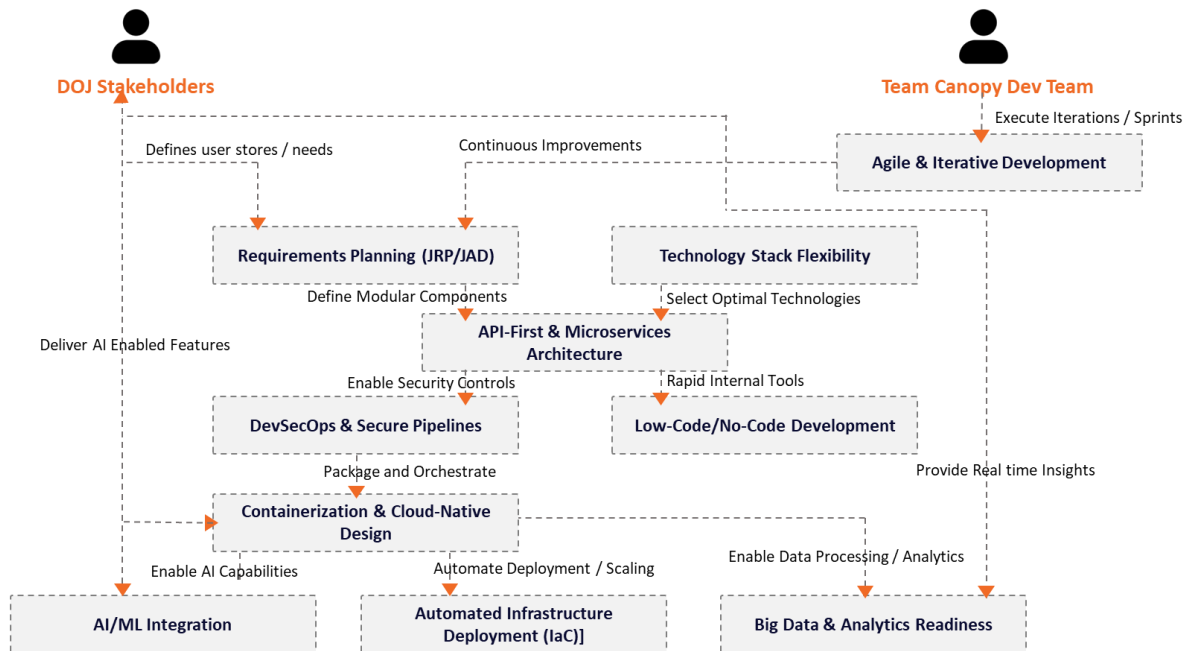
**Approach:**

- **Agile and Iterative Development**
  - Employ Agile Scrum, Kanban, and SAFe (Scaled Agile Framework) methodologies to support iterative delivery with continuous stakeholder involvement.
  - Tailor Agile ceremonies—including sprint planning, daily stand-ups, backlog grooming, and sprint reviews—to ensure DOJ engagement and feedback is integrated throughout development.
  - Support parallel task orders through scalable Agile teams able to coordinate dependencies and share reusable components.

- **Collaborative Requirements Definition**
  - Facilitate Joint Requirements Planning (JRP) and Joint Application Development (JAD) sessions with DOJ stakeholders to define user stories, process flows, and system requirements collaboratively.
  - Use visualization tools (e.g., wireframes, process maps) to validate requirements early, minimizing rework and aligning system capabilities with DOJ's functional needs.

- **Modular, API-First, and Microservices Architecture**
  - Design systems using API-first principles with RESTful and GraphQL services to enable seamless integration and interoperability with existing DOJ systems and future platforms.
  - Implement microservices architectures to support modular development, independent scaling, simplified maintenance, and service reuse across multiple BPA Calls.

- **Accelerated Delivery through Low-Code/No-Code Platforms**
  - Where appropriate, leverage low-code/no-code platforms for rapid development of internal tools, dashboards, and lightweight applications.
  - Empower DOJ business users with configurable applications that reduce development cycles and improve responsiveness to changing requirements.

- **DevSecOps Integration for Secure Development**

- o Fully integrate DevSecOps practices into our pipelines, embedding automated static (SAST) and dynamic (DAST) code analysis, continuous testing, and compliance validation.
- o Utilize tools (e.g., SonarQube, Jenkins, GitHub Actions) to automate security scanning and ensure each build aligns with federal security requirements, including FedRAMP, NIST RMF, and FISMA.

- **Technology Stack Flexibility and Expertise**
  - o Leverage enterprise platforms and languages aligned with DOJ's environment, and selecting the most suitable technologies per task.
  - o Where applicable, propose using platforms such as ServiceNow or equivalent for case management or workflow automation, ensuring compatibility and reusability.

- **Containerization and Cloud-Native Architectures**
  - o Design and deploy applications using containerized environments (Docker, Kubernetes) for scalability, portability, and efficient resource utilization.
  - o Support cloud-native development with serverless computing (e.g., AWS Lambda, Azure Functions) for event-driven tasks, improving flexibility and cost-efficiency.

- **AI/ML Integration for Enhanced Capabilities**
  - o Incorporate AI/ML models and algorithms, where applicable, to support intelligent process automation, data-driven insights, and operational efficiency.
  - o Examples include natural language processing for document classification or predictive analytics to support decision-making—tailored to DOJ mission needs if required.

- **Big Data Architecture and Analytics Readiness**
  - o Support DOJ's potential data-heavy use cases by designing data lakes, warehouses, and ETL pipelines using platforms like Apache Spark, Snowflake, or equivalent tools.
  - o Enable real-time analytics and reporting capabilities for mission-critical functions such as system performance monitoring or anomaly detection.

- **Automated Infrastructure Deployment**
  - o Utilize Infrastructure-as-Code (IaC) tools such as Terraform and Ansible for consistent, rapid, and repeatable infrastructure provisioning across cloud and on-premises environments.
  - o Streamline environment replication for development, testing, and production, reducing human error and improving deployment speed.

**Key Success Factors:**
- **Agile and Secure Development Workflows:** Continuous delivery cycles integrated with automated testing, compliance checks, and real-time feedback loops.
- **Legacy System Interoperability:** Use of APIs and middleware to integrate new solutions with DOJ's existing systems, minimizing disruptions during modernization.
- **Scalable, AI-Ready Design:** Architected to support AI/ML, big data, and emerging technologies without requiring future re-architecture.
- **Cloud-Native and Modular Design:** Supporting hybrid and multi-cloud deployments, enabling flexibility and service reusability across task orders.

**Value Proposition:**

- Accelerated Delivery of Mission-Critical Applications: Faster time-to-value through Agile practices and low-code solutions.
- Cost-Effective and Reusable Components: Microservices and APIs reduce duplication and simplify maintenance.
- Reduced Risk and Downtime: DevSecOps ensures secure, resilient releases with automated rollback and rapid incident response.
- Long-Term Maintainability and Flexibility: Containerization, serverless computing, and IaC make DOJ systems future-proof and adaptable to change.

## 2.4 Operations Support & Sustainment

Our Operational support ensures the DOJ's mission-critical systems are continuously available, Operational support and sustainment are vital to ensuring that DOJ's mission-critical systems remain continuously available, optimized for performance, and protected from risks. Canopy One understands that sustaining complex IT systems in a dynamic operational environment requires not just reactive support but proactive, preventive measures to anticipate issues before they affect mission execution.

Our approach emphasizes real-time monitoring, predictive maintenance, structured knowledge management, and a tiered support model designed to maximize system uptime, improve user experience, and extend the lifecycle of DOJ's IT assets. We combine automation, analytics, and human expertise to ensure uninterrupted service delivery, rapid incident resolution, and continuous system optimization.
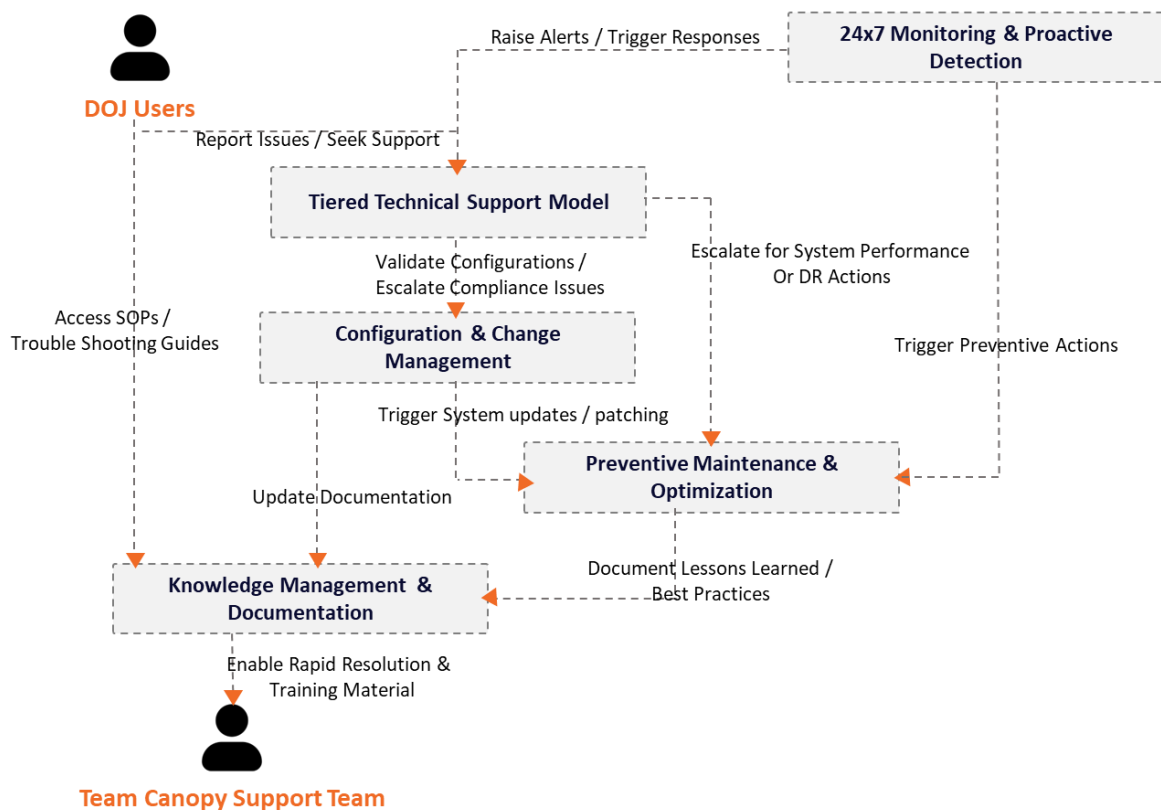


**Approach:**

- **24x7 Monitoring and Proactive Issue Detection**
  - Implement 24/7 monitoring of infrastructure, applications, and databases using advanced monitoring tools (e.g., Splunk, SentinelOne, ServiceNow or equivalent) to track system health, performance, and security.
  - Use real-time log analysis and AI-assisted anomaly detection to proactively identify and address potential issues—before they escalate into service disruptions.
  - Align incident response protocols with DOJ's escalation procedures, ensuring timely detection, automated alerting, and rapid incident resolution.
- **Tiered Technical Support Model**

Establish a three-tiered support framework to provide rapid issue resolution, efficient escalation management, and expert-level problem solving:
  - **Tier 1 - Help Desk Support:** Initial user support, triage, basic troubleshooting, and guidance.
  - **Tier 2 - Application and Database Support:** In-depth issue analysis, platform-level troubleshooting, and database administration (DBA) support for performance and data integrity.
  - **Tier 3 - Engineering and Expert Support:** Advanced technical support, root cause analysis, complex bug fixes, and architecture-level problem resolution.
- **Configuration and Change Management**
  - Maintain a centralized Configuration Management Database (CMDB) to track system components, software versions, configurations, and dependencies.
  - Enforce rigorous change management processes to minimize risks associated with updates, patches, and infrastructure modifications.
  - Ensure comprehensive asset visibility and support auditability of system changes.
- **Preventive Maintenance and Optimization**
  - Conduct routine patching, system updates, backups, and disaster recovery (DR) testing to ensure resilience and data protection.
  - Implement performance tuning, database optimization, and periodic health checks to enhance system stability and reduce latency.
  - Execute capacity planning and predictive scaling to ensure systems handle workload spikes without degradation.
- **Knowledge Management and Documentation**
  - Establish a robust knowledge repository using platforms like **Confluence or SharePoint** to document known issues, resolutions, procedures, and best practices.
  - Continuously capture lessons learned and incorporate them into standard operating procedures (SOPs) to facilitate rapid issue resolution and reduce knowledge loss.
  - Empower DOJ personnel with access to training materials, troubleshooting guides, and system documentation to support self-service and knowledge transfer.

**Key Success Factors:**
- **Proactive Monitoring and Predictive Maintenance:** Leveraging AI-driven monitoring tools to prevent incidents before they impact operations.
- **Scalable Support Model:** Tiered support ensures DOJ receives the right expertise at the right time while allowing scalability based on workload and task order demands.

- **Knowledge Retention and Accessibility:** Structured knowledge management reduces dependency on individuals and improves troubleshooting efficiency.

**Value Proposition:**
- **Enhanced System Availability and Performance:** Continuous monitoring and preventive maintenance ensure mission systems operate at peak efficiency with minimal downtime.
- **Optimized Resource Utilization and Cost Efficiency:** Proactive support minimizes expensive emergency fixes and system failures, extending the lifespan of DOJ's IT assets.
- **Risk Reduction and Rapid Recovery:** Rigorous change control, DR readiness, and expert escalation paths reduce operational risks and support fast recovery when incidents occur.
- **Empowered Users and Stakeholders:** Knowledge management enhances DOJ's internal capacity, enabling quicker resolutions and better informed system users.

### 2.5 IT Security & Compliance

Given the sensitive nature of the Department of Justice (DOJ)'s data, systems, and mission operations, robust security and compliance are fundamental to every aspect of Canopy One's technical approach. Protecting DOJ's assets requires embedding security controls throughout the solution lifecycle—from design and development to deployment and operations—while maintaining strict compliance with federal mandates and DOJ-specific security policies.

Our strategy emphasizes Zero Trust Architecture (ZTA), continuous monitoring, automated security testing, and proactive threat detection. By integrating cybersecurity best practices, advanced tools, and continuous compliance verification, Canopy One ensures DOJ's systems remain resilient against evolving cyber threats and aligned with stringent federal requirements.
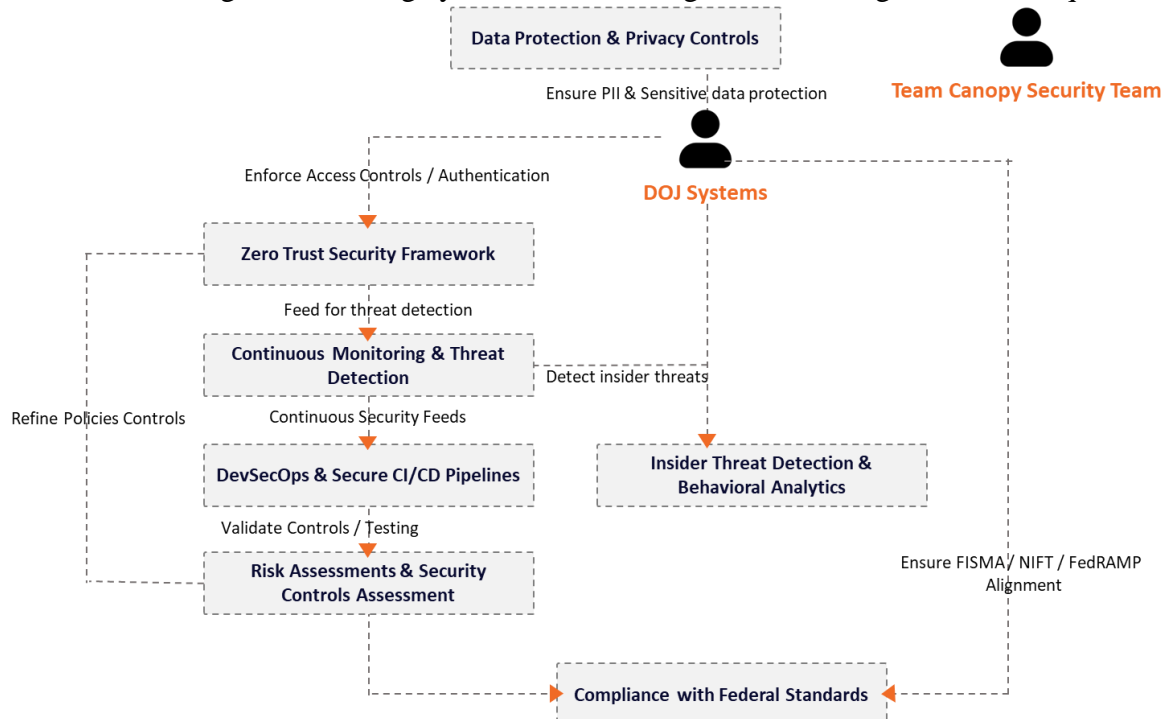


**Approach:**
- **Zero Trust Security Framework**

- o Implement a Zero Trust Architecture (ZTA) where no user, device, or application is inherently trusted inside or outside the network perimeter.
- o Enforce least-privilege access controls, micro-segmentation, and continuous authentication to protect sensitive data and critical DOJ systems.
- o Utilize Identity and Access Management (IAM) frameworks and support integration with multi-factor authentication (MFA) solutions to strengthen access security.

- **Continuous Monitoring and Threat Detection**
  - o Deploy real-time, continuous monitoring solutions to track system activities, detect anomalies, and generate automated alerts for potential threats.
  - o Leverage tools such as Splunk, SentinelOne, Tenable Nessus (or equivalent) for comprehensive log analysis, vulnerability scanning, and endpoint threat detection.
  - o Incorporate AI-driven analytics and machine learning models to enhance behavioral analysis, detect insider threats, and predict emerging risks based on anomalous patterns.

- **Security Integration in DevSecOps Pipelines**
  - o Embed security-as-code into Continuous Integration/Continuous Deployment (CI/CD) pipelines to automate vulnerability detection and enforce secure coding practices.
  - o Perform Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) during development to identify vulnerabilities early in the software lifecycle.
  - o Integrate compliance verification scripts within deployment pipelines to ensure continuous adherence to federal security standards.

- **Risk Assessments, Security Controls Assessment (SCA), and Audits**
  - o Conduct regular risk assessments to identify, evaluate, and mitigate security risks associated with systems, data, and user interactions.
  - o Perform Security Controls Assessments (SCA) to validate the effectiveness of security controls and recommend improvements.
  - o Prepare systems for external audits and certifications by ensuring evidence collection, documentation, and testing align with DOJ and federal standards.

- **Alignment with Federal Security Standards and Policies**
  - o Design, develop, and operate systems fully compliant with federal cybersecurity requirements, including:
    - Federal Information Security Management Act (FISMA)
    - National Institute of Standards and Technology Risk Management Framework (NIST RMF)
    - Federal Risk and Authorization Management Program (FedRAMP)
    - DOJ-specific cybersecurity and privacy policies
  - o Maintain continuous awareness of evolving compliance standards and incorporate updates proactively into system designs and operations.

- **Insider Threat Detection and Behavioral Analytics**
  - o Implement advanced behavioral analytics tools to monitor user behavior and detect anomalous activities indicative of insider threats or compromised accounts.
  - o Integrate user behavior analytics (UBA) and endpoint detection and response (EDR) systems to enable DOJ to proactively identify and respond to suspicious activities.

- **Data Protection and Privacy Controls**

o Enforce robust data protection mechanisms, including encryption at rest and in transit, secure key management, and role-based access controls (RBAC).
o Apply privacy controls aligned with DOJ guidelines to safeguard personally identifiable information (PII) and sensitive law enforcement data.

**Key Success Factors:**
- **Security at Every Layer:** Integrating security from the outset of system design, through development, deployment, and operations, reduces vulnerabilities and enhances resilience.
- **Continuous Monitoring and AI-Powered Threat Detection:** Real-time visibility into system activities combined with AI-enhanced detection reduces response times and improves defense against sophisticated threats.
- **Compliance-Driven Frameworks:** Strict alignment with FISMA, NIST RMF, FedRAMP, and DOJ-specific policies ensures consistent compliance and audit readiness.
- **Insider Threat and Behavioral Monitoring:** Proactive monitoring and behavioral analysis strengthen defenses against internal risks—often the most challenging to detect.

**Value Proposition:**
- **Strengthened Cyber Defense:** Our integrated approach enhances DOJ's cybersecurity posture, reducing exposure to external and internal threats while maintaining system integrity.
- **Automated Compliance and Cost Savings:** Automation of security scans, compliance checks, and reporting reduces manual effort, lowers operational costs, and minimizes the risk of audit findings.
- **Enhanced Data Protection:** DOJ's sensitive data—ranging from law enforcement records to financial and legal information—is safeguarded through layered defenses and continuous validation.
- **Rapid Incident Response and Recovery:** Real-time monitoring, AI-driven analytics, and pre-established response protocols ensure DOJ can contain and recover from security incidents swiftly with minimal operational impact.

### 2.6 Cloud Services & DevOps

Cloud adoption and DevOps practices are central to DOJ's modernization efforts. Canopy One Cloud computing and DevOps are foundational to achieving the DOJ's goals of rapid modernization, enhanced scalability, and increased operational efficiency under the RTS BPA. Canopy One recognizes that cloud adoption is not merely about infrastructure migration but about enabling agility, resilience, and secure delivery of mission-critical services.

Our approach focuses on leveraging FedRAMP-authorized cloud platforms, implementing automation through Infrastructure as Code (IaC), and integrating DevSecOps pipelines to support continuous delivery, monitoring, and compliance. By combining these capabilities, we enable DOJ to realize faster release cycles, reduce technical debt, and maintain secure, cost-optimized cloud operations that adapt to evolving mission requirements.
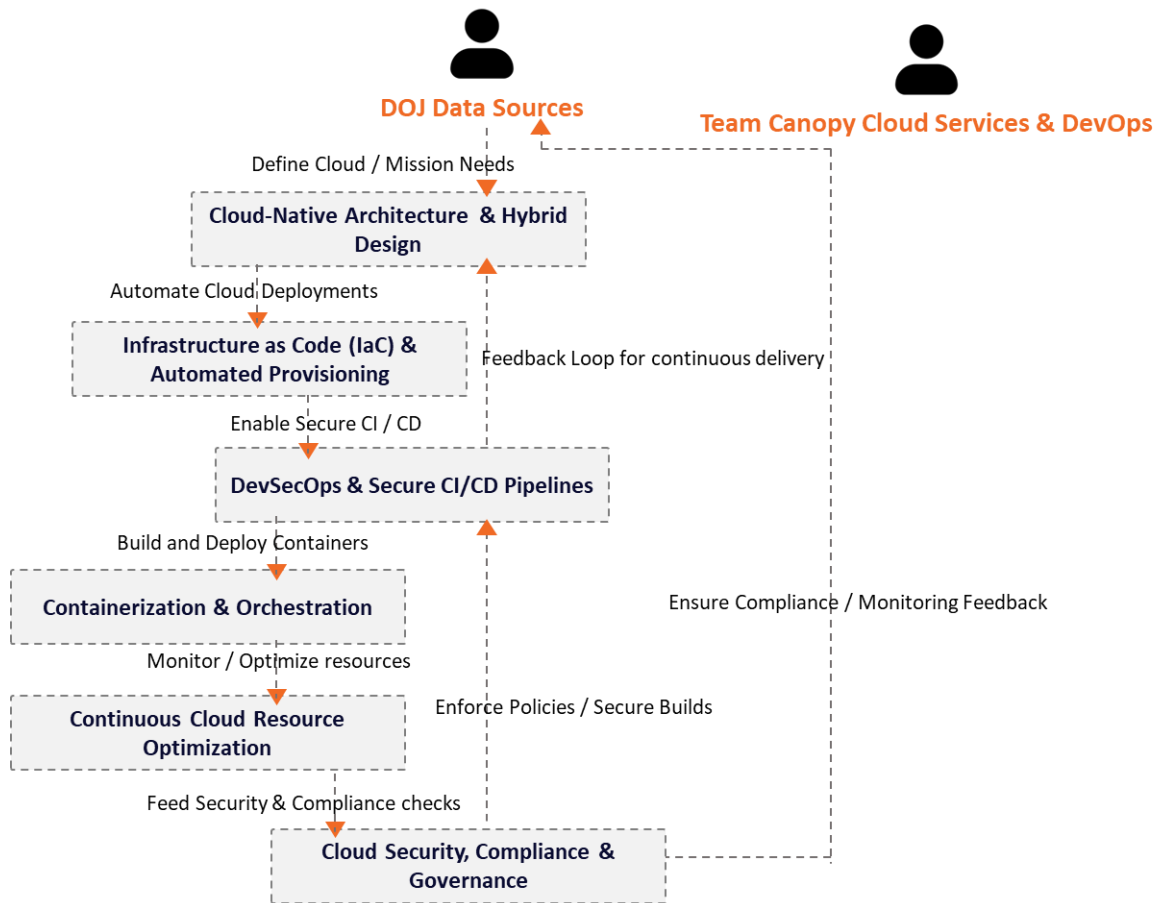
**Approach:**

- **Cloud-Native Architecture and Design**
  - Design scalable, secure, and modular cloud architectures tailored to DOJ's mission requirements using FedRAMP-certified platforms such as AWS, Microsoft Azure, and Google Cloud Platform (GCP).
  - Architect hybrid cloud or multi-cloud solutions where appropriate, ensuring interoperability between DOJ's on-premises systems and cloud environments.
  - Apply best practices such as auto-scaling, high availability, disaster recovery, and fault tolerance in cloud design to ensure mission continuity.
- **Infrastructure as Code (IaC) and Automated Provisioning**
  - Leverage Infrastructure as Code (IaC) tools such as Terraform, Ansible, or equivalent to automate cloud resource provisioning, configuration, and versioning.
  - Codify infrastructure templates to enable rapid, consistent, and repeatable environment deployments across development, testing, and production stages.
  - Utilize IaC to minimize human error, ensure traceability of changes, and accelerate deployment cycles.
- **DevSecOps and Continuous Integration/Continuous Deployment (CI/CD)**
  - Establish secure, automated CI/CD pipelines that enable DOJ to rapidly build, test, and deploy applications with integrated security checks and compliance validation at every stage.

- o Incorporate tools such as Jenkins, GitHub Actions, Azure DevOps, or similar to manage code integration, automated testing, and release management.
- o Integrate automated security scans, code quality checks, and compliance enforcement into pipelines to ensure every release meets DOJ's cybersecurity standards.
- **Containerization and Orchestration**
  - o Containerize application components using Docker to enable portability, rapid deployment, and efficient resource utilization.
  - o Use Kubernetes or equivalent orchestration platforms to manage container clusters, support dynamic scaling, and simplify deployment of microservices architectures.
  - o Enhance application resilience and availability by distributing workloads and enabling automated failover.
- **Continuous Cloud Resource Optimization**
  - o Implement cloud cost monitoring and optimization practices to manage resource utilization efficiently and control operational expenditures.
  - o Use cloud-native tools or third-party solutions to identify underutilized resources, right-size instances, and automate cost-saving actions where feasible.
  - o Perform periodic reviews of cloud consumption against performance requirements to ensure optimal balance between cost and system responsiveness.
- **Cloud Security, Compliance, and Governance**
  - o Integrate cloud-native security features and third-party tools for continuous monitoring, encryption, identity management, and threat detection within cloud environments.
  - o Ensure compliance with FedRAMP, FISMA, NIST RMF, and DOJ-specific security policies by embedding automated policy enforcement and audit trails.
  - o Utilize IAM controls, role-based access management, and secure API gateways to maintain a strong cloud security posture.

**Key Success Factors:**
- **Automated, Repeatable Deployments:** Leveraging IaC ensures consistent environment provisioning, minimizing manual errors and reducing deployment times.
- **Scalable, Flexible Architecture:** Supports DOJ's ability to scale resources up or down rapidly based on mission demand and workload fluctuations.
- **Security and Compliance by Design:** Security controls and compliance checks are integrated into every step of development and deployment, ensuring systems remain protected and audit ready.
- **Optimized Cloud Operations:** Ongoing monitoring and cost management practices ensure DOJ maximizes the value of its cloud investments.

**Value Proposition:**
- **Accelerated Delivery and Innovation:** Automated pipelines and cloud-native designs enable faster delivery cycles, allowing DOJ to respond quickly to mission-critical needs.
- **Cost-Effective Cloud Management:** Continuous optimization reduces waste and ensures DOJ's cloud operations are aligned with budgetary and performance objectives.
- **Sustainable, Future-Ready Infrastructure:** Modular and containerized architectures support long-term maintainability, easier upgrades, and seamless adoption of emerging technologies.

- **Enhanced Security and Control:** Integrated DevSecOps and governance frameworks maintain DOJ's control over cloud environments while reducing risk exposure.

## 2.7 Artificial Intelligence & Data Analytics

The Department of Justice (DOJ) generates and manages vast volumes of structured and unstructured data across its mission areas. Extracting actionable insights from this data is critical to driving informed decision-making, detecting risks, enhancing operational efficiency, and supporting complex investigations and legal proceedings.

Canopy One understands that leveraging Artificial Intelligence (AI), Machine Learning (ML), and advanced data analytics frameworks enable DOJ to shift from reactive data processing to proactive, insight-driven operations.

Our approach combines scalable data architectures, robust governance, and AI models designed with transparency, fairness, and compliance in mind—empowering DOJ to maximize the value of its data assets while maintaining control and security.
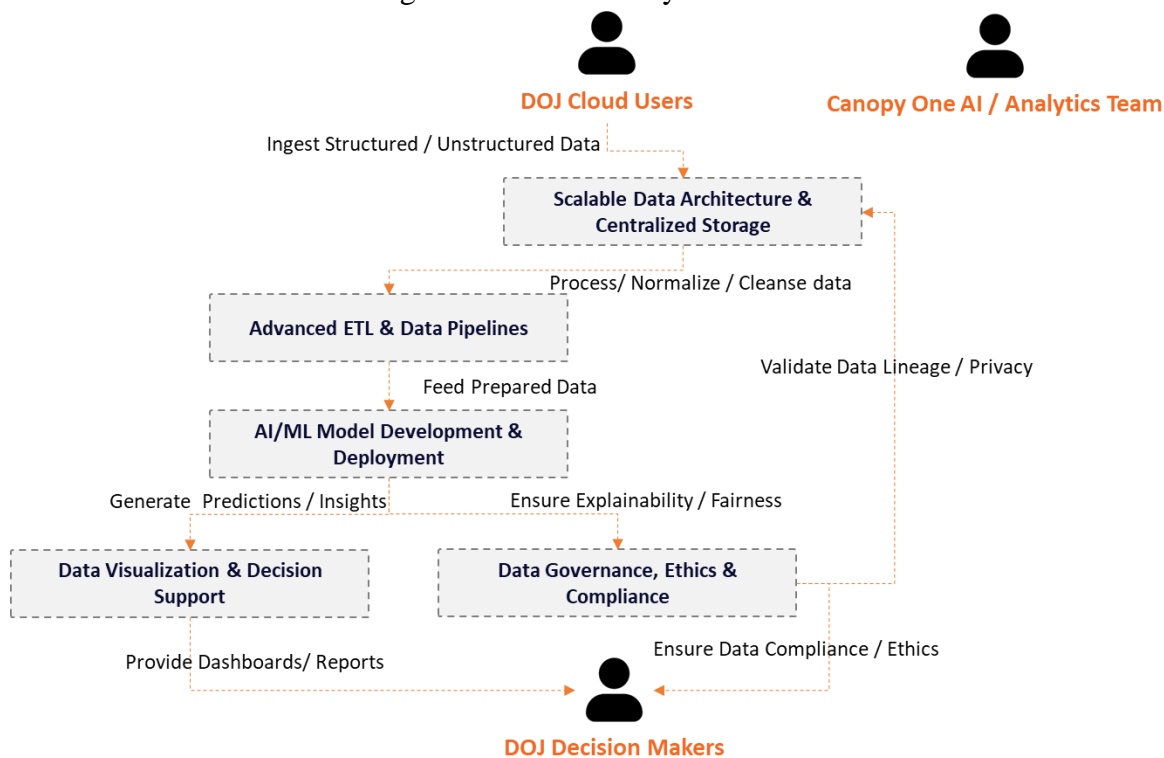


**Approach:**

- **Scalable Data Architecture and Centralized Storage**
  - o Design and implement data lakes and data warehouses capable of handling large-scale data ingestion from multiple DOJ sources.
  - o Support structured, semi-structured, and unstructured data storage, enabling comprehensive analysis across diverse data types, including documents, audio, video, and metadata.
  - o Ensure storage environments are scalable, secure, and compliant with DOJ data protection policies.
- **Advanced ETL Pipelines for Data Processing**

- o Develop Extract, Transform, Load (ETL) and streaming data pipelines to support real-time, near-real-time, and batch processing of DOJ datasets.
- o Use industry-standard tools and platforms (examples include Apache NiFi, AWS Glue, Talend, or equivalents) to ensure reliable data flow and preparation for analytics or AI model consumption.
- o Implement data validation, cleansing, and normalization routines to improve data quality and analysis accuracy.

- **AI/ML Model Development and Deployment**
  - o Design and train AI/ML models tailored to DOJ's mission needs, such as:
    - ▪ Predictive analytics for case outcomes, resource forecasting, or fraud detection.
    - ▪ Natural Language Processing (NLP) models for document summarization, legal text classification, and entity recognition to support case management.
    - ▪ Pattern recognition and anomaly detection for investigations or risk assessment.
  - o Enable model explainability and traceability to ensure transparency and compliance with emerging ethical AI guidelines.

- **Data Visualization and Decision Support**
  - o Develop interactive dashboards and reporting tools using platforms such as Power BI, Tableau, or equivalent to translate complex datasets and AI-generated insights into actionable information for DOJ decision-makers.
  - o Enable visual drill-downs, trend analyses, and real-time monitoring dashboards for operational and strategic use cases.

- **Data Governance, Ethics, and Compliance**
  - o Implement a robust data governance framework ensuring data lineage, quality, access control, and privacy protections are maintained across all AI and analytics workflows.
  - o Align AI/ML activities with the NIST AI Risk Management Framework (RMF) and DOJ's policies for responsible AI use.
  - o Apply ethical AI principles to mitigate bias, ensure fairness, and safeguard civil liberties in model design and deployment.
  - o Integrate compliance checks to protect sensitive information, including personally identifiable information (PII) and law enforcement data.

**Key Success Factors:**

- **Scalable and Future-Ready AI Models:** Designed to accommodate DOJ's growing data volumes and evolving mission requirements.
- **Mission-Aligned Use Cases:** AI/ML models are developed to directly support DOJ's functional needs, such as fraud detection, case analytics, and resource planning.
- **Ethical AI and Robust Governance:** Built-in controls ensure models are explainable, fair, and compliant with legal and ethical standards, reducing risks related to algorithmic bias or misuse.

**Value Proposition:**

- **Enhanced Data-Driven Decision-Making:** Empowers DOJ with real-time, predictive insights that improve operational efficiency, resource allocation, and mission success.
- **Reduced Manual Workload and Improved Accuracy:** AI/ML automation minimizes repetitive tasks, accelerates analysis, and reduces the risk of human error in complex data assessments.

- **Proactive Risk Identification:** Advanced analytics and AI enable DOJ to identify potential risks, fraud, or anomalies early—supporting preemptive actions rather than reactive responses.
- **Sustainable AI/Analytics Framework:** A modular, scalable approach that allows DOJ to evolve its AI/analytics capabilities over time without major re-architecture.

### 2.8 End-User Support & Training

Sustainable system adoption, operational efficiency, and user satisfaction within DOJ depend on the ability of personnel to confidently use, maintain, and maximize the systems delivered under the RTS BPA. Canopy One recognizes that comprehensive end-user support and targeted training are critical to empowering DOJ's workforce and ensuring long-term success.

Our approach focuses on delivering structured, role-based training programs, providing responsive user support, and establishing knowledge-sharing mechanisms that reduce dependency on vendor support. We design continuous learning environments that adapt to different learning styles, promote user self-sufficiency, and support DOJ's evolving mission needs.
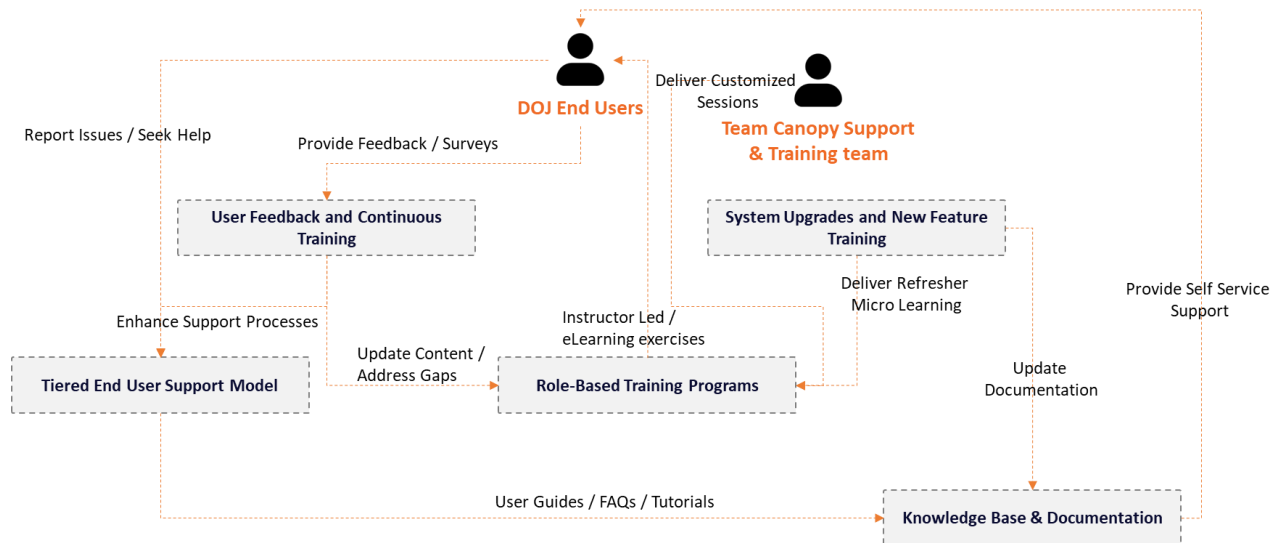


**Approach:**
- **Role-Based, Customized Training Programs**
  - o Design and deliver role-specific training programs tailored to DOJ user groups, including administrators, analysts, technical staff, and end-users.
  - o Training formats include:
    - Instructor-led sessions (in-person and virtual) for hands-on learning and interactive Q&A.
    - Self-paced e-learning modules covering key system functionalities and processes.
    - Scenario-based exercises to reinforce real-world application of new systems and tools.
  - o Update training content continuously to reflect system changes, upgrades, and lessons learned.
- **Tiered End-User Support Model**

- o Provide a multi-level user support framework to ensure DOJ users receive prompt assistance:
    - **Tier 1 - Help Desk Support:** General inquiries, password resets, system navigation support.
    - **Tier 2 - Functional/System Support:** Application-specific troubleshooting, workflow clarifications, and configuration assistance.
    - **Tier 3 - Technical Support and Escalation:** Addressing complex system issues, bugs, or backend errors that require developer or engineering involvement.
- **Comprehensive Documentation and Knowledge Base**
    - o Develop and maintain an easily accessible **knowledge base** that includes:
        - User manuals and quick reference guides tailored to DOJ's systems.
        - FAQs covering common tasks and troubleshooting steps.
        - Video tutorials and how-to guides to support visual learners and reinforce complex processes.
    - o Update documentation regularly to reflect software enhancements and policy changes.
- **User Feedback, Continuous Learning, and Knowledge Retention**
    - o Implement feedback loops to collect user input after training sessions, during support interactions, and through periodic surveys.
    - o Use feedback to:
        - Identify knowledge gaps.
        - Improve training materials.
        - Enhance support service delivery.
    - o Capture lessons learned and best practices in the knowledge base to support knowledge continuity, especially during staff transitions or turnover.
- **Support for System Upgrades and New Feature Adoption**
    - o Provide change management support, including refresher training and updated guides, when new system features or upgrades are deployed.
    - o Offer targeted micro-learning modules to enable quick adoption of new functionalities without disrupting daily operations.

**Key Success Factors:**
- **Flexible, Multi-Modal Training Delivery:** Supports varied learning styles and user needs across DOJ's diverse workforce.
- **Sustainable Knowledge Management:** Ensures knowledge is retained and accessible, reducing the learning curve for new staff and minimizing repetitive support requests.
- **Continuous Improvement:** User feedback is actively used to refine training programs and support services, ensuring relevance and effectiveness over time.
- **Seamless Integration with System Rollouts:** Training and support are tightly aligned with system implementations, updates, and new feature releases to ensure user readiness.

**Value Proposition:**
- **Increased User Confidence and Self-Sufficiency:** DOJ personnel gain the skills and resources needed to operate systems effectively, reducing reliance on vendor support for routine tasks.
- **Accelerated System Adoption:** Structured onboarding and hands-on training enable quicker adoption of new tools and workflows, enhancing productivity.

- **Lower Long-Term Support Costs:** Knowledge transfer reduces recurring support requests, enabling DOJ to sustain operations with minimal vendor intervention.
- **Improved User Satisfaction and Performance:** Clear documentation, responsive support, and continuous learning foster a positive user experience and efficient system use.

### 2.9 Records & Document Management

Effective records and document management is essential to ensure compliance with federal regulations, safeguard sensitive information, support legal defensibility, and preserve institutional knowledge. For DOJ, where records may contain sensitive law enforcement, legal, and administrative information, the ability to manage records efficiently, securely, and in compliance with the National Archives and Records Administration (NARA) guidelines is critical.

Canopy One's approach ensures DOJ's records lifecycle—from creation and active use to retention and disposition—is managed systematically. We focus on integrating records management capabilities directly into DOJ's mission systems, automating key processes, and ensuring records are readily accessible, auditable, and protected against unauthorized access or accidental loss.
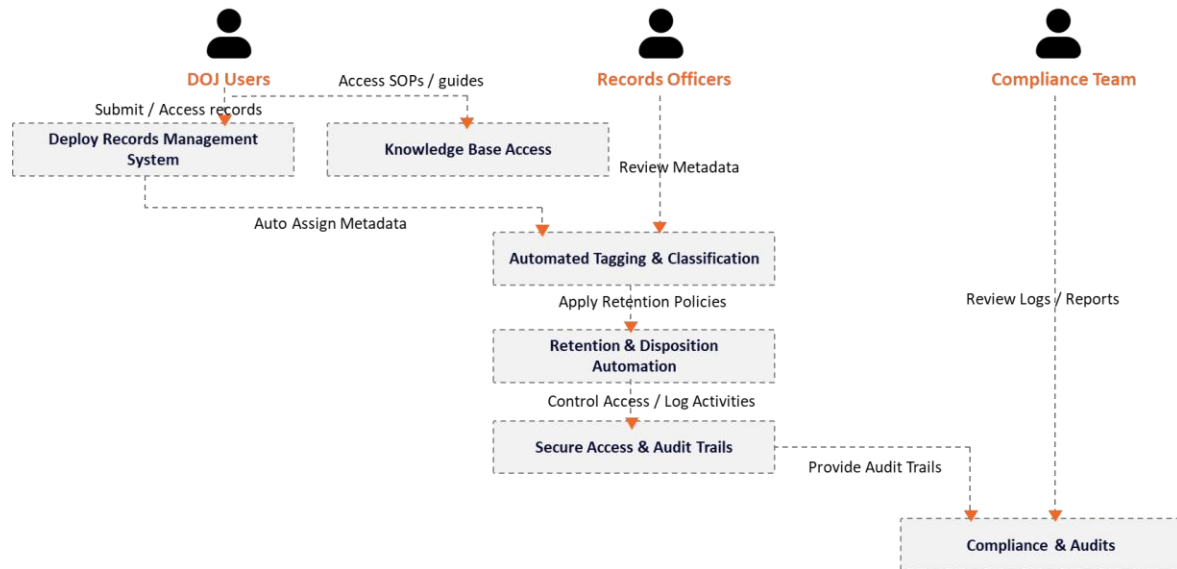


**Approach:**

- **Deployment of Compliant Records Management Systems**
  - Implement records and document management solutions that are compliant with NARA guidelines, DOJ policies, and federal records regulations.
  - Ensure systems support management of both electronic and physical records, handling diverse formats including documents, emails, audio/video files, and case files.
  - Integrate records management capabilities within DOJ's existing platforms and systems to reduce silos and support efficient access.
- **Automation of Recordkeeping Processes**
  - Automate document tagging, classification, metadata assignment, and indexing to ensure accurate record categorization and retrieval.
  - Implement automated retention schedules that enforce timely archival or destruction of records based on NARA-approved schedules and DOJ-specific retention policies.

- o Enable automated alerts for record reviews, retention period expirations, and destruction approvals, minimizing manual intervention and human error.
- **Secure Access, Version Control, and Auditability**
  - o Provide role-based access controls (RBAC) and encryption mechanisms to ensure records are accessed only by authorized personnel.
  - o Maintain version control and detailed audit trails for every record to track changes, access events, and movement across systems, supporting accountability and compliance audits.
  - o Ensure disaster recovery and backup protocols are in place to protect records from data loss or corruption.
- **Seamless Integration with DOJ Mission Systems**
  - o Design records management workflows to integrate with case management, litigation support, Freedom of Information Act (FOIA) systems, and other DOJ applications.
  - o Facilitate easy retrieval of relevant records to support legal proceedings, investigations, and public records requests.
  - o Ensure interoperability with federal government-wide records systems where necessary to maintain consistency in compliance and reporting.
- **Support for eDiscovery, Litigation Hold, and Compliance Reviews**
  - o Provide capabilities to support eDiscovery requests, including search, legal holds, and extraction of relevant records.
  - o Enable DOJ to quickly identify and preserve records subject to litigation holds while continuing normal operations on other records.

**Key Success Factors:**

- **Strict Adherence to NARA and DOJ Policies:** Comprehensive compliance reduces the risk of audit findings or legal exposure.
- **Automation Reduces Errors and Increases Efficiency:** Minimizes manual effort while ensuring accurate and timely record management activities.
- **Seamless System Integration:** Embedding records management within DOJ's operational systems enhances usability and accessibility without disrupting workflows.
- **Enhanced Search and Retrieval Capabilities:** Metadata tagging and indexing support quick access to mission-critical records.

**Value Proposition:**

- **Streamlined Records Lifecycle Management:** Canopy One's approach ensures records are created, maintained, and disposed of according to policy, reducing the burden on DOJ staff.
- **Improved Records Accessibility and Usability:** Integrated search, indexing, and tagging improve efficiency in retrieving records for investigations, legal reviews, or compliance reporting.
- **Minimized Compliance and Legal Risks:** Automated policy enforcement, secure access controls, and auditability reduce the risk of non-compliance, data breaches, or loss of critical records.
- **Sustainable Knowledge Preservation:** Long-term records management ensures DOJ retains institutional knowledge, historical data, and critical case information necessary for ongoing mission success.

3. **STAFFING APPROACH**
**3.1 Staffing Framework**

Recognizing the crucial role of effective staffing in achieving project success, Team Canopy is dedicated to implementing a comprehensive Staffing and Retention Plan that prioritizes recruiting, managing, and retaining highly qualified personnel.

Leveraging our proven experience from large-scale federal IT projects, our framework is designed to retain existing talent, minimize loss of knowledge, and maintain high service levels. The plan incorporates proactive recruitment, robust retention strategies, and contingency measures to manage unanticipated personnel challenges – all aligned with DOJ's mission and operational objectives.
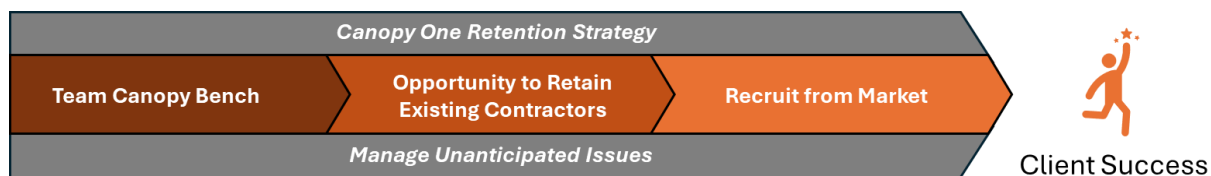


**Talent Engagement Process:**

- **Assessing**: We engage closely with DOJ to understand project needs, goals, and organizational culture—building success profiles that align technical skills and traits with DOJ's environment.
- **Attracting**: Our 40+ global recruiters operate 24/7, supported by AI-driven tools and Applicant Tracking Systems (ATS), to target both active and passive candidates nationwide.
- **Evaluating**: Candidates undergo rigorous multi-step screening, skills assessments, and cultural fit evaluation, ensuring alignment with DOJ's high standards.
- **Selecting**: Once selected, candidates complete comprehensive onboarding in compliance with federal regulations, ensuring readiness from day one.

Below is a description of the ATS platform that we use for recruitment. One of the key strengths of Canopy One is a global recruitment capacity of 80+ recruiters working 24/7.



**Retaining the Existing Talent**

In our strategic approach to staffing for the DOJ project, Team Canopy places a high value on the expertise of personnel currently engaged through other vendors. Understanding the profound impact

that their accumulated knowledge and experience can have on our project outcomes, we are deeply committed to retaining as much of this existing talent as possible. These individuals have a nuanced understanding of the current environment, which is instrumental in navigating the complexities and specific challenges of the systems we will manage.

The continuity provided by retaining experienced personnel makes sure that our team remains robust and deeply informed, minimizing the learning curve and enhancing our ability to maintain high service levels without disruption. Their firsthand insights into past and ongoing operations are invaluable for troubleshooting, strategic planning, and implementing improvements effectively.

Efforts to integrate and retain these experienced team members are supported by a comprehensive approach that includes competitive compensation, professional development opportunities, and a positive work environment that aligns with their career goals and personal values. This strategic inclusion not only stabilizes our workforce but also enriches our team's capabilities, fostering a culture of excellence and continuity that will directly contribute to the success of the DOJ's objectives.

## Retention Approach

Team Canopy acknowledges that employee retention is critical for maintaining a motivated, skilled, and stable workforce. Our retention approach is multifaceted:

- **Competitive Compensation and Benefits**: We provide industry-competitive remuneration packages, periodically reviewed to reflect market and inflation changes.
- **Professional Development**: We offer extensive opportunities for training and development, which include workshops and access to industry certifications.
- **Positive Work Environment**: Our company culture emphasizes respect, inclusivity, and support, fostering a collaborative and supportive work environment.
- **Recognition and Rewards**: We recognize and reward significant employee contributions, enhancing job satisfaction and loyalty.

## Managing Unanticipated Personnel Issues

Team Canopy has proactive measures and contingency plans to manage unexpected personnel challenges effectively, ensuring seamless project execution:

- **Proactive Measures**: Regular check-ins and feedback sessions help us address potential concerns early, maintaining open communication with all employees.
- **Contingency Planning**: Our plans include a reserve of qualified personnel ready to fill roles temporarily, ensuring continuity in critical project areas.
- **Robust HR Support**: Our HR team is trained to handle various personnel issues, providing support and resolution with empathy and discretion.

These strategies are meticulously designed to align with DOJ's objectives and promote a successful partnership. Through this detailed management approach, Team Canopy is committed to delivering high-quality IT support services that meet and exceed DOJ's expectations.

### 3.2 Key Personnel

Team Canopy recognizes that high-caliber leadership and technical expertise are critical for successful contract execution and delivering mission-driven outcomes for the Department of Justice (DOJ). We have pre-identified, secured, and committed three highly qualified professionals for the Key Personnel roles, ensuring immediate operational readiness, domain expertise, and continuity throughout the engagement.

Each of these leaders brings not only extensive technical knowledge but also deep experience managing complex federal IT programs, understanding compliance requirements, and driving modernization efforts similar to DOJ's objectives under this BPA.

| Role | Candidate | Key Strengths & Value to DOJ |
|---|---|---|
| Program Manager | Andre Butters | Federal program leadership, Agile/DevOps expertise, experience with DOJ, SEC, DOL |
| Senior Solution Architect | Saurabh Saxena | 20+ years in enterprise architecture, Zero Trust, Cloud, AI/ML, TOGAF Certified |
| Scrum Master | Suja Rajasekharan Jalaja | Agile/SAFe leadership, Salesforce, 508 Compliance, USCIS/DOL federal experience |

**Program Manager – Andre Butters**

Andre Butters is a highly experienced Program Manager with over 16 years of leading complex federal IT programs. His extensive background managing large-scale initiatives for agencies like the Securities and Exchange Commission (SEC), Department of Labor (DOL), and Department of Justice (DOJ) makes him uniquely qualified to lead this engagement.

Key Qualifications & Value to DOJ:
- Proven leadership in Agile, DevOps, PMBOK, and Lean management methodologies
- Deep knowledge of federal governance frameworks and multi-vendor coordination
- Skilled in managing cost, schedule, and scope, while ensuring quality and client satisfaction
- Experience with contract oversight, performance monitoring, and risk mitigation
- Exceptional interpersonal and communication skills for effective stakeholder engagement
- Familiarity with DOJ's operational environment enhances his ability to align project execution with mission needs

**Value Contribution:**

Andre will ensure strategic leadership, contract compliance, proactive risk management, and continuous performance optimization—serving as the primary liaison to DOJ and ensuring seamless service delivery.

**Senior Solution Architect – Saurabh Saxena**

Saurabh Saxena is an accomplished Senior Solution Architect with over 20 years of experience in cloud computing, Zero Trust architecture, enterprise IT modernization, AI/ML integration, and cybersecurity—specializing in complex federal projects.

**Key Qualifications & Value to DOJ:**
- Certified TOGAF 10 Architect, capable of developing scalable, secure enterprise architectures
- Demonstrated success supporting USPS, DOT, Selective Service System (SSS), ATF, and healthcare domains

- Extensive experience in Zero Trust principles, FedRAMP compliance, and hybrid cloud architecture.
- Expertise in AI/ML solution design, predictive analytics, and big data frameworks
- Skilled in technology gap analysis, modernization roadmaps, and interoperability design
- Strong knowledge of federal IT policies, compliance standards (NIST RMF, FISMA, 508)

**Value Contribution:**
Saurabh will drive DOJ's technical strategy, ensuring solution architectures are future-proof, security-compliant, and mission-aligned—supporting complex integrations, emerging technologies, and continuous modernization.

### Scrum Master – Suja Rajasekharan Jalaja

Suja Rajasekharan Jalaja brings over 10 years of hands-on Agile leadership experience, serving as Scrum Master and Product Owner across federal projects, including at USCIS and DOL. Her expertise enables efficient Agile delivery in complex regulatory environments.
Key Qualifications & Value to DOJ:

- Deep understanding of Agile (Scrum, Kanban, SAFe) and DevOps methodologies
- Proven record of managing sprints, backlog grooming, and stakeholder collaboration
- Expertise in Salesforce platform support and compliance-driven development cycles
- Strong focus on 508 compliance, continuous testing, and DevSecOps integration
- Skilled in fostering team collaboration, transparency, and iterative process improvement
- Experienced in aligning Agile delivery with federal project governance requirements

**Value Contribution:**
Suja will ensure the Agile teams operate at peak efficiency, facilitating iterative delivery, sprint planning, and issue resolution—all while maintaining compliance and aligning development efforts with DOJ's mission needs.

### 3.3 Program Management, Communication, and Oversight Approach

Team Canopy with Canopy One acting as the Prime Vendor is committed to providing a strong program management structure, robust oversight, proactive communication, effective subcontractor management, and a disciplined quality control framework to ensure the successful execution of this engagement. Our approach is built on proven federal program management best practices, ensuring alignment with DOJ's objectives, timely delivery, risk mitigation, and stakeholder satisfaction.

### Governance and Oversight

Our governance model ensures clear lines of authority, accountability, and collaboration across all contract activities. This structure supports performance monitoring, continuous improvement, and rapid decision-making.

- **Program Manager (PM):** The Program Manager serves as the day-to-day leader and a single point of accountability for this contract. The PM is responsible for:
  - Overseeing all program operations, ensuring delivery milestones are met
  - Managing resource allocation, including staffing adjustments based on task order requirements
  - Monitoring contract compliance, financial performance, and schedule adherence
  - Providing strategic direction to project teams
  - Facilitating coordination between DOJ, subcontractors, and internal teams

- o   Serving as the primary point of contact (POC) for DOJ, ensuring responsiveness and transparency
- **Executive Oversight:** Team Canopy's senior leadership provides executive-level program governance by:
    - o   Monitoring contract health, risk exposure, and overall performance metrics
    - o   Conducting periodic internal reviews to assess compliance with contract requirements and service level agreements (SLAs)
    - o   Escalating unresolved programmatic issues and ensuring accountability at the leadership level
    - o   Serving as an escalation point for DOJ should critical issues arise that require executive intervention
- **Technical Leads / Subject Matter Experts (SMEs):** Our Technical Leads and SMEs ensure the technical quality, security, and compliance of all deliverables by:
    - o   Overseeing daily technical workstreams
    - o   Ensuring alignment with DOJ's strategic objectives, IT standards, and security policies
    - o   Supporting Agile sprint planning, backlog refinement, and technical decision-making
    - o   Ensuring compliance with federal regulations, including FISMA, FedRAMP, NIST RMF, and Section 508

## Communication and Escalation

Team Canopy emphasizes structured, proactive, and transparent communication at all levels to ensure project alignment, rapid issue resolution, and informed decision-making.

- **Structured Multi-Level Escalation Framework:**
    - o   **Tier 1:** Scrum Master / Technical Leads handle daily operational and technical challenges
    - o   **Tier 2:** Program Manager addresses complex issues, resource challenges, and contractual matters
    - o   **Tier 3:** Executive Leadership engages when unresolved programmatic risks require escalation or strategic decisions impacting contract delivery

This framework ensures that issues are addressed at the appropriate level with escalation protocols enabling timely resolution and minimal disruption.

- **Regular Reporting and Stakeholder Engagement:**
    - **Bi-weekly Meetings with DOJ:** Program Manager leads bi-weekly status meetings to:
        - o   Review task progress, milestones, and upcoming deliverables
        - o   Discuss emerging risks, challenges, and resource needs
        - o   Facilitate two-way communication and feedback exchange
    - **Monthly Status Reports:** Comprehensive reports covering:
        - o   Performance metrics, SLA compliance, and resource utilization
        - o   Risk register updates and mitigation actions
        - o   Incident trends, lessons learned, and process improvements
        - o   Contractual deliverables status
    - **Ad-hoc Reporting:** Immediate updates and briefings on:
        - o   Urgent issues or incidents affecting service delivery
        - o   Requests from DOJ leadership

o   Unplanned risks or changes impacting project execution

## Quality Control and Risk Management

Ensuring the quality, timeliness, and compliance of all deliverables is central to Team Canopy's management approach. Our framework incorporates the federal program best practices, continuous improvement cycles, and proactive risk management strategies designed to align with DOJ's operational environment and toolsets.

**Task Tracking, Reporting, and Performance Monitoring Tools:** Team Canopy will leverage existing tools and systems within the DOJ environment for tracking, reporting, and performance monitoring. Where applicable, we are prepared to adapt to DOJ's preferred platforms to ensure seamless integration with agency workflows and reporting requirements.

Examples of tools we are experienced with and can adapt to include (but are not limited to):

- Agile task and sprint management: Tools like JIRA, Azure DevOps, or equivalent
- Incident and change management: Tools such as ServiceNow, Remedy, or agency-specific ticketing systems
- Data visualization and reporting: Platforms like Power BI, Tableau, or existing DOJ dashboards for real-time visibility into project health, risks, and KPIs

## Continuous Improvement and Lessons Learned

Our Program Manager will lead regular retrospectives, lessons learned sessions, and continuous improvement workshops as part of our Agile and ITIL-aligned management approach. This includes:

- Identifying process inefficiencies or bottlenecks impacting delivery
- Implementing corrective actions to improve performance and optimize operations
- Documenting best practices to enhance future task execution
- Establishing feedback loops with DOJ stakeholders to incorporate insights, evolving requirements, and mission-critical needs into future planning

This proactive approach ensures that the program continuously adapts and improves throughout the lifecycle of the engagement.

## Risk Register and Mitigation Strategies

We maintain a dynamic risk register as a living document, reviewed and updated regularly to support proactive risk management. This includes:

- Early identification of new risks as the project evolves
- Prioritization of risks based on impact and probability analysis
- Development of mitigation plans and contingency strategies tailored to each risk
- Continuous monitoring of risk status, triggers, and response actions

Risk discussions and updates will be integrated into bi-weekly meetings and monthly reporting to DOJ, ensuring transparent communication and enabling DOJ leadership to make informed, proactive decisions.

Team Canopy's Program Management, Communication, and Oversight Approach ensures:

- Accountability and transparency at every operational level
- Proactive risk identification and rapid mitigation
- Data-driven decision-making and performance visibility
- Collaborative stakeholder engagement

- Continuous improvement mechanisms aligned with DOJ mission priorities

By leveraging existing DOJ tools and systems, our approach delivers operational agility, efficiency, and measurable outcomes—ensuring DOJ's objectives are achieved with consistency, security, and quality throughout the contract.

### 3.4 Recruitment Timelines and Responsiveness

Team Canopy is fully committed to supporting DOJ's dynamic resource needs. Our recruitment framework is designed for agility, backed by a deep talent pool, AI-driven sourcing, and 24/7 recruiting operations.

For non-key personnel, our average recruitment cycle is 15 business days (excluding any government-mandated background investigations or clearance processing). This enables us to rapidly identify, vet, and onboard qualified candidates in response to task order requirements while adhering to DOJ's security protocols. By integrating existing talent familiar with DOJ's environment and deploying domain-specific experts, Team Canopy ensures sustained operational continuity and mission-aligned service delivery.

### 3.5 Small Business and Subcontractor Participation

Team Canopy is proud of our small business 8(a) status and our strong commitment to promoting small business participation in the delivery of this program. Our team consists of:

- **Canopy One Solutions Inc. (Prime Contractor):**
  - A small business, SBA 8(a)-certified firm with extensive experience delivering complex IT services across federal agencies. Our 8(a) status demonstrates our capability and capacity to support DOJ's mission while meeting small business utilization goals.

- **Stealth Solutions Inc. (Subcontractor):**
  - An SBA-certified 8(a) small business and a distinctive provider of innovative technology and management services. Stealth Solutions brings:
  - Deep expertise in low-code/no-code platforms
  - Advanced capabilities in cloud technologies, digital transformation, and emerging tech adoption
  - A strong record of success supporting federal agencies with modern technology solutions.

- **Value of the Team Canopy Approach**
  - Our combined team ensures:
  - Compliance with SBA small business goals
  - Diverse technical capabilities including emerging technology support
  - Expanded resource pool and rapid surge capability
  - Commitment to collaboration, innovation, and mission alignment

Together, Team Canopy delivers a small business-led, high-impact team fully capable of supporting DOJ's evolving technological needs while reinforcing the Department's commitment to small business participation.

Canopy One Solutions Inc.
Rapid Technology Services (RTS)
Solicitation Number: 15JPSS25Q00000041                    Solicitation Due Date:  04/04/2025 12:00 PM EDT

CANOPYONE

4. **PAST PERFORMANCES**

**4.1 Past Performance 1 – GPO (Government Publishing Office)**

| Client Name | GPO (Government Publishing Office) |
|---|---|
| Prime Vendor | Canopy One Solutions Inc |
| Project / Program Name | Functional Support for Oracle Business information Systems |
| Contract # | 040ADV-22-C-0145 |
| Contract Value | $4,341,504.00 |
| Period of Performance | Oct 1$^{st}$, 2022 – Sep 30$^{th}$ 2027 |
| Point of Contact | Timothy Archer, tarcher@gpo.gov |

**Description of the Project:**

Canopy One provides extensive functional support for GPO's Oracle-based Business Information Systems, focusing on critical business and financial modules. These modules include Projects, Payables and Receivables (AP & AR), Inventory, General Ledger, Fixed Assets, Purchasing, Contract Lifecycle Management (CLM), and more. Our services are designed to ensure the optimal performance, system sustainment, and operational continuity of these essential systems.

Our services include issue analysis and resolution, specializing in quickly addressing application issues, user concerns, and change requests to minimize disruptions and maintain the seamless flow of financial operations. Our support model aligns with Tiered Technical Support best practices, offering proactive monitoring, rapid troubleshooting, and detailed resolution pathways, ensuring availability of critical systems.

Our functional support encompasses proactive troubleshooting, system setup, and configurations, process optimization, and integration of evolving requirements such as new reporting needs or data-driven insights preparation, laying a foundation for advanced analytics readiness.

Comprehensive user-focused training programs empower staff to effectively use Oracle Financial modules, enhancing user adoption and reducing reliance on external support. Training materials are updated regularly, and user confidence is reinforced through targeted workshops, change management support, and just-in-time learning resources, reflecting a structured end-user support model.

Weekly status reports provide clear insights into financial operations, ongoing support activities, and areas for improvement. Additionally, we conduct meticulous accounting reconciliation between sub-ledgers and general ledgers to ensure financial accuracy and integrity.

These services address several challenges GPO faces, such as enhancing CLM support for acquisition teams by updating playbooks, refining training materials, and conducting user training sessions. Our support also extends to other Oracle suite modules and integrates new initiatives like GInvoicing. Through regular audits, preventive diagnostics, and a strong change management framework, we ensure optimal performance, efficiency, and compliance, allowing GPO to adapt to evolving requirements for sustained success.

### 4.2 Past Performance 2 – IRS (Internal Revenue Service)

| | |
|---|---|
| Client Name | IRS (Internal Revenue Service) |
| Prime Vendor | Canopy One Solutions Inc |
| Project / Program Name | BigFix Support |
| Contract # | 2032H524F00397 |
| Contract Value | $4,090,764.00 |
| Period of Performance | 8/2024 – 7/2029 |
| Point of Contact | Heller Amanda M, amanda.m.heller@irs.gov |

**Description of the Project:**

Canopy One Solutions Inc. provides comprehensive Operations Support and Sustainment for HCL BigFix to the IRS, focusing on operational optimization, advanced technical support, system sustainment, and continuous improvement. The engagement covers key BigFix modules including Lifecycle, Inventory, Compliance, and Insights—critical for maintaining system performance, compliance, and IRS mission readiness.

Leveraging their status as an HCL Federal Business Partner, and in collaboration with Four Inc., Canopy One delivers dedicated HCL Accelerated Value Program (AVP) services, which include proactive system assessments, risk mitigation, performance tuning, advanced troubleshooting, knowledge transfer, and acting as a liaison for HCL Federal support cases. This structured support aligns with Tiered Technical Support models, ensuring that BigFix systems operate efficiently to support mission-critical initiatives like tax code changes, while maintaining high availability and minimizing downtime.

A key aspect of Canopy One's approach is the review, integration, and optimization of automation strategies, aligning with AI/Data-Driven Task Areas of the RFP. The team enhances the performance and configuration of tools such as BigFix Runbook AI, ServiceNow, Ansible, and Tableau, supporting the IRS's automation-driven workflows for version upgrades, system health monitoring, SQL tuning, and bandwidth optimization.

These automation enhancements align with DevSecOps principles, improving workflow efficiency, enabling real-time monitoring, and streamlining incident management. Canopy One ensures faster issue resolution, reduced manual overhead, and improved scalability and resilience of BigFix operations—all critical to maintaining IRS system security and compliance.

Additionally, Canopy One emphasizes knowledge transfer and end-user enablement by executing a robust knowledge transition plan. IRS personnel receive hands-on training, process documentation, and operational support—empowering them to sustain optimized and automated operations long term, consistent with End-User Support & Training best practices.

### 4.3 Past Performance 3 – USAID (United States Agency for International Development)

| | |
|---|---|
| Client Name | USAID |
| Prime Vendor | Stealth Solutions Inc |
| Project / Program Name | Contract Hiring and Management Processing System (CHAMPS) |
| Contract # | 7200AA23C00083/YD1691253017F |
| Contract Value | $4,178,890.42 |
| Period of Performance | 09/2023 – 03/2026 |
| Point of Contact | Andrea McNamara, amcnamara@usaid.gov |

**Description of the Project:**

Stealth Solutions is currently implementing CHAMPS (Contract Hiring and Management Processing System) for USAID using Salesforce Government Cloud Plus, a FedRAMP-authorized Platform-as-a-Service (PaaS). CHAMPS is a low-code/no-code solution designed to streamline and modernize USAID's hiring and management of Personal Services Contractors (PSCs), replacing fragmented, manual, and spreadsheet-heavy processes.

**Project Scope:**

- Design and implementation of a centralized hiring and contractor management system on Salesforce Government Cloud Plus
- Use of low-code/no-code Salesforce tools including Flow, App Builder, and Process Builder for rapid configuration and scalability
- Integration with USAID identity and security services using platform-native access controls
- End-to-end automation of workflows related to hiring, approvals, onboarding, and contract management
- Development of dashboards, reporting tools, and audit trails for compliance and transparency
- Support for agile project execution with iterative releases and stakeholder engagement

**Key Technologies & Platform Features:**

- Salesforce Government Cloud Plus (FedRAMP High) – secure, scalable PaaS foundation
- Low-Code/No-Code Tools – Flow, Dynamic Forms, App Builder
- Salesforce Lightning Experience – for intuitive and responsive user interface
- Agile Project Delivery – sprint-based releases using Agile/Scrum methodologies
- Integrated Security – Role-Based Access Control (RBAC), multi-factor authentication, and FedRAMP compliance
- Cloud-Hosted Architecture – scalable, reliable access across global USAID offices

**Benefits:**

- Eliminates manual and inconsistent hiring processes
- Provides a **centralized, authoritative data source** for all contractor-related records
- Improves **data accuracy, process transparency, and reporting**
- Enables **automated workflows**, reducing processing times and administrative overhead
- Enhances oversight, compliance, and decision-making with real-time insights
- Supports **remote collaboration** and scalability across global missions

The CHAMPS project showcases Stealth Solutions' ability to deliver complex, mission-critical systems using modern cloud platforms and low-code solutions, accelerating delivery while ensuring flexibility, compliance, and long-term maintainability.