RESPONSE TO:

West Virginia Office of Inspector General

Investigation and Fraud Case Management System

CRFP 0513 OIG 2600000001 – TECHNICAL PROPOSAL ORIGINAL

6 January 2026

Prepared by:

IBM Consulting
Brian Cunningham
West Virigina Lead Client Partner
304-552-0032
brian.cunningham@ibm.com

IBM **Consulting**

"International Business Machines Corporation ("IBM") is submitting this Proposal, for services that will be led by IBM's Consulting division ("IBM Consulting")

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1838429
Doc Description: INVESTIGATIONS AND FRAUD CASE MANAGEMENT SYSTEM
Proc Type: Central Master Agreement

Reason for Modification:
ADDENDUM 1
TO PROVIDE ANSWERS TO
VENDOR QUESTIONS

Date Issued	Solicitation Closes	Solicitation No	Version
2025-12-29	2026-01-06 13:30	CRFP 0513 OIG2600000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:
Vendor Name : IBM Corporation
Address :
Street : 300 Summers St. Suite 600
City : Charleston
State : West Virginia **Country :** United States **Zip :** 25301
Principal Contact : Brian Cunningham
Vendor Contact Phone: (304) 552-0032 **Extension:** N/A

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X **FEIN#** 13-0871985 **DATE** 6 January 2026

All offers subject to all terms and conditions contained in this solicitation

300 Summers St., Ste. 600
Charleston, West Virginia 25301

6 January 2026

Crystal Hustead
Senior Buyer
Department of Administration
Purchasing Division
2019 Washington St E.
Charleston, WV 25305

Dear Ms. Hustead,

Thank you for the opportunity to respond to the State of West Virginia's Request for Proposal for the Office of Inspector General's (OIG) Investigations and Fraud Case Management System Solution (CRFP 0513 OIG2600000001).

IBM is a **well-established systems integrator with decades of experience delivering large, complex public sector modernization programs**—projects that require deep domain expertise, disciplined program management, and unwavering commitment to security, transparency, and on time delivery. We have successfully led some of the nation's most significant **digital transformation initiatives**, helping governments modernize operations, improve constituent engagement, and achieve measurable efficiency gains.

As a **Salesforce implementation leader**, IBM brings unparalleled expertise in designing and deploying secure, scalable, and user-friendly solutions. Our approach leverages proven best practices in **Salesforce Public Sector Solutions**, ensuring seamless integration with existing systems while providing a flexible platform that can evolve with West Virginia's future needs.

IBM maintains longstanding relationships with the State of West Virginia, including managing the State's Medicaid data warehouse in partnership with the WV Department of Human Services (DoHS). In that role, it is coordinating with the DoHS and other vendors to help improve outcomes for some of the State's most vulnerable foster children and families, serving as the preferred partner for creating the DoHS artificial intelligence roadmap, and delivering advanced analytics and reporting. These partnerships demonstrate IBM's commitment to West Virginia while validating its capacity to bring the right tools and assets for the job. IBM will deliver this engagement onshore within the United States with help-desk support provided in the state of West Virginia.

Ultimately, IBM represents the **safe, reliable, and experienced** trusted partner capable of delivering a modern investigative case management solution that meets today's needs while preparing the State for tomorrow's growth. We look forward to the opportunity to collaborate with West Virginia to realize this vision and to demonstrate how IBM's experience, innovation, and stability make us the right partner for this important initiative.

Sincerely,

Brian Cunningham
IBM Lead Client Partner
(304) 552-0032
brian.cunningham@ibm.com

Proposal Signature Page

IBM has provided a signed proposal signature form on the following page.

REQUEST FOR PROPOSAL

CRFP OIG2600000001

Case Management System

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

IBM Corporation

(Company)

Brian Cunningham, West Virginia Lead Client Partner

(Representative Name, Title)

(304) 552-0032 / N/A

(Contact Phone/Fax Number)

1/6/26

(Date)

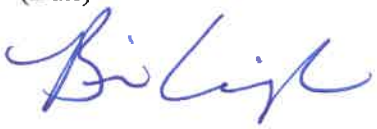


Table of Contents

Executive Summary

The West Virginia Office of Inspector General (OIG), Investigations and Fraud Management Division requires a modern, secure, and scalable platform to support fraud detection, investigation tracking, evidence management, and complete case lifecycle management. As documented in Section 4 of this solicitation, current investigative processes are constrained by fragmented systems, manual workflows, and limited visibility, creating operational inefficiencies and compliance risk as investigative volume and complexity increase.

Current State and Challenges

Today, OIG investigators operate without a single, authoritative system of record. Investigative intake, case activities, evidence, communications, and outcomes are managed across disconnected tools, limiting OIG's ability to consistently track investigations from initiation through closure. Evidence management is particularly challenging, as digital and physical artifacts must be manually tracked to preserve chain of custody and auditability. Leadership lacks real-time insight into investigative workloads, timelines, and fraud trends, making prioritization and oversight difficult. These challenges directly impact OIG's ability to efficiently manage investigations while maintaining strict security and compliance standards

Desired Future State per Section 4 of the RFP

Section 4 calls for a secure, cloud-based case management system that supports:

- Fraud detection and investigation tracking
- Evidence management with lifecycle controls
- End-to-end case lifecycle management
- Secure access controls and auditability
- Ongoing system maintenance, upgrades, and technical assistance

Salesforce Public Sector Solutions Investigative Case Management directly aligns with — and exceeds — these requirements.

Alignment of Salesforce to WV Requirements

Secure, Cloud-Based Platform

WV Requirement: "Implementation of a secure, cloud-based case management system"

Salesforce Investigative Case Management is a FedRAMP-authorized, cloud-native platform designed specifically for public sector investigative and regulatory use cases. Data is encrypted at rest and in transit, with robust identity management, role-based access controls, and detailed audit logging. This ensures sensitive investigative and fraud data is protected while remaining accessible to authorized users across OIG.

Investigation Tracking and Case Lifecycle Management

WV Requirement: "Support fraud detection, investigation tracking, and case lifecycle management"

Salesforce provides a unified case model that tracks investigations from allegation intake through assessment, investigation, resolution, and closure. Configurable workflows guide investigators through each phase, ensuring consistency while allowing flexibility for differing case types. Tasks, milestones, deadlines, outcomes, and investigator assignments are all managed within a single case record, eliminating manual tracking and reducing administrative burden.

Evidence Management and Chain of Custody

WV Requirement: "Evidence management"

Salesforce Investigative Case Management includes purpose-built evidence management capabilities that allow investigators to collect, categorize, link, and secure digital and physical evidence directly to investigative cases. Chain-of-custody is preserved through system-enforced controls, time-stamped activity logs, and role-based permissions. Evidence can be assessed, annotated, and prepared for proceedings while maintaining audit integrity — a critical requirement for OIG investigations.

Fraud Detection and Pattern Analysis

WV Requirement: "Support fraud detection"

Salesforce's data model and analytics capabilities enable OIG to identify patterns, repeat actors, and emerging fraud risks across investigations. Advanced reporting and dashboards provide real-time visibility into case trends, investigator workloads, and fraud indicators. Over time, OIG can leverage automation and AI-assisted insights to improve prioritization and proactively identify high-risk cases.

Reporting, Oversight, and Transparency

WV Requirement: Implied need for oversight, tracking, and reporting across investigations

Salesforce delivers configurable dashboards and reports that provide leadership with real-time insight into investigative performance, backlog, timelines, and outcomes. Audit trails capture every action taken on a case, supporting internal oversight, external audits, and compliance reviews. This transparency strengthens governance and accountability across the investigative function.

Scalability and Long-Term Viability

WV Requirement: Multi-year contract with ongoing maintenance, upgrades, and support

Salesforce's multi-tenant architecture ensures West Virginia OIG automatically receives regular platform upgrades, security enhancements, and new functionality without disruption. The platform scales easily as investigative volume increases or new programs are added, protecting the State's investment and eliminating the need for future system replacements.

Training, Support, and Sustainability

WV Requirement: "In-person and reproducible, web-based training." "system upgrades and maintenance, technical assistance"

Salesforce supports comprehensive training through role-based instruction, reusable learning assets, and ongoing enablement. Combined with structured support services, this ensures

investigators, supervisors, and administrators can effectively adopt and sustain the system long-term.

Why Salesforce for West Virginia OIG

Salesforce Investigative Case Management is not a generic case tracking tool; it is a purpose-built investigative platform proven across public sector agencies with similar oversight, compliance, and fraud investigation mandates. It directly addresses the shortcomings of West Virginia OIG's current environment while delivering a secure, scalable, and future-ready solution aligned with the State's objectives.

By implementing Salesforce, West Virginia OIG gains a single system of record for investigations, stronger evidence governance, improved fraud detection, and enhanced transparency — enabling investigators to focus on outcomes rather than administration, and leadership to manage risk with confidence.

Addenda Acknowledgement

IBM acknowledges receiving Addendum 1. Signed Addenda Acknowledgment form is provided on the following page.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP OIG2600000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

- [x] Addendum No. 1
- [ ] Addendum No. 2
- [ ] Addendum No. 3
- [ ] Addendum No. 4
- [ ] Addendum No. 5
- [ ] Addendum No. 6
- [ ] Addendum No. 7
- [ ] Addendum No. 8
- [ ] Addendum No. 9
- [ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

IBM Corporation
Company

Authorized Signature

11/6/26
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Designated Contact and Certification and Signature Form

IBM has provided a signed designated contact form on the following page.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Brian Cunningham, West Virginia Lead Client Partner

(Address) 300 Summers St., Suite 600; Charleston, WV 25301

(Phone Number) / (Fax Number) (304) 552-0032 / N/A

(email address) brian.cunningham@ibm.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

IBM Corporation
(Company)

(Signature of Authorized Representative)

Brian Cunningham, West Virginia Lead Client Partner
(Printed Name and Title of Authorized Representative) (Date)

(304) 552-0032 / N/A
(Phone Number) (Fax Number)

brian.cunningham@ibm.com
(Email Address)

IBM Response to Goals and Objectives

4.2.1.1 Deploy a cloud-based case management system that fully complies with CJIS Security Policy, FedRAMP High, and HITECH requirements ensuring that both criminal justice information (CJI) and protected health information (PHI) are protected throughout the data lifecycle.

IBM will deploy the solution on **Salesforce Government Cloud Plus**, a **FedRAMP High-authorized** environment that supports CJIS and HITECH-aligned workloads. Salesforce GovCloud meets the encryption, audit logging, access control, and incident response standards outlined in **CJIS Security Policy**, **NIST 800-53 Rev. 5**, and **HIPAA/HITECH**. All data — including **Criminal Justice Information (CJI)** and **Protected Health Information (PHI)** — will remain within the compliant boundary throughout the data lifecycle, from ingestion to archive.

4.2.1.2 Streamline investigative processes through workflow automation, standardized data capture, and analytics-driven reporting to improve productivity and accuracy.

The proposed solution leverages **Salesforce Public Sector Solutions (PSS)** configured to support:

- **Workflow automation** for investigative case intake, review, approval, and closure
- **Standardized data capture** via OmniStudio-guided intake forms and record templates
- **Analytics-driven reporting** using native Salesforce dashboards, configurable reports, and field-level audit tracking

This approach will reduce manual effort, increase investigative throughput, and improve auditability and accuracy.

4.2.1.3 Supports seamless and stable, simultaneous access for multiple users to all areas, including the same case, ensuring no performance degradation.

Salesforce's multitenant architecture ensures **real-time, simultaneous access for multiple users**, including concurrent editing/viewing of the same investigative case without performance degradation. The system is horizontally scalable and supports performance SLAs aligned to large-scale government deployments.

4.2.1.4 Ensure the system integrates securely with state information technology infrastructure, law-enforcement databases, and healthcare data systems while maintaining scalability to support future growth for possible additions of other departments and evolving compliance requirements.

The solution will integrate with state IT infrastructure and external systems via:

- Named Credentials and External Services for secure API-based integration
- Azure AD/Entra ID for SSO, aligned to state identity standards
- Scalable architecture supporting future departmental expansion and evolving compliance (e.g., 508, WCAG, additional data domains)

The system is built to scale horizontally with minimal technical rework.

4.2.1.5 Demonstratable and verifiable experience implementing at least three (3) information cloud-based systems within the past five (5) years. Documentation should include:

- System description, name, purpose, and core function.
- References from the contracting agency, including contact name, title, phone number, and email address, capable of verifying the implementation and compliance status.

- Scope of implementation, size, user base, modules, and complexity.
- Operating environment, hosting model, and security posture.

New Mexico Regulation and Licensing Department

The project seeks to strengthen the Securities Division's ability to regulate effectively by improving efficiency, accuracy, and transparency across all core functions. By automating manual processes, consolidating workflows, and integrating with national securities systems, the Division will reduce administrative burdens and minimize errors.

The initiative also aims to provide leadership and staff with better insight into operations through modern reporting and dashboards, supporting data-driven decision-making. Ultimately, the goal is to deliver a sustainable platform that enhances compliance, improves service delivery, and positions the Division for long-term operational success.

The project is a comprehensive modernization of the New Mexico Regulation and Licensing Department's Securities Division, delivered within the agency's Salesforce environment. It replaces aging legacy systems with a secure, scalable platform that supports the Division's core functions, including securities registrations, examinations, filings, and financial processing. The work also encompasses data migration, workflow automation, and advanced reporting to provide greater visibility into regulatory activities. A major focus is the integration with industry-specific systems such as Blue Express and CRD, creating a unified interface that reduces manual effort and significantly improves staff efficiency in managing compliance and oversight responsibilities

Project governance has been established with a structured PMBOK-aligned framework, and discovery and design activities have been completed with stakeholder validation. Core Salesforce configuration is underway, with initial securities workflows built and prepared for testing. Data migration mapping from legacy systems has been finalized, and development of integrations with Blue Express and CRD is in progress. Reporting and dashboard prototypes have been created and reviewed with business users, and training and adoption planning are embedded into the delivery schedule. The project remains on track against milestones and budget

Contracting Agency Reference

Agency Name: New Mexico Regulation and Licensing Department
Contact Person: Juan Torres
Title: Chief Information Officer
Phone Number: (505) 538-0115
Email Address: juan.torres@rld.nm.gov

Utah Department of Health and Human Services

The Department of Health and Human Services (DHHS) needed greater insight and control over the Medical Cannabis industry. The existing systems did not provide the insights or access needed. DHHS also wanted to hand back control of CRM to the stakeholders/licensees.

The State of Utah restricts cannabis use to medical purposes only. DHHS and the Department of Agriculture and Food (UDAF) are jointly responsible for managing the State's rapidly growing medical cannabis industry. DHHS and UDAF recognized a need to modernize and improve the State's Medical Cannabis eligibility and inventory tracking processes as well. Having experienced success with Salesforce Public Sector Solution, they also chose to migrate the

existing electronic verification system (EVS) and inventory control system (ICS) to the Salesforce platform.

IBM was selected to implement the new EVS and ICS system due to our proven track record of delivery success for UDAF and other Utah state agencies as well as our prior experience with inventory tracking and accounting related to the cultivation of cannabis. Our vision for the EVS and ICS hub includes an architectural standards-based approach centered around APIs that can unlock monolithic legacy systems where core data and services are siloed. This enables information to be available anytime, anywhere by facilitating statewide and intergovernmental information sharing in a secure, reliable, innovative, and cost-effective platform. State employees can react faster than ever, supported by a complete view of the data, real-time collaboration tools, and recommended actions from seed to sale.

The EVS system features:

- A secure online application system to allow individuals to apply for and renew a medical cannabis card/registration.
- Integration with GovPay, the State of Utah's online payment system.
- Access for state or local law enforcement to determine if an individual subject to a law enforcement encounter has a valid medical cannabis card.
- Connects with the inventory control system to verify cardholder status, patient purchase limits and track in real time and archive purchases of any cannabis in a medicinal dosage form, cannabis product in a medicinal dosage form, or a medical cannabis device, including:
  - Time and date of each purchase
  - Quantity and type of cannabis, cannabis product, or medical cannabis device purchased
  - Cannabis production establishment, any medical cannabis pharmacy, or any medical cannabis courier associated with the cannabis, cannabis product, or medical cannabis device
  - Personally identifiable information of the medical cannabis card holder who made the purchase

Contracting Agency Reference

Agency Name: Utah Department of Health & Human Services (DHHS)
Contact Person: Rich Oborn
Title: Bureau Manager
Phone Number: (801) 530-6767
Email Address: roborn@utah.gov

Massachusetts Department of Telecommunications and Cable (DTC)

The Department of Telecommunications and Cable (DTC) oversees the telecommunications and cable industries in Massachusetts, ensuring that residents receive high-quality communication services at reasonable rates. DTC was seeking to modernize its intake processes and data management systems for ease of submission, increased data utilization, improved efficiency, and more effective cross-division collaboration.

The client's document management solution was paper-based and disconnected, which accrued significant cost within the business. DTC sought a digital transformation partner that could review its existing business processes and provide an effective path to overcome these challenges related to document management.

IBM's history of successful modernization within State and Local Government made it the ideal partner. DTC has streamlined the internal processes related to the management of application submissions and has drastically improved efficiencies. The solution is used by MassDTC staff to review and approve or deny applications for State Business Offices (SBO), Tariff Filing, and Form 500s submitted by Telecom and Cable providers. It is also being leveraged to approve and deny newly created business user accounts.

Other benefits include:

- 100% elimination of paper process
- A fully supported online form intake process
- The addition of a public portal

DTC benefitted from IBM's successful Salesforce DMS implementation, replacing outdated processes with a modern solution increasing productivity, improving online submissions, and enabling efficiencies.

Contracting Agency Reference

Agency Name: Massachusetts Department of Telecommunications & Cable (DTC)
Contact Person: Kathleen Morrissey
Title: Program Coordinator – Business Solutions
Phone Number: (857) 289-5800
Email Address: kathleen.morrissey@mass.gov

4.2.1.6 The vendor should assign personnel with professional certifications and expertise appropriate for this project. The agency is seeking a vendor that will meet these requirements, vendors should detail how they will meet each of the following areas:

- A Project Manager who holds a current Project Management Professional (PMP) or equivalent certification.
- An Information Security Lead who holds an active Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or equivalent credential, and who has verifiable experience designing and maintaining environments compliant with NIST SP 800-53 Rev. 5 controls and CJIS Security Policy requirements.
- Qualified System Architects and Cloud Engineers with experience configuring, deploying, and supporting FedRAMP-authorized cloud environments (AWS GovCloud, Azure Government, or equivalent).
- Experienced Training Specialists or Organizational Change Managers who have developed and delivered end-user and administrator training for prior government technology implementations.
- Copies of active certification credentials shall be provided upon request by the Agency.

IBM is committed to providing WV OIG with highly credentialed professionals who possess the certifications and specialized expertise required for this critical case management implementation. Our team members maintain current industry certifications and bring demonstrated experience in public sector technology implementations, cloud security, and FedRAMP-authorized environments. This section details how our proposed team meets each of the Agency's certification and expertise requirements.

Colleen McGarry, our designated Project Manager for this engagement, holds an active Project Management Professional (PMP) certification issued by the Project Management Institute (PMI). Colleen brings 20 years of consulting experience directing large, complex engagements and has successfully managed Salesforce implementations. She holds multiple

Salesforce certifications including Certified Administrator, Certified Service Cloud Consultant, Certified Sales Cloud Consultant, Certified Experience Cloud Consultant, and Certified Platform App Builder, providing her with unique business and technology translation skills essential for complex cloud implementations.

Colleen has led multiple high-profile Salesforce projects including CRM transformations, organizational consolidations, and Einstein Analytics implementations. She has successfully managed geographically dispersed teams of 20+ resources across multiple countries and time zones and is well-versed in projects requiring integration and data migration. Ms. McGarry holds an MBA from the University of Chicago and a Bachelor of Science from the University of Illinois Champaign/Urbana, positioning her to navigate the unique requirements of public sector projects while ensuring on-time, on-budget delivery.

Brenden Glynn, **our Information Security Lead,** holds an active Certified Information Systems Security Professional (CISSP) certification issued by (ISC)², along with GIAC Certified Incident Handler (GCIH) and CompTIA Advanced Security Practitioner (CASP) certifications. Brenden brings 20 years of cybersecurity experience and verifiable expertise in designing and maintaining environments compliant with NIST SP 800-53 Rev. 5 controls and CJIS Security Policy requirements through his extensive military and government contracting background. As a Major and Cyber Warfare Officer in the U.S. Army Reserves since 2004, he has been responsible for developing mission defense plans, cyber threat intelligence, and risk mitigation strategies for National Mission Forces and Combatant Command Mission Forces.

Brendon facilitates executive-level cyber crisis simulations and leads incident response content development for IBM Security SOAR and QRadar solutions. He has conducted over 400 training sessions and workshops globally, advising Fortune 500 companies and government entities on crisis management, incident response, and defensive cyber operations. During his tenure with General Dynamics Information Technology supporting a multimillion-dollar government contract (2010-2016), he served as Lead Engineer providing technical oversight for boundary security technologies and worked directly with IT Assurance teams to validate security controls for production infrastructures handling sensitive classified information.

Siddarth Sinha, our Salesforce Solution Architect, possesses 18 active Salesforce certifications demonstrating comprehensive platform expertise across architecture, development, integration, and deployment disciplines. His certifications include Salesforce Certified System Architect, Certified Application Architect, Certified Integration Architect, Certified Identity and Access Management Architect, Certified Development Lifecycle and Deployment Architect, Certified Data Architect, and Certified Sharing and Visibility Architect. Siddharth brings 16 years of experience in the Salesforce ecosystem, having engaged in over 40 implementations for Fortune 500 companies across diverse industries including public sector, healthcare, travel and transportation, telecommunications, and energy and utilities.

His public sector experience includes serving as Salesforce Technical Architect for the State of Florida's Vaccine Management program, where he designed a community-based application allowing users to self-register and book appointments while ensuring HIPAA-compliant data encryption and secure transportation of personally identifiable information. Mr. Sinha has extensive experience with identity management and single sign-on (SSO) implementations using Azure, PingID, and Okta, and has designed system integrations using SAML, OAuth, OpenID Connect with Active Directory and LDAP—critical security protocols for government environments. As Enterprise Architect at IBM (March 2018-Present), he has served as a trusted advisor on end-to-end enterprise architecture decisions and has successfully designed and delivered complex implementations involving Sales Cloud, Service Cloud, Experience Cloud, and Einstein AI capabilities. He holds an MBA in Information Technology from Western Governors University and a Bachelor of Technology in Information Technology.

Tracy Kirschen, our Change Management Lead, is a Senior Managing Consultant in Organization Change Strategy at IBM with over 15 years of experience specializing in large-scale transformation programs. Tracy holds a Master of Arts in Organizational Psychology with a concentration in Organization Change and Consultation from Columbia University Teachers College and has led change management programs on numerous enterprise technology implementations including SAP S/4HANA, SAP Analytics Cloud, and Salesforce projects. Her expertise includes developing and executing organizational change management and training strategies, conducting stakeholder impact assessments, creating Change Agent and Super User networks, establishing training curriculum design and Train-the-Trainer programs, and measuring adoption success through business readiness scorecards and post-implementation support models.

Tracy's experience includes serving as OCM Lead for multiple global transformation projects where she has developed change management strategies for tens of thousands of end-users across diverse functions including Finance, Supply Chain, Procurement, and HR. She has successfully established Change Networks comprised of Change Champions (senior influential leaders) and Super User Networks to provide first-line support, and has designed and executed Train-the-Trainer workshops for global client trainers. Her approach emphasizes leadership alignment and engagement, stakeholder management, communications planning, and driving adoption through structured readiness programs—critical capabilities for ensuring WV OIG personnel successfully transition to the new Salesforce Case Management system. Tracy's experience managing change in large, complex organizational environments positions her to address the unique dynamics of public sector technology adoption.

Certification Documentation

IBM will provide copies of all active certification credentials for the personnel named above upon request by WV OIG. All certifications are current and in good standing.

These credentials, combined with our team's demonstrated experience in public sector implementations, cybersecurity compliance, and case management systems, position IBM to successfully deliver this critical project for WV OIG. Our certified professionals bring both technical expertise and practical understanding of government operational requirements, ensuring a solution that meets security standards while supporting investigative mission objectives.

IBM Response to Mandatory Project Requirements

FBI CJIS Security Policy Compliance

4.2.2.1 The proposed solution must comply with the FBI CJIS Security Policy which can be found at https://www.fbi.gov/file-repository/cjis/cjis_security_policy_v5-9_20200601.pdf/view

The proposed Salesforce-based solution, deployed via **Government Cloud Plus (GovCloud Plus)**, aligns fully with the **FBI CJIS Security Policy v5.9**. IBM and Salesforce jointly ensure adherence to all relevant CJIS controls, as described below.

4.2.2.1.1 Encrypt all data at rest and in transit using Federal Information Processing Standards (FIPS) 140-3 validated encryption modules.

- All data is encrypted at rest and in transit using FIPS 140-2 validated cryptographic modules, with transition to FIPS 140-3 underway in accordance with NIST timelines.
- Salesforce Government Cloud uses TLS 1.2+ for all in-transit data and AES-256 encryption for data at rest.

CJIS Sections 5.10.1.2 and 5.10.1.3 are fully met.

4.2.2.1.2 Provide multi-factor authentication (MFA) for all users accessing the solution.

- The system enforces **MFA for all users**, including internal users, administrators, and external integrations.
- Authentication is managed via **Salesforce MFA or external identity providers** (e.g., Azure AD) configured with **SAML 2.0** or **OAuth 2.0** and MFA policies.

CJIS Section 5.6.2.2.1 is met.

4.2.2.1.3 Maintain comprehensive and immutable audit trails for all system access, modifications, and deletions, with the ability to generate audit logs for the Agency upon demand.

- The solution maintains **comprehensive and immutable audit logs** for user access, data changes, and system actions.
- Audit logs include timestamp, user ID, event type, and object affected.
- Authorized administrators can **generate audit reports on demand**, and logs can be **exported for CJIS compliance reviews**.

CJIS Sections 5.4 and 5.6.2.1.1.2 are met.

4.2.2.1.4 Ensure that all vendor personnel, subcontractors, or third parties with access to the system have completed CJIS Security Awareness Training and signed the CJIS Security Addendum.

- All IBM personnel, subcontractors, and delivery partners who may access the system or environments will:
  - Complete CJIS Security Awareness Training
  - Sign the CJIS Security Addendum
- Training records and signed addenda are retained per CJIS retention requirements and made available to the Agency upon request.

CJIS Sections 5.2.1 and Appendix H are met.

4.2.2.1.5 Maintenance of a documented incident response plan consistent with CJIS Security Policy Section 5.10, including breach notification within one hour of discovery.

- IBM maintains a documented **CJIS-aligned Incident Response Plan (IRP)** and follows NIST 800-61 guidelines.
- In the event of a confirmed or suspected breach, IBM will notify the Agency **within one hour of discovery**, per **CJIS Section 5.10.1.1**.
- The IRP includes defined roles, escalation paths, containment steps, and post-incident review procedures.

CJIS Section 5.10 is fully addressed.

FedRAMP Compliant Hosting

4.2.2.2 The system's hosting environment must hold an active FedRAMP High Authorization to Operate (ATO) issued by either the federal Joint Authorization Board (JAB) or a federal agency.

The proposed solution will be deployed on **Salesforce Government Cloud Plus**, which holds an active **FedRAMP High Authorization to Operate (ATO)** issued by the **Joint Authorization Board (JAB)**. IBM will implement, monitor, and support the application within this FedRAMP-authorized boundary.

4.2.2.2.1 Proof of an active Authorization to Operate (ATO) at the High level issued by a federal agency or the Joint Authorization Board (JAB).

- Salesforce Government Cloud Plus holds an active **FedRAMP High ATO** granted by the **JAB**, with listing available on the official FedRAMP Marketplace:
  - https://marketplace.fedramp.gov
- Documentation of the ATO letter will be provided upon request or during the award phase.

4.2.2.2.2 The vendor must provide documentation outlining the security assessment completed by the Third-Party Assessment Organization.

- Salesforce undergoes a full annual FedRAMP security assessment by an approved Third-Party Assessment Organization (3PAO).
- IBM will provide the latest Security Assessment Report (SAR) summary, which includes:
  - Controls testing results (NIST 800-53 Rev. 5)
  - System boundary definition
  - Remediation actions (if applicable)

4.2.2.2.3 The vendor must provide documentation of continuous monitoring, including vulnerability scanning, patch management, incident response, and reporting practices prior to award.

- Salesforce Government Cloud Plus supports FedRAMP-mandated **continuous monitoring**, including:
  - Weekly vulnerability scanning
  - Ongoing patch management
  - Documented incident response procedures
  - Monthly and quarterly compliance checks
- IBM supplements this with its own monitoring and escalation procedures tailored to the WV OIG implementation.

4.2.2.2.4 The vendor must provide quarterly reports demonstrating ongoing compliance with FedRAMP requirements.

- IBM will submit **quarterly compliance reports** summarizing:
- FedRAMP scan results
- Security patch status
- Open vulnerabilities (if any)
- Incident activity (if any)
- Any changes affecting authorization boundary
- These reports are based on the Salesforce continuous monitoring outputs and IBM's operational support data.

HITECH Compliance

4.2.2.3 The system must comply fully with HITECH and all applicable provisions of Health Insurance Portability and Accountability (HIPAA). The vendor must describe their approach on how they will comply with the following areas:

IBM will implement and operate the solution using security and privacy-by-design controls to support full compliance with **HITECH** and the applicable **HIPAA Security Rule and Privacy Rule** requirements. The approach assumes WV OIG may store or process **PHI** within investigative case records and ensures safeguards are enforced throughout the PHI lifecycle (collection, access, use, disclosure, retention, and disposal).

4.2.2.3.1 Current implementation of all required Administrative, Physical, and Technical Safeguards as described in 45 CFR §§164.308–316.

IBM will implement a HIPAA-aligned control framework covering:

- **Administrative safeguards:** documented policies and procedures; security risk assessment and risk management; workforce security; access authorization and termination; security awareness and training; contingency planning; vendor management.
- **Physical safeguards:** controlled access to facilities and workstations used by support personnel; device and media controls; secure handling of any exported data.
- **Technical safeguards:** unique user identification, role-based access control, MFA/SSO, encryption in transit and at rest, automatic session timeouts, audit logging, and integrity controls.

Safeguards will be documented and validated as part of implementation security design and operational readiness.

4.2.2.3.2 Breach-notification procedures consistent with HITECH Section 13402 and 45 CFR Part 164, Subpart D.

IBM will maintain and execute breach-notification procedures consistent with HIPAA/HITECH, including:

- Formal incident triage to determine whether an event constitutes a reportable breach of unsecured PHI.
- Defined escalation and notification procedures, including timelines and required content for notifications.
- Coordination with WV OIG to support required notifications to affected individuals, HHS, and other parties as applicable.

IBM's incident response runbooks will include PHI-specific handling, evidence preservation, and post-incident corrective actions.

4.2.2.3.3 Vendor must complete the WV Business Associate Agreement (BAA) provided as Attachment C and include in their proposal; the BAA must be provided prior to contract award.

IBM will complete and return the **WV Business Associate Agreement (BAA)** provided in Attachment C and include it in the proposal package, with execution prior to award as required. Where subcontractors or hosting providers may have access to PHI (as applicable), IBM will ensure appropriate downstream contractual protections are in place consistent with HIPAA business associate obligations.

4.2.2.3.4 Access control, encryption, and audit mechanisms for all Protected Health Information (PHI) processed by the system.

The solution will enforce PHI protections through:

- **Access controls:** least-privilege role-based access, case-level restrictions, and segregation of duties for investigators, supervisors, and administrators.
- **Encryption:** encryption for data in transit and at rest within the authorized hosting boundary; secure API authentication for any approved integrations.
- **Audit mechanisms:** detailed audit trails for user access and record activity (view, create, update, export, delete where permitted), supporting both internal oversight and external audit requests.

Controls will be configured to ensure PHI is only accessible to authorized users with a valid business need.

4.2.2.3.5 Ensure all vendor personnel with access to PHI complete annual HIPAA/HITECH training.

IBM will require annual HIPAA/HITECH training for all personnel with access to PHI, including workforce members supporting administration, configuration, integrations, and incident response. IBM will maintain training completion records and provide documentation to WV OIG upon request in accordance with contract requirements.

RBAC Security Architecture

4.2.2.4 The system must include a comprehensive security architecture that enforces Role-Based Access Control (RBAC) based on least privilege principles. The agency is seeking a solution that will meet necessary security requirements, vendors must detail how their solution will meet each of the following areas:

IBM will implement a comprehensive Role-Based Access Control (RBAC) security architecture on Salesforce Public Sector Solutions that enforces **least privilege**, supports CJIS/FedRAMP High/HITECH-aligned controls, and enables WV OIG administrators to manage access and configuration without vendor dependency. The security model will use standard Salesforce capabilities (profiles, permission sets, permission set groups, roles, sharing rules, restriction rules, session policies, and auditing) and will be validated through security testing and administrative procedures.

4.2.2.4.1 RBAC: Access must be restricted to only those functions and data necessary for the user's role.

Access is restricted by role using a layered approach:

- **Profiles** establish baseline access (minimum permissions by job function).

- **Permission Sets / Permission Set Groups** provide additive entitlements for specific duties (e.g., evidence handling, approvals, reporting).
- **Roles and Sharing** enforce record-level access (e.g., investigator/team/division visibility).
- **Restriction Rules** (where applicable) provide additional constraints to prevent overexposure of sensitive records.

This model ensures users can only access the data and actions required for their assigned responsibilities.

4.2.2.4.2 Implementation of multi-factor authentication and session timeout controls

The solution will enforce:

- **Multi-factor authentication (MFA)** for all interactive users, integrated with WV's identity standard (Azure AD/Entra ID) or Salesforce MFA as required.
- **Session timeout and reauthentication** using Salesforce session settings and conditional access policies to reduce risk of unauthorized access from unattended sessions.

4.2.2.4.3 Secure Remote Access: Including encryption, and protection of data accessed from outside the state network.

Remote access is protected through:

- **Encrypted communications (TLS 1.2+)** for all user sessions and API traffic.
- Identity-based controls (SSO/MFA) and device/network posture policies where the State applies conditional access.
- Role-based restrictions that limit what remote users can view/export based on assigned privileges, supporting secure access outside the state network.

4.2.2.4.4 Deployment of Security Information and Event Management (SIEM) tools to monitor system activity and detect anomalies.

The solution supports integration with WV's SIEM through:

- Exportable event and access logs (including login events and administrative actions).
- Standard log forwarding patterns and operational procedures to support centralized monitoring and anomaly detection.

If WV uses a specific SIEM (e.g., Splunk, Microsoft Sentinel), IBM will align log formats and collection methods to agency standards.

4.2.2.4.5 Integration with Data Loss Prevention (DLP) and Intrusion Detection and Prevention Systems (IDPS).

IBM will enable compatibility with WV's enterprise security stack by:

- Supporting secure browser and network access patterns consistent with agency-managed **DLP** and **IDPS** controls.
- Configuring export and file-handling permissions to reduce unauthorized data movement.
- Supporting monitoring and enforcement via existing state tooling (e.g., endpoint DLP, network IDPS), and integrating relevant Salesforce events/logs into those systems where feasible.

4.2.2.4.6 Agency administrators must be able to assign, monitor, and revoke user roles immediately.

WV OIG administrators can immediately:

- Assign or revoke roles and access using permission sets/groups and role assignments.
- Disable users, reset sessions, and enforce reauthentication.
- Apply standardized access packages for investigators, supervisors, administrators, and read-only stakeholders to ensure rapid onboarding/offboarding and least-privilege control.

4.2.2.4.7 System must allow administrator(s) full control of administrative tables without vendor assistance, including but not limited to edit all fields, labels, data types, validation rules, drop down and picklist content and alerts.

The solution is designed to be **administrator-operable** using declarative tools. WV OIG admins will have full control to manage configuration elements such as:

- Fields, page layouts, validation rules, picklists, labels, notifications, and workflow rules/flows
- Configuration tables and reference data (e.g., case types, statuses, routing values)

IBM will provide admin training and documentation to ensure WV OIG can safely maintain and update the system within governance procedures.

4.2.2.4.8 Logging and notification of all administrative and configuration changes.

The system will log administrative and configuration changes using Salesforce auditing capabilities (e.g., setup audit trail and related security logs). IBM will also configure notifications/workflows where appropriate so that WV OIG security and admin leadership can be alerted to significant configuration changes based on agency policy.

Full-Case Lifecycle Management

4.2.2.5 The solution must provide full-case lifecycle management capabilities, including case intake, triage, assignment, investigation, evidence management, and closure. The agency is seeking a solution that will meet these requirements, vendors must detail how their solution will meet each of the following areas:

The proposed Salesforce Public Sector Solution, implemented by IBM, supports end-to-end case lifecycle management — including intake, triage, assignment, investigation, approvals, evidence handling, and closure. The platform is fully configurable to support role-based workflows, auditability, and investigative rigor.

4.2.2.5.1 The ability to log complaints, referrals, or leads and route them for review.

The system enables logging of complaints, referrals, or tips through configurable intake forms. Submissions can be manually routed or automatically queued for review based on predefined criteria such as case type, severity, or source.

4.2.2.5.2 Support automated or manual assignment of a unique case identifier upon creation of a new record.

Each new case record is automatically assigned a system-generated unique case identifier, which can be formatted to include agency-specific prefixes, time-stamps, or classification codes. Each new case record is automatically assigned a system-generated unique case identifier, which can be formatted to include agency-specific prefixes, time-stamps, or classification codes.

4.2.2.5.3 Support ad hoc workflows that allow the ability to generate custom, on demand reports and/or memos that aren't covered by regular, predefined report and automatic generation of related tasks.

Users may initiate ad hoc workflows, generate memos or investigative reports, and assign related tasks directly from the case interface. This allows for flexible response to dynamic investigative needs outside predefined process paths.

4.2.2.5.4 The ability for all users to enter case notes to document case activity.

All users with appropriate permissions can enter timestamped case notes that are securely stored and linked to the case record. These notes are versioned and auditable to maintain chain-of-events clarity.

4.2.2.5.5 Assign cases to investigators, monitoring status, and ensuring accountability.

Supervisors can assign or reassign cases to investigators. The system supports workload balancing, SLA tracking, and real-time visibility into case status, ensuring accountability and timely follow-up.

4.2.2.5.6 Allow user defined items requiring higher-level approval such as case status changes, or investigator generated report or memo approvals.

The platform supports configurable approval workflows for investigator-generated memos, case status changes, and other user-defined actions. Approvals can be triggered based on case type, role hierarchy, or content category.

4.2.2.5.7 Secure storage and management of documents, images, videos, and other evidence, with full chain-of-custody tracking.

Documents, photos, videos, and other evidentiary files are securely uploaded to the case record with full metadata. The system logs all access, edits, and transfers to support complete chain-of-custody tracking.

4.2.2.5.8 Tools to manage subpoenas, subjects, and witnesses within a case record.

Dedicated record structures allow users to track subpoenas issued or received, subjects of investigation, and witnesses. These are linked to the parent case and can include interview notes, contact logs, and supporting documentation.

4.2.2.5.9 Advanced search across structured and unstructured data, and secure export of case records in auditable formats.

The system includes advanced global and contextual search capabilities across structured data (fields) and unstructured data (notes, attachments). Authorized users can securely export case data and documents in audit-ready formats (e.g., PDF, CSV).

4.2.2.5.10 Allow administrator(s) to control file management and data retention.

Administrators can define file access rules, configure document retention policies, and enforce deletion controls based on legal and regulatory requirements. These controls ensure compliance with WV OIG and state/federal retention standards.

Audit, Reporting and Analytic Capabilities

4.2.2.6 The solution must provide audit, reporting, and analytic capabilities to support investigative oversight, compliance, and management decision-making. The agency is seeking a solution that will meet these requirements, vendors must detail how their solution will meet each of the following areas:

The proposed solution leverages Salesforce's native analytics (Reports & Dashboards), auditability, and automation features—configured by IBM to support investigative oversight,

performance tracking, and regulatory reporting for WV OIG. Features are tailored to support both frontline investigators and agency leadership.

4.2.2.6.1 Provide configurable dashboards tailored to user roles (e.g., investigators, supervisors, administrators) that display case status, workload distribution, and investigative outcomes.

The solution includes configurable, real-time dashboards tailored to specific user roles:

- **Investigators** view caseloads, deadlines, and status indicators.
- **Supervisors** monitor team assignments, case progress, and workload distribution.
- **Administrators** track system performance, compliance exceptions, and operational metrics.

Dashboards are built using Salesforce's native tools and can be customized without code.

4.2.2.6.2 Provide alerts to users as new tasks and case assignments are made.

The system generates automated, real-time alerts and notifications when:

- New cases or tasks are assigned
- Deadlines are approaching or missed
- Case statuses change

Notifications can be delivered in-platform, via email, or SMS based on user preferences and agency policies.

4.2.2.6.3 Track caseloads and assignments by investigator, team, or division, including timelines, task status, and completion rates.

Supervisors can track:

- Caseload volume by investigator, team, or division
- Task completion timelines, bottlenecks, and SLA compliance
- Case reassignment and aging trends

These insights support workforce balancing and timely escalation when necessary.

4.2.2.6.4 Generate standardized reports required by federal and state regulations, including fraud statistics, investigative results, and audit-ready documentation.

A library of standard reports will be configured to support:

- Federal and state fraud tracking
- Investigative outcomes and audit trails
- Monthly, quarterly, and annual compliance reporting

Reports are exportable in PDF, Excel, and CSV, and can be scheduled or run on demand.

4.2.2.6.5 Maintain permanent, tamper-evident logs of all system access, modifications, and transactions, which can be exported for internal and external audits.

Salesforce's platform includes built-in audit logging features to:

- Track all user access, record changes, and system actions
- Maintain tamper-evident audit trails required by CJIS and FedRAMP
- Support forensic investigations and internal/external audits

Logs are securely stored and exportable upon request.

4.2.2.6.6 Provide automated tools to generate structured or narrative memoranda of investigation, summaries, or briefing documents by drawing from multiple data points within a

case file (e.g., subject information, witness interviews, evidence entries, financial records, and investigative notes). The system must allow customization of memo templates to align with Agency investigative standards and ensure that generated documents are properly formatted, exportable, and securely stored within the case file.

The system allows users to generate:

- Structured Memoranda of Investigation (MOIs)
- Case summaries, briefings, and closure documents
- Outputs drawing from structured and unstructured case data (e.g., evidence, interviews, financials)

Templates are fully customizable to WV OIG formats and securely stored in the case record. Finalized documents can be exported in secure, standardized formats such as PDF or Word.

Document Management

4.2.2.7 The system must support the storage, viewing, import, export, and generation of documents in common government-accepted formats such as Microsoft Office and Google Workspace to ensure compatibility, accessibility, and ease of sharing with internal and external stakeholders. The agency is seeking a solution that will meet these requirements, vendors must detail how their solution will meet each of the following areas:

IBM will implement Salesforce Public Sector Solutions (PSS) document capabilities using **Salesforce Files** and case-related document relationships to support secure evidence and case documentation management. The solution supports common government file formats, secure storage and retrieval, metadata capture, auditability, and controlled export consistent with CJIS and FedRAMP High hosting requirements.

4.2.2.7.1 Support upload, storage, search, and retrieval of documents in PDF, Microsoft Word (.docx), Excel (.xlsx), PowerPoint (.pptx), text (.txt), image (.jpg/.png/.tiff), and audio/video (.mp3/.mp4/.wav) formats.

The system supports upload and storage of standard file formats, including **PDF, DOCX, XLSX, PPTX, TXT, JPG/PNG/TIFF, and MP3/MP4/WAV**, and associates them to the appropriate case record (and related records such as subjects, evidence, or subpoenas). Files are searchable and retrievable via case context, global search, and configured filters (e.g., category, date, uploader, case ID).

4.2.2.7.2 Allow documents to be thumbnail/first page previewed. Files that contain images, and/or audio must be opened and are not subject to preview.

Salesforce provides file preview functionality for supported previewable document types (e.g., PDFs and many Office formats), including **thumbnail and first-page/inline preview** within the case context. For files that do not support preview (e.g., certain media formats), users can securely download/open them subject to permissions, consistent with the requirement that images/audio may require opening rather than preview.

4.2.2.7.3 Allow export of reports, memos, and case summaries in both PDF (.pdf) and Microsoft Word (.docx) formats.

The solution supports exporting reports and case summaries to **PDF** using native report export capabilities and configurable print views. For **DOCX-formatted outputs** (e.g., memoranda of investigation), IBM will implement standardized document templates and generation approaches aligned to agency standards (either via Salesforce-native document template mechanisms or an approved document generation approach if DOCX output is mandated for official memoranda).

4.2.2.7.4 Incorporate spell check, cut and paste, and other routine word processor functions throughout narrative fields.

Narrative fields in Salesforce support standard browser-based editing behaviors, including **cut/paste, undo/redo, and basic formatting** as configured. Spell check is supported through **browser spell check** and can be enabled by agency standard workstation configuration. This applies across narrative fields such as notes, summaries, and memo content fields.

4.2.2.7.5 Maintain original file metadata (author, date, source) and preserve chain of-custody for all documents uploaded or generated within the system.

The system maintains file metadata (e.g., filename, upload timestamp, uploader identity, version history) and links files to the case record. Chain-of-custody is supported through **role-based access controls**, **file versioning**, and **audit logging** of access and changes where enabled. IBM will configure evidence categorization fields and controlled workflows to support evidentiary handling and disclosure processes.

4.2.2.7.6 Ensure that all files are encrypted at rest and in transit in accordance with CJIS and FedRAMP High standards.

Files are encrypted **in transit** using **TLS 1.2+** and encrypted **at rest** within the FedRAMP High authorized hosting boundary. Encryption controls align to CJIS and FedRAMP High requirements for protecting case documentation and evidence throughout the lifecycle.

4.2.2.7.7 Permit secure bulk download or export of case documentation for lawful disclosure, audit, or prosecution purposes with appropriate access controls.

Authorized users can perform controlled export of case documentation (including reports and associated files) using role-based permissions and audit controls. Bulk export can be executed for lawful disclosure or audit purposes with administrative governance (e.g., export authorization, case-level access restrictions, and audit logging). IBM will configure export procedures and access policies aligned to WV OIG operational and legal requirements.

Integration

4.2.2.8 The solution must provide secure integration capabilities with state and federal systems as applicable. The agency is seeking a solution that will meet these requirements, vendors must detail how their solution will meet each of the following areas:

- Medicaid Management Information System (MMIS).
- State financial and payment systems.
- Google applications (e.g. Gmail, Docs, etc.)
- Law enforcement databases (e.g. NCIC, Nlets), as applicable.

IBM's solution uses Salesforce's standards-based integration framework to securely connect to state and federal systems **as applicable** and based on WV OIG's authorized endpoints, data-sharing agreements, and CJIS/FedRAMP boundary requirements. Integrations are implemented using **Named Credentials**, **OAuth 2.0/SAML**, **TLS 1.2+**, and API-led patterns (with middleware used only when required for protocol transformation, routing, or CJIS boundary controls).

- **MMIS / Medicaid systems:** Supported via secure API integration (REST/SOAP) through state-approved endpoints. If MMIS exposes HL7/FHIR interfaces, IBM will support those via an integration layer (middleware) to ensure protocol compliance and governance.
- **State financial and payment systems:** Supported via secure service integrations for payment status, vendor/payee lookups, or transaction references, using state-approved APIs and audit logging for all data exchanges.

- **Google applications (Gmail/Docs):** Supported through controlled integration patterns only where WV OIG authorizes Google Workspace use for relevant data. Integration options include secure email relay and API-based document linkage/metadata capture, subject to agency security policy and FedRAMP/CJIS constraints.
- **Law enforcement databases (NCIC/Nlets):** Supported **when applicable** and only through CJIS-compliant, state-approved access methods (typically brokered via law-enforcement gateways, rather than direct application connections). IBM will integrate using the access pattern and interface approach approved by WV OIG and the responsible CJIS Systems Agency (CSA).

Assumption for estimation/scope: Initial delivery includes **SSO with Azure AD/Entra ID** and **up to two (2) additional integrations**; other integrations listed above are supported by the architecture and can be implemented as future phases based on authorization and priority.

Data Exchange Protocol

4.2.2.9 The solution must support industry-standard data exchange protocols (e.g., HL7, FHIR, XML, or RESTful APIs) and allow secure import and export of data without compromising compliance requirements.

The solution supports industry-standard data exchange protocols through Salesforce APIs and integration patterns:

- **RESTful APIs** (standard), **SOAP** (as needed), and **XML/JSON payloads** are supported natively for secure import/export and system-to-system exchanges.
- **HL7/FHIR** can be supported when required through an integration layer capable of FHIR resource handling and transformation, with security controls maintained within the FedRAMP High boundary.

All data exchange is secured using strong authentication (OAuth/SAML), encryption in transit, and audit logging consistent with CJIS/FedRAMP requirements

System Resilience

4.2.2.10 The selected solution must ensure system resilience and continuity of operations. The agency is seeking a solution that will meet these requirements, vendors must detail how their solution will meet each of the following areas:

IBM will deploy the solution in **Salesforce Government Cloud Plus**, which maintains a **FedRAMP High** authorization and provides documented business continuity and security controls within the authorized boundary. Salesforce Government Cloud Plus maintains a FedRAMP High JAB P-ATO and provides access to security documentation packages through the approved FedRAMP process.

4.2.2.10.1 A Disaster Recovery Plan (DRP) with a Recovery Time Objective (RTO) of no more than 24 hours and a Recovery Point Objective (RPO) of no more than 1 hour.

IBM will provide a documented **Disaster Recovery Plan** that meets the required **RTO (≤24 hours)** and **RPO (≤1 hour)** by combining:

- Salesforce Government Cloud Plus continuity capabilities (within the FedRAMP High boundary), and
- An implementation-specific backup/restore and operational runbook appropriate for WV OIG's data criticality and compliance needs.

RTO/RPO commitments will be documented and validated during implementation planning and operational readiness.

4.2.2.10.2 Hosting in a geographically redundant, FedRAMP High-authorized data centers located within the continental United States.

The solution is hosted within **FedRAMP High-authorized** Government Cloud Plus infrastructure. Hosting location, redundancy, and boundary details are documented within the FedRAMP security package available through the FedRAMP Marketplace access process.

4.2.2.10.3 System uptime of at least 99.9%, excluding scheduled maintenance windows communicated in advance.

The solution is hosted within **FedRAMP High-authorized** Government Cloud Plus infrastructure. Hosting location, redundancy, and boundary details are documented within the FedRAMP security package available through the FedRAMP Marketplace access process.

4.2.2.10.4 Documented Incident Response Plan aligned with NIST and CJIS requirements, including mandatory notification to the Agency of any outage, data breach, or security incident within 1 hour of discovery.

IBM maintains a documented Incident Response Plan aligned with NIST incident handling practices and CJIS expectations. IBM will provide **notification to WV OIG within one (1) hour of discovery** of an outage, suspected breach, or confirmed security incident impacting the solution, consistent with CJIS reporting expectations and the project's operational procedures.

Training and Knowledge Transfer

4.2.2.11 The vendor must provide comprehensive training and support to ensure adoption and operation of the system. The agency is seeking a vendor that will meet these requirements, vendors must detail how their solution will meet each of the following areas:

- Initial and refresher training programs under an in-person train the-trainer model.
- A staffed help desk with defined Service Level Agreements (SLAs) for incident response and resolution.
- Updated user manuals, administrator guides, and training materials.
- A 24/7/365 help desk with defined response and resolution times.
- All vendor staff with access to Agency systems must complete annual CJIS Security Awareness Training. The vendor must provide documentation of the CJIS Security Awareness Training to the Agency within 7 business days, if requested.

IBM will deliver a structured training and knowledge transfer program to ensure WV OIG can effectively adopt, administer, and sustain the solution. Training will be role-based, repeatable, and aligned to investigative workflows, security requirements, and operational support needs.

Initial and Refresher Training (In-Person Train-the-Trainer)

IBM will provide an initial training program using an in-person train-the-trainer model to build internal WV OIG capability for ongoing onboarding and sustainment. Training will include:

- Role-based end user training (e.g., investigators, supervisors, administrators)
- Hands-on scenarios aligned to OIG investigative processes (intake, evidence handling, approvals, closure)

- Train-the-trainer sessions to enable WV OIG to deliver refresher training internally
  Refresher training materials and repeatable course outlines will be provided for re-use and annual onboarding.

Staffed Help Desk with Defined SLAs

IBM will provide a staffed support function with documented SLAs for incident intake, triage, escalation, and resolution. Support will include:

- Standardized ticket intake and categorization (incident vs. service request vs. enhancement)
- Defined severity levels (e.g., Sev 1–Sev 4) with associated response and resolution targets
- Escalation paths for security, availability, and business-critical issues

SLAs will be finalized with WV OIG during SOW and Negotiation phases after contract award.

Updated User Manuals, Administrator Guides, and Training Materials

IBM will deliver and maintain the necessary documentation for both operational users and system administrators, including:

- End-user guides and quick reference job aids for case lifecycle workflows
- Administrator guide covering configuration, security model, and operational procedures
- Training decks, exercises, and recordings (as applicable) suitable for repeat delivery
  Materials will be updated to reflect approved changes implemented during stabilization and ongoing support.

24/7/365 Help Desk with Response and Resolution Times

IBM will provide 24/7/365 support coverage for priority incidents impacting availability, security, or time-sensitive investigative operations.

All IBM personnel (and any subcontractors) with access to WV OIG systems or environments will complete annual CJIS Security Awareness Training. IBM will maintain training records and, upon WV OIG request, provide documentation of completion within seven (7) business days, consistent with CJIS compliance expectations.

IBM will provide a 24/7/365 help desk located at the ***West Virginia Rocket Center near Keyser, WV*** , to begin following the conclusion of the implementation and roll-out to end users. The help desk will provide basic Level 1 support which could include items such as password resets. More complex issues such as break fixes, enhancement requests, and system changes will be documented, triaged, and queued for consideration with the OIG during the next business day and addressed by the fixed capacity development team upon mutual agreement.

The full scope of the help desk will be negotiated as part of the award including potential integration with the existing WV Office of Technology Service Desk, preferred ticketing system for documentation and number of licenses, and specific items to be addressed by the help desk both during and after business hours. Doing so will allow for IBM and the OIG to mutually identify opportunities to maximize reuse of existing resources while mitigating costs.

Qualification and Experience

Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

4.3.1 Qualification and Experience Information

Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

4.3.1.5 The vendor should provide a narrative summary of its corporate history, years in business, and primary lines of service. The vendor should describe its experience providing technology solutions for investigative, law-enforcement, or oversight agencies, including experience with systems that support fraud, waste, and abuse detection, case tracking, or evidence management. The response should highlight the vendor's familiarity with federal and state compliance standards such as CJIS Security Policy, FedRAMP, HIPAA, and applicable data-protection statutes.

IBM is a multinational technology corporation with a rich and extensive history spanning over a century, dating back to its founding in 1911. Originally established as the Computing-Tabulating-Recording Company (CTR) through the amalgamation of several companies specializing in record-keeping and measuring systems, it was renamed "International Business Machines" in 1924 by Thomas J. Watson. Headquarters in Armonk, New York, IBM is a publicly traded company that has evolved into one of the largest and most respected technology companies globally, serving customers in over 175 countries with approximately 270,300 employees worldwide and reporting revenues of $62.8 billion in 2024.

We bring over 30 years of experience providing Fraud, Waste, and Abuse (FWA) analytic and audit solutions to state clients including Case Management. We currently offer case management services related to tracking Medicaid FWA services for agencies including Iowa, Missouri, North Carolina, and West Virginia. In addition, our experience in case management in other State and Local agencies as well as large health plans give IBM the experience and expertise to help RIAG implement a case tracking solution that will streamline work and effectively track investigations.

Beyond our FWA and Medicaid Investigations support, we have long standing partnerships with States across the country providing a continuum of solutions and services, enabling them to meet and complete work in the area of audits, analytics and reporting enforced by the State statutes, Code of Federal Regulations (CFR), and CMS. We have supported several of these clients for more than 20 years, often over multiple contracts, and many with staff who have been there for the length of our tenure. The portfolio of current customers speaks to our unparalleled Medicaid experience.

4.3.1.6 The vendor should provide detailed descriptions of prior projects that demonstrate experience comparable in size, scope, and complexity to the requirements of this RFP. Each project description shall include:

- The client organization and project title.
- A summary of project objectives, deliverables, and outcomes.
- The duration of the project, implementation methodology, and total contract value.
- Key technologies, platforms, and security frameworks used.
- Measurable results achieved, such as improved efficiency, enhanced security compliance, or cost savings.

IBM was engaged by the **State of Utah, Department of Commerce** to develop a case management and investigation solution for consumer protection to assist in reviewing complaints and educating consumers and businesses about the statutes regulated by the division, and licensing or registering regulated entities.

To accomplish this, we provided an online self-service hub for complainants to find, submit, and check status quickly and easily. Powering this solution required the integration of data from multiple systems into a single view of the constituent, making it easy to deliver personalized, proactive services faster than ever.

Given the extensibility of the Salesforce platform, the initial deployment for the Division of Consumer Protection was expanded to include the Division of Real Estate, the Division of Professional Licenses and the Division of Securities. Investigation modules were added to aid in the follow-up on complaints.

- Our solution has helped improve the efficiency of the Department of Commerce by digitizing their specific processes and services rapidly with a public sector data model, components, and capabilities.
- The consumer complaints solution and investigations modules integrate with the Licensing, Permitting and Inspections solution also built by our team, as well as multiple back-end and State and Federal systems.
- Solution is also integrated with the State's existing payment system.
- Reduced manual processing and time and cost with paperless, no-touch constituent services.
- The extensible and scalable solution, purpose-built for case management, streamlined communication and increased collaboration across departments, with citizens, and with businesses.
- Best-in-class standardization on the Salesforce platform enabled self-service for consumers, dashboards and reports for data visualization, and accessibility anywhere with cloud.
- Our team deployed the solutions with purpose-built industry apps, integrations, data models on a secure compliant platform and greatly reduced the time to go live.

When **New York City** needed help modernizing its criminal justice processes, it reached out to our team. This complex, multi-year application modernization and systems integration effort of a critical system required coordination across ten NYC agencies / organizations.

The solution needed to support near real-time data and system integrations with continuous uptime and guaranteed data integrity and delivery. Legacy application and integrations needed to be replaced. Extremely complex business rules needed to be defined, many of which had to be reengineered from scratch due to lack of documentation or legacy knowledge. IBM helped the city move to a hybrid cloud-based platform (Salesforce & Azure Gov Cloud + On- Prem) that increases platform stability, maintainability, security and flexibility for the agencies involved as

well as provides improved workflows and a fully virtual and paperless environment when required.

Our team has partnered with the **New Jersey Department of Community Affairs (NJDCA)** since 2017 to drive inspections modernization across the agency's many divisions. NJDCA is the state agency created to provide financial support and administrative and technical assistance to local governments, community development organizations, businesses and individuals to improve the quality of life in New Jersey as well as offer programs and services that focus on fire/building safety and housing development. Our team has helped NJDCA replace outdated, fragmented, and inefficient inspection processes with a centralized cloud-based inspection platform -- that would simplify the inspection and citation processes -- and enable faster decision-making to resolve public safety hazards.

The transformation included a user-friendly inspection application to support a variety of users across the state, a portal to enable owners to manage their buildings from registration to payment, integration with state interfaces to support printing, on-line payments and finance, and the migration of millions of records from legacy application in a 2-week window.

Our team's modernization efforts have also helped the NJDCA make it easier for New Jersey citizens to stay warm. When many residents found themselves struggling to pay their heating and cooling bills in the wake of the pandemic, NJDCA (via a federal economic stimulus bill) stepped up to help support New Jersey residents. We worked together with NJDCA to quickly develop and launch a flexible, streamlined application with adjudication process that could help citizens quickly move through the program and obtain the needed financial support. In just a handful of weeks, IBM was able to launch an arrearage forgiveness portal that let applicants submit their information and apply for assistance online — along with a corresponding call center and adjudication platform. Since its launch in 2021, the utility debt relief program has processed more than 50,000 applications, handled more than 300,000 citizen interactions, and dispensed more than $125M in financial aid.

Northeast Ohio Regional Sewer District, OH (NEORSD) is a public utility district serving most of Cuyahoga County and a portion of Summit and Lorain Counties in the state of Ohio. NEORSD serves **more than one million residents** in these areas.

NEORSD used an in-house developed application to support the process of gathering customer inquiries specific to wastewater service, billing questions, and maintenance. Originally designed as a temporary solution, the Inquiry Tracking Log (ITL) system had evolved into the de facto system for tracking all customer contacts whether they be from the web, phone, or e-mail. NEORSD Customer Service Representatives (CSRs) log all customer inquiries into the ITL.

Our Customer Inquiry System powered by Salesforce Service Cloud replaced several systems into a single modern solution for case management, enabling NEORSD to optimize case workflows and automate case closure processes. Omni-channel input now supports inbound ticket creation via live chat, online forms, email, and phone. An online customer portal enables self-service capabilities, while in-built automation helps close cases quickly and concatenates data from multiple systems into Salesforce.

Founded in July 2022, the **City of Saint Louis, Office of Violence Prevention** (OVP) coordinates public safety resources and community violence intervention programs to make St. Louis neighborhoods safer. The new division, funded in part from the America Rescue Plan, is designed to improve public safety outcomes using data-driven community violence intervention strategies. From its initiation, OVP hit the ground running without any major technology helping them to manage their partner/provider network, and with nothing but spreadsheets and emails to help manage distribution of grant funding and RFPs. OVP wanted to have a streamlined solution to manage what were manual processes in segregated documents in a new modern and automated interface that interconnects all information.

The first phase of the project aimed to address several critical business problems faced by the organization. As part of the solution, our team built a comprehensive system to streamline the management of grants and contracts, facilitate efficient communication with contracted partners, and enhance the overall client contact and case management process. Additionally, the system integrated with Salesforce Maps to provide a visual representation of violent crime incident data along with relevant neighborhood information.

- **Grants and Contracts Management**: Before the implementation of the new system, St. Louis OVP encountered challenges in managing their grants and contracts efficiently. Tracking project progress, monitoring partner responses to RFPs (Request for Proposals), and managing project-related metrics and invoices were complex and time-consuming tasks. To address these issues, a centralized portal was developed where contracted partners could easily respond to RFPs and log their project metrics and invoices. This streamlined process improved collaboration and communication between the organization and its contracted partners.
- **Partner Portal Authorization:** The newly created portal provided partner users with secure access to the relevant functionalities based on authorization by OVP staff. This ensured that only authorized personnel could access sensitive data and perform specific actions, enhancing data security and maintaining compliance with confidentiality requirements.
- **Contact and Case Management:** The implementation of a contact and case management system aimed to improve client interactions and service delivery. St. Louis OVP previously faced difficulties in effectively tracking and managing client information, which could result in inefficiencies and potentially impact the quality of services provided. The new system allowed for a centralized database where OVP staff could efficiently manage client data, track interactions, and progress with cases, ultimately leading to more streamlined and effective service delivery.
- **Violent Crime Incident Data Visualization:** To gain deeper insights into crime patterns and trends, the project integrated Salesforce Maps, enabling OVP staff to view violent crime incident data on a geographical map. The data visualization included the plotting of crime incidents, which could be superimposed with additional information layers such as neighborhoods. This feature allowed OVP staff to analyze crime data spatially, identify high crime areas, and make data-driven decisions to allocate resources and plan crime prevention strategies more effectively.

Overall, the St. Louis OVP Phase One project successfully addressed the organization's business challenges by providing comprehensive solutions for grants and contracts management, partner communication, client contact, and case management. Additionally, the integration of crime incident data visualization empowered the organization to make informed decisions.

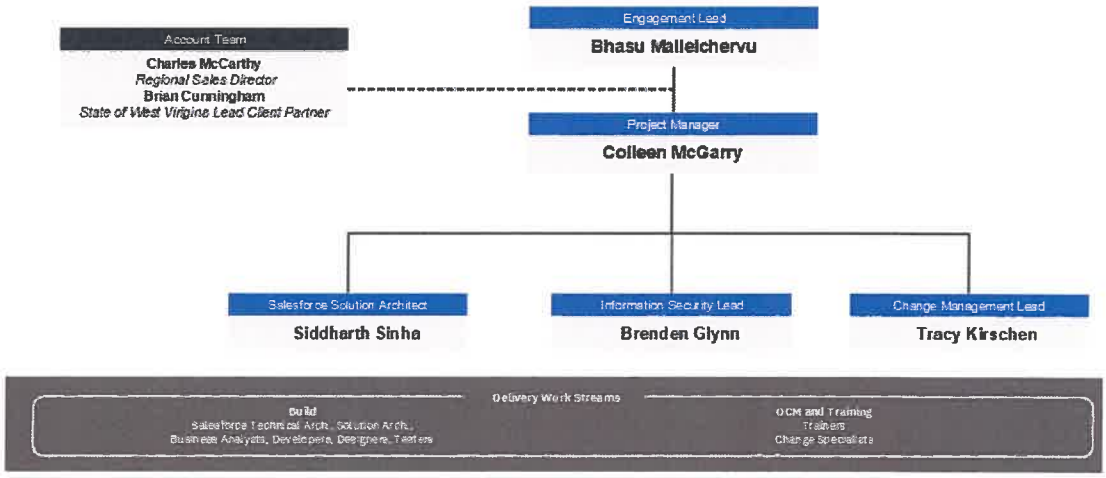
4.3.1.7 The vendor should submit a proposed staffing plan identifying all key personnel who will participate in the project, including their titles, roles, and responsibilities. The plan shall describe the organizational structure of the project team and delineate lines of authority and communication between the vendor and the Agency. Résumés for key staff must include education, relevant certifications, professional experience, and specific expertise in system implementation, cybersecurity, and public-sector investigations.

IBM has assembled a highly qualified team of professionals to support WV OIG's implementation. Our staffing approach ensures the right blend of technical expertise, public sector experience, and change management capabilities necessary for successful system delivery. This section outlines our proposed organizational structure, key personnel assignments, and the lines of authority and communication that will govern project execution.

Organizational Structure

Our project team is structured to provide clear accountability and efficient decision-making throughout the implementation lifecycle. The organizational framework establishes Colleen McGarry, Project Manager, as the single point of contact and primary liaison with WV OIG. All project communications, escalations, and decisions will flow through the Project Manager to ensure consistency and accountability. The Project Manager will maintain regular communication with WV OIG's Project Manager.

Supporting the Project Manager are three primary workstreams: Technical Implementation, Business Process & Testing, and Organizational Change Management. The Technical Implementation workstream is led by Siddharth Sinha, Salesforce Solution Architect, who oversees the development team and ensures technical quality. Our designated Business Analyst/Test Lead will manage requirements gathering and testing activities. The organizational change workstream is led by Tracy Kirschen, Change Management Lead, who will be supported by a Training Specialist. Brenden Glynn, Information Security Lead, operates across all workstreams to ensure security compliance and risk mitigation throughout the implementation.



Organizational chart. IBM proposes the above organizational chart for the WV OIG Case Management System Implementation.

Key Personnel and Responsibilities

Project Manager – Colleen McGarry serves as the overall project leader and primary point of contact for WV OIG. The Project Manager is accountable for delivering the Salesforce Case Management system on time, within budget, and meeting all defined requirements. Key responsibilities include developing and maintaining the integrated project schedule, managing project risks and issues, facilitating communication between IBM and WV OIG, conducting weekly status meetings, and ensuring coordination across all workstreams. The Project Manager will establish project governance structures, manage vendor team performance, coordinate with Agency stakeholders, and provide regular status reporting to Agency leadership. She will also be responsible for contract management, change order processing, and ensuring all deliverables meet quality standards before submission.

Business Analyst/Test Lead – the Business Analyst/Test Lead leads all requirements gathering, business process analysis, and testing activities for the case management implementation. This role serves as the bridge between WV OIG's investigative processes and

the technical solution. The Business Analyst/Test Lead will conduct stakeholder interviews with investigators, supervisors, and administrative staff to document current state workflows and pain points. They will facilitate requirements workshops, develop functional specifications, and create user stories that guide development activities. As Test Lead, they will develop the overall test strategy, create detailed test plans and test cases specific to case management workflows, coordinate User Acceptance Testing (UAT) with Agency personnel, and manage defect tracking through resolution. This role ensures that the Salesforce solution accurately reflects investigative business processes and meets all functional requirements for case intake, assignment, tracking, documentation, evidence management, and reporting.

Salesforce Solution Architect – Siddharth Sinha provides technical leadership and architectural oversight for the Salesforce Case Management platform. The Solution Architect is responsible for designing the overall system architecture, including object model design, data relationships, security model, and integration architecture. He will translate business requirements into technical specifications, define configuration versus customization approaches, and establish development standards for the project team. The Solution Architect oversees all technical aspects of the case management implementation, including custom object creation for case types, workflow automation, approval processes, record sharing rules, and role hierarchies appropriate for investigative operations. Siddharth will also design integration points with external systems, define data migration strategies, conduct technical reviews of developer work products, and ensure platform best practices are followed. This role serves as the technical advisor to WV OIG IT staff and provides guidance on long-term platform scalability and maintainability.

QA Tester(s) – The Quality Assurance Tester(s) execute comprehensive testing of the Salesforce Case Management system to ensure functionality, performance, and reliability. QA resources will execute test cases developed by the Business Analyst/Test Lead, document test results, identify and log defects, and verify defect resolution through regression testing. The QA Tester(s) will test all aspects of case management functionality including case creation, assignment workflows, status updates, evidence tracking, reporting capabilities, and user permissions. This role ensures quality standards are maintained throughout the development lifecycle and that the system performs reliably under various scenarios before UAT begins.

Salesforce Developers – The Salesforce Development team implements the technical solution designed by the Solution Architect. Developers will configure and customize the Salesforce platform to support case management requirements, including creating custom objects, fields, page layouts, record types, and validation rules. The development team will build workflow automation, process builder flows, Lightning components, and custom functionality required for investigative case tracking. Developers will implement security controls including profiles, permission sets, sharing rules, and field-level security appropriate for sensitive investigative data. The team will also develop custom reports and dashboards for case metrics and investigator performance tracking. All development work will follow Salesforce best practices and WV OIG's technical standards, with code reviews conducted by the Solution Architect before deployment.

Training Specialist – The Training Specialist designs and delivers all end-user training for the Salesforce Case Management system. The Training Specialist will develop role-based training curricula for different user groups including investigators, supervisors, administrative staff, and system administrators. They will create training materials such as user guides, quick reference cards, video tutorials, and hands-on exercises that reflect actual investigative workflows. They will conduct train-the-trainer sessions to build internal Agency training capacity and deliver end-user training sessions prior to system go-live. The Training Specialist coordinates with the Change Management Lead to ensure training aligns with the overall change strategy and

addresses user adoption concerns. They will also develop post-implementation training resources and provide knowledge transfer to Agency staff for ongoing user support.

Change Management Lead – Tracy Kirschen leads organizational change management activities to ensure successful user adoption of the new Salesforce Case Management system. The Change Management Lead will conduct stakeholder assessments to identify change impacts, resistance points, and adoption risks across WV OIG. She will develop a comprehensive change management strategy that includes communication planning, stakeholder engagement, and adoption measurement. Tracy will create and execute a communications plan that keeps Agency personnel informed throughout the implementation, addresses concerns, and builds enthusiasm for the new system. This role coordinates with Agency leadership to identify change champions, facilitates user feedback sessions, and monitors adoption metrics post-implementation. The Change Management Lead ensures that organizational readiness activities align with technical implementation milestones and that users are prepared for the transition to the new case management platform.

Information Security Lead – Brenden Glynn ensures that all security, privacy, and compliance requirements are addressed throughout the Salesforce Case Management implementation. The Information Security Lead will conduct security assessments of the Salesforce platform configuration, review and implement security controls for sensitive investigative data, and ensure compliance with all applicable standards. He will work with WV OIG's security team to complete security authorization processes, conduct vulnerability assessments, and implement required security hardening. Brenden will design and implement access controls, audit logging, data encryption, and secure integration patterns. This role ensures that case data, evidence information, and investigative records are protected according to public sector security requirements. The Information Security Lead will also provide security training to the project team, conduct security testing during UAT, and develop security documentation for system authorization.

Resumes

This staffing structure provides WV OIG with experienced professionals who bring specialized expertise in Salesforce implementation, public sector case management, cybersecurity, and organizational change. Detailed resumes for all named key personnel are provided on the following pages, documenting their education, certifications, professional experience, and specific expertise in system implementation, cybersecurity, and public-sector investigations.

Colleen McGarry

Project Manager

Experience

20 years of experience managing large, complex engagements and implementing change and transformation

Specialized and Managerial Experience

- Directed complex challenging implementations for multiple Salesforce products including Salesforce Community Cloud, Service Cloud, Sales cloud and CPQ
- Well versed in projects requiring integration and data migration
- Managed team of 20+ business analysts and trainers for proprietary software company

Education

- MBA - University of Chicago
- BS - University of Illinois Champaign/Urbana

Certifications

- PMP from Project Management Institute
- Salesforce Certified Administrator
- Salesforce Certified Experience Cloud Consultant
- Salesforce Certified Platform App Builder
- Salesforce Certified Sales Cloud Consultant
- Salesforce Certified User Experience Designer
- Salesforce Certified Service Cloud Consultant
- Salesforce Certified Nonprofit Cloud Consultant
- Salesforce Net Zero Cloud Accredited Professional
- Einstein Prediction Builder Accredited Professional

SUMMARY

Highlights of Expertise:

Colleen has 20 years of consulting experience implementing change and transformation, directing large, complex engagements, and delivering quality, on-time, and on-budget results. She has experience working across industries, including, Chambers of Commerce, Nonprofits, member-based organizations, higher education, manufacturing, and financial institutions to improve user and customer experience, increase revenues, and reduce costs. She has unique business and tech translations skills for cloud and premise-based technology. She is proficient in metrics and data driven management methodology supporting customer and team informed decisions. She is an accomplished problem solver and coach and has experience with statement of work development and negotiation, strategic planning, P&L responsibility, agency relationships, national account management, trade show management, promotions, media relations, and staff development. Her key skills include:

- Project Management
- Business Analysis
- Requirements Analysis

- Accounting Principles
- Software Implementations

Her experience will prove invaluable in leading the team in the right directing and providing DBPR with rapid, reliable project success.

RELEVANT PROFESSIONAL EXPERIENCE

EMPLOYMENT HISTORY

Project Manager, IBM, USA | Apr 2021 - Present

Sr. Project Manager, 7Summits (acquired by IBM), USA | Mar 2019 - Apr 2021

- Responsible for ongoing operations and continuous improvement of the Delivery Operations team and PMO, including program management, engagement governance/oversight, stewardship of and refinements to methodology, tools, processes, enablement assets.

Managing Director Chicago and Managed Services Director, Community Brands, USA| Oct 1998 - March 2019

- Responsible for delivery among existing client base for Salesforce platform customers and provided consultation on software, particularly A/R sub-ledger operations in software and change management.
- Managed both large ($5M+) and small ($200K) implementations across the US and Canada

ASSIGNMENT HISTORY

Program Manager, For Profit Higher Education, USA | May 2022 - Present

Project Name: B2B Cross Sell and B2C Org Consolidation

Project Details: Started with the smaller Cross Sell project and then moved to their large org consolidation project to:

- Manage team and lead all planning, communications, budget for the projects
- Work with both the IBM team and the client team to achieve on time/on budget delivery while assisting with guidance of the client change management group to affect the needed business process consolidations
- Manage the B2B Cross Sell project and enable product teams to:
  - Obtain and easily utilize the data needed to upsell and cross sell to new and existing customers
  - Increase revenue and decrease costs through best practice/process adoption while streamlining and enhancing with best of breed functionality

Project Manager, Printing and Financial Services Company, USA | Oct 2021 - Apr 2022

Project Name: Einstein Analytics

Project Details: Managed the project to complete six initiatives to:

- Create new data flows and dashboards for sales and marketing
- Create new functionality demonstrating effects of marketing and sales activities

Project Manager, HR Software, USA | Dec 2020 - Nov 2021

Project Name: CRM Transformation (Salesforce Service Cloud)

Project Details: Managed the project that included full analysis, configuring Service Cloud, enhancing self-service through Experience Cloud, and migrating data to:

- Improve organization efficiency and create groundwork for AI engagement points

- Leverage 30+ co-development resources located in four countries and time zones
- Enable email reduction by approximately 35,000 emails per day

Siddharth Sinha

Education

MBA in Information Technology, Western Governors University, US, 2020

Bachelor of Technology in Information Technology, Uttar Pradesh Technical University, IN, 2008

Languages

English - Fluent

Industry Experience

Media & Entertainment - Experienced

Travel & Transportation - Experienced

Memberships

Computing Technology Industry Association (CompTIA), member

Profile

A trusted advisor and seasoned Salesforce Architect with 16+ years in salesforce ecosystem, having engaged in 40+ implementations for fortune 500 companies. 18x certified SME in designing, developing, and supporting salesforce solutions. Responsible for designing and implementing performant, scalable, maintainable and secure solutions on the Salesforce platform.

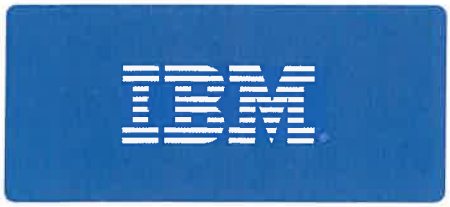
Industry experience includes Public Sector, Travel-Transportation & Hospitality, Telecommunications, Healthcare, Energy & Utilities, Banking and Media. Delivery roles include Technical Architect, Integration Architect, Program Architect and Development Team Lead.

Key skills

Salesforce Sales Cloud
Salesforce Service Cloud
Salesforce Experience Cloud
Salesforce Industries
Apex Triggers and Apex Classes, Lightning Web Components
Identity Management and SSO using Azure, PingId, Okta using with IDP initiated and SP Initiated methods
System Integrations involving SAML, OAuth, OpenID Connect and with Active Directory and LDAP
System Integrations using REST/SOAP/GraphQL or with middleware like Mulesoft, TIBCO, WebMethods, SAP PI, AWS
Einstein for Sales and Service clouds
Field Service Lightning (FSL)
CPQ and Billing - Revenue Cloud
Knowledge
Data Migration, Extract, Transform and Load
Data Backup and Restore
DevOps using Copado, (ANT+Git+Jenkins), Flosum and Gearset
AppExchange

Key courses and training

Salesforce Certified System Architect
Salesforce Certified Integration Architect
Salesforce Certified Identity and Access Management Architect
Salesforce Certified Development Lifecycle and Deployment Architect
Salesforce Certified Platform Developer I
Salesforce Certified Application Architect
Salesforce Certified Sharing and Visibility Architect
Salesforce Certified Data Architect



Salesforce Certified Platform App Builder
Salesforce Certified Administrator
Salesforce Certified Sales Cloud Consultant
Salesforce Certified Service Cloud Consultant
Salesforce Certified AI Associate
Salesforce Certified Omni Studio Developer
Certified SAFe 5 Practitioner
IBM Recognized Speaker/ Presenter
IBM Enterprise Design Thinking Practitioner
IBM Applied AI Professional

Work experience

Salesforce Enterprise Architect
IBM, United States | Mar 2018 - Present

Senior Enterprise Architect responsible for implementing Sales, Service, Experience (Community), Marketing Cloud, Vaccine Cloud, and myTrailhead. SME for buy versus build, config and code, integrations and new feature rollouts. Trusted advisor to the clients for taking end to end enterprise architecture decisions and single verus multi org design. Data migration, archival and backup strategy to store off platform. Implementing customer 360 views. Integrating using Mulesoft, SAP PI, TIBCO or microservices.

Salesforce Technical Architect
Accenture, United States | Aug 2009 - Mar 2018

Technical Architect playing a critical role within Salesforce services to the company's largest, most complex enterprise customers. Provide guidance on application and integration development best practices, Enterprise Architecture standards, functional and technical solution architecture & design, environment management, testing, and Salesforce Platform delivery.

Assignment history

Enterprise Architect Saleasforce
MEDTRONIC | Jan 2025 - Present

Project name: Easy for Everyone (E4E)

Salesforce Service Cloud Rollout with AI enabled IVR/Routing/Decision Engine

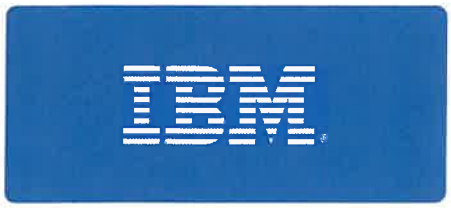
Contribution

Principle Architect Salesforce

Enterprise Architect
BROTHER INDUSTRIES,LTD., United States | Jun 2024 - Present

Project name: Enterprise Architect - Salesforce, Web and E-Commerce

Enterprise Architect in the EA team specifically focussed on designing Rough Order or Magnitude estimation, advise business on best practices, work with senior leadership to ideate future state roadmaps and Salesforce implementation involving Sales, Service, Manufacturing, Data, Commerce and



Marketing Cloud offerings from Salesforce. Involved with re-architecture of existing infrastructure using E-Commerce technologies and designing a future state implementation. Involved with design of e commerce payment infrastructure enhancements involving multiple systems in the enterprise.

Contribution

Face of IBM to client leadership as a Salesforce Enterprise Architect
Design and Deliver Rough order of Magnitude (ROM) estimates for new programs/features
Recommend best practice implementation
Advise on buy versus build, identify software vendors based on business requirements (ex. appexchange)
Participate in E-Commerce from a current state perspective and provide future state recommendation
Ideate off salesforce solutions requiring integrations with SAP and other systems.
Design and participate in enterprise architecture related tickets involving Sitecore, Kibo, CMS, Payment Systems, Dealer portals and B2B/B2C functions
Design solutions for the platform engineering team with new enhancements to Sales, Service, Marketing Cloud on a case by case basis

Salesforce Technical Architect

Delta Airlines, United States | Oct 2023 - Jan 2023

Project name: Jetstream - On Board Services

Enabling the onboard services team (Food and Beverage) onto the existing JetStream instance, where food safety business unit having 1200+ users join the cloud based service cloud instance. This specific implementation caters for overall efficiencies and clear management of food safety issues involving multiple departments and external vendors. The solution incorporates enhancements to an existing salesforce Org, and uses Service Cloud, Field Service and Experience Cloud.

Contribution

Salesforce Technical Architect responsible for Design, Integration and Custom development of the solution.

Salesforce Technical Architect

Princess Cruise Lines, United States | Sep 2023 - Oct 2023

Project name: Princess Brain - Sales & Service

The project was a discovery and creation of design blueprints for enabling Sales, Service and Experience Clouds for PCL, and to scope all potential data and integrations into multiple phases.

Contribution

Salesforce Program Architect responsible for discovery sessions, producing deliverables of technical design and development solutions documented in Jira

Salesforce Technical Architect

Marriott International, United States | Apr 2023 - Aug 2023

Project name: Vacations Club

One of the most technically complex projects ever at IBM, involving real time integrations to more than 8+ systems to cater to online booking, cancellation and reservations for a new Elite membership club program. This included Sales Cloud, Service Cloud, Marketing Cloud, Data Cloud, CPQ, Revenue Cloud, Field Service and Experience Clouds. Other features included 10+ app exchange products along with Copado DevOps.

Contribution

Salesforce Enterprise Architect leading the design, development, DevOps, Integration and Data work streams of 5 TA's, 3 SA's, 5 Dev Leads, 12 Developers and 5 testers.

Salesforce Technical Architect

Delta Airlines, United States | Aug 2022 - Apr 2023

Project name: JetStream Crew Assist - In Flight Services

Project JetStream IFS catered to onboard 35000 flight attendants to use an experience cloud site connected to Service Cloud at the back. 15+ back end office teams were also onboarded to support all the business functionality for these flight attendants. This project was a huge success and helped Delta to start its shift to cloud based salesforce services for its scattered and fragmented business processes and tools.

Contribution

Salesforce Delivery Architect responsible for functional, technical, integration and DevOps.

Salesforce Technical Architect

Delta Airlines, United States | Feb 2022 - Jul 2022

Project name: JetStream Crew Assist - Flight Ops

Custom iOS based mobile application built on Salesforce Experience Cloud and Service Cloud catering to 12000 pilots using the new tool and 15+ back end office teams. The pilots and flight attendants use this app to stay coordinated and organized with the back offices in the massive delta ecosystem.

Contribution

Salesforce Technical Solution Architect responsible for desing, development, integration, data and DevOps

Salesforce Technical Architect

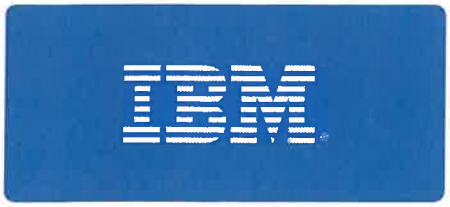
Abbott Laboratories | Mar 2021 - Feb 2022

Project name: Oasis

Create a new portal on AEM (Adobe Experience Manager) that links to Salesforce via AWS Lambda and provides healthcare practitioners a way to register, sign in and perform various tasks keeping the system of experience as AEM but the system of record as Salesforce, and to provide detailed functionality inside salesforce for the sales reps to utilize this information. Integrations with Marketing Cloud for running one time and recurring campaigns.

Contribution

Enterprise Architect



Salesforce Technical Architect

Campbell Soup Company, United States | Feb 2021 - Feb 2021

Project name: myTrailhead

Evaluated the salesforce product myTrailhead. Assessed and designed the SSO options with Okta and myTrailhead, with connected app options to the salesforce instance. Set up and delivered the custom myTrailhead instance, which helps the Sales teams learn about the products and how to go to market with their offerings. It also educates them about the various products, costs and competitive edge.

Contribution

Design and Development Lead, Program architect

Salesforce Technical Architect

State of Florida, United States | Jan 2021 - Jan 2021

Project name: State of Florida - Vaccine Management

Worked on the design for the Vaccine distribution rollout. The salesforce community instance allows users to self register and book appointments. Integrations with Digital Health Pass enable secure PII and HIPAA data encryption and transportation using the mobile app.

Contribution

Salesforce Technical Architect providing blueprint for design of the application

Salesforce Integration Architect

AmerisourceBergen, United States | Nov 2018 - Dec 2020

Project name: AmerisourceBergen BTT program

Led the application integration squad to connect salesforce with external systems using 40+ APIs. Provided best practice recommendations for application and integration development. Part of the ARB to take decisions based on business needs across four in-parallel squads. Lead the design and implementation across multi org merge and complex redesign based on design thinking and modern systems. Implemented integrations with Marketing Cloud for contact preferences opt in/out along with two way sync. Evaluated app exchange products and decided for/against them. Participated in solution sessions for Data Migration, Backup and Archival. Integrated Outlook and Sharepoint with Salesforce. Set up AVAYA CTI with Saleforce for Service cloud. Delivered successful outcomes for Sales, Service, Marketing, Contact Center and Customer Onboarding.

Contribution

Salesforce Integration Architect

Salesforce Technical Architect

Airgas, United States | Jun 2018 - Oct 2018

Project name: Total Access Group Phase-1

Implemented Sales Cloud for Inside and Outside Sales representatives using Campaigns, Leads, Accounts, Opportunity and Products using CPQ. Integrated with SAP on multiple levels using both data ingestion and REST/OData

leveraging Salesforce Connect. Used relevant appexchange products and set up integrations with on premise and cloud systems as deemed fit. This resulted in 400% more effectiveness for the Sales Teams in doing their work in a better and standard manner, eliminating silos and data gaps, getting rid of too many excel files and stickers.

Contribution

Design and Delivery of the Saleforce Technical Solution

Additional information

https://www.salesforce.com/trailblazer/sidsinha

Brenden Glynn

Phone: 617-775-4984
Email: bglynn@us.ibm.com

Education

Bachelor of Science in Computer Network and Information Systems, Wentworth Institute of Technology, US

Digital Credentials

IBM Mentor - 2024

IBM Consulting - Core Expert - 2024

IBM Consultant Profession Certification - Experienced - 2020

IBM Recognized Teacher/ Educator - 2018

IBM Recognized Speaker/ Presenter - 2018

Enterprise Design Thinking Practitioner - 2018

Languages

English - Fluent

Profile

Transformative Executive Advisor | Cybersecurity Strategist

With 20 years of experience in driving global security initiatives across corporate and military sectors, I specialize in empowering organizations to navigate complex threats and enhance resilience. I have successfully conducted over 400 training sessions and executive workshops worldwide, advising leaders, executives, and board members from Fortune 500 companies on effective crisis management and response strategies.

As a recognized thought leader in incident and crisis response, I maintain a commitment to professional excellence through certifications such as CISSP, GCIH, and CASP, ensuring I remain at the forefront of industry trends. My approach fosters a culture of innovation and resilience within organizations. Outside of my professional endeavors, I embrace diverse experiences, including exploring the world as a PADI Open Water Diver.

Key skills

- Executive Leadership / Advisory
- Strategic Planning
- Cross-functional Team Leadership
- Joint Operations
- Defensive Cyber Operations
- Incident Response
- Cybersecurity Strategy Development
- Risk Management
- Crisis Communications

Key courses and training

- United States Army – Command and General Staff College
- United States Army – Cyber Operations Planners Course
- Certified Information Systems Security Professional (CISSP)
- GIAC Certified Incident Handler (GCIH)
- CompTIA Security+ (SEC+)
- PADI Open Water Diver

Work experience

Lead Executive Advisor/Facilitator – Principal Cybersecurity Consultant
IBM X-Force, United States | Oct 2021 - Present

Performs as a Global Executive Lead Facilitator for the IBM Security X-Force Cyber Range, challenging client's
business responses with immersive simulated whole of business crisis-level scenarios.

Leads the development of incident response content for the IBM Security SOAR and QRadar Suite solutions.

Drives strategic and operational collaboration between the IBM Security Threat Management Sales, Services,
Development, and Product Teams.

Establishes best practices, processes, and technologies essential for cross-functional business response to
cybersecurity incidents.

Major – Cyber Warfare Officer (17A) Information Systems Manager (26B/53A) All-Source Intelligence Officer (35D)
U.S. Army Reserves, United States | Jan 2004 - Present

Responsible for developing, implementing, and supervising an appropriate mission-oriented training program to
train the CPT to perform its collective tasks, Defining Cyber Key Terrain and Assets, Risk Mitigation Plan and
Mission Defense Plan development, Cyber Threat Intelligence development and Threat Response Reporting.

Provide trained and ready cyber forces to support the operational requirements of National Mission Forces and
Combatant Command Mission Forces in active defense of U.S. and allied networks.

Incident Response Business/Cybersecurity Consultant, Security Expert Labs
IBM SOAR, United States | Jun 2016 - Oct 2021

Deliver Incident Response Process design, Cybersecurity Advisory, and Technical Leadership through interactive
customer workshops.

Perform as a respected voice of the customer, and as a thought leader for the Incident Response and the
Cybersecurity communities.

Drive strategic and operational collaboration between the IBM Security Threat Management Services and Product
Teams. Leveraging their respective strengths and capabilities, to best provide value to our customers and support
IBM's competitive edge and dominance in the Cybersecurity Industry.

Work closely with the Resilient Engineering, Integration, and Design Teams to deliver industry first Features.

Senior Network Engineer, Advanced Technology Services

General Dynamics Information Technology, United States | Aug 2010 - Jun 2016

Served as the Lead Engineer in support of a multimillion-dollar government contract, providing technical
oversight and guidance to four Principal Engineers, one Senior Engineer, and two Technical Editors.

Engineered, designed, and implemented new modernization and boundary security technologies.

Integrated with the IT Assurance and Operations teams to validate current and future devices deployed in
customers production infrastructures.

Worked with security vendors to ensure the delivery of relevant products and security information.

Development of technical Task Orders, Field Change Orders as well as Test Plans, Test Cards, and Test Reports.

Traveled to CONUS and OCONUS in support of engineering efforts.

Malware Analyst - Information Services Department

MIT Lincoln Laboratory, United States | Aug 2009 - Dec 2009

Monitored several online journals, publications, blogs, mailing lists, vendor and security websites to keep abreast of current and Zero-Day malware and virus threats.

Worked closely with the IT Security Operations team to determine corrective steps for infected and compromised systems.

Assisted in the development of an information monitoring program to track malware and intrusion events, which improved the efficiency and accuracy of the security systems.

Worked with security vendors to ensure the delivery of relevant products and security information.

Wrote detailed reports of each security event investigation and provided metrics to the Department and Directors Offices.

Systems Engineer

Cisco Systems, United States | Jan 2009 - May 2009

Supported Cisco Advanced Lab Operations, Technical Services in the recreation of customer's specific network segments for testing, debugging, and upgrading.

Kept extensive documentation on each lab recreation, including software and hardware configurations, cabling diagrams, and network topologies.

Monitored case-tracking tools for recreation requests. Located and interconnected physical layer components. Established layer 2 and layer 3 connectivity and loaded appropriate IOS images and configurations on devices.

On a daily average, completed 10 recreate cases within the specified time frame based on priority and age.

Installed, configured, upgraded, and maintained Cisco security devices, switches, routers, and workstation PCs.

Updated and maintained the inventory tracking management system for all equipment within the CALO labs.

Enforced lab policies and assisted with ISO compliance.

Systems Administrator

Raytheon Company, United States | Jun 2006 - Dec 2008

Responsible for configuring, maintaining, and troubleshooting network technologies which included: Active Directory, Applications/File servers, NAS devices, and 200+ multiplatform servers/clients per program.

Maintained detailed documentation for events such as installation, inventory, maintenance, and implementation.

Performed security auditing activities such as searching for attempts to compromise security, initiating complete investigations on questionable occurrences, and immediately reporting potential issues up the security chain.

Raytheon Six Sigma qualified. (2006)

Tracy Kirschen

Education

M.A. in Organizational Psychology with a concentration in Organization Change and Consultation, Columbia University - Teachers College, US

B.A. in Psychology Departmental Honors, Phi Beta Kappa, University of Massachusetts at Amherst, Honors College, US

Languages

English - Fluent

Publications

Why a business case for change management (white paper), 2015

Profile

Tracy Kirschen is a Senior Managing Consultant in Organization Change Strategy, within the SAP Process Adoption practice. She has over 15 years of experience at IBM, specializing in large-scale transformation programs. She has led change management programs on several S/4HANA SAP projects, with a focus on driving leadership and employee engagement as well as learning and adoption of the new ways of working.

Key skills

- Driving large-scale S/4HANA SAP transformation programs
- Leading an internal IBM thought leadership initiative on the Rapid Discovery offering and continuous improvement measures

Work experience

Senior Managing Consultant - Org. Change Strategy
IBM, United States | Jul 2007 - Present

- Provide expertise on change management and training to prepare and empower clients to achieve their desired results associated with transformational change
- Over 15 years of change management experience on large- scale ERP transformation projects - strong background in the development and execution of leadership alignment and engagement, business readiness, end-user engagement, and adoption programs
- Additional Experience: Global Change Agent & Super User Networks, Change Impacts and Action Planning, Journey Mapping, Communications, and Training

Assignment history

OCM & Training Lead
Global Healthcare / Distribution Company | Apr 2025 - Present

Project name: Enterprise Forecast Process Redesign (EFPR)

The EFPR program is an enterprise-wide initiative to transform how the client forecasts and plans. The core of the program is a driver-based planning and forecasting methodology powered by SAP Analytics Cloud (SAC). Once deployed, it will drive greater accuracy and faster forecasting, enable business partnering, and enhance decision-making.

Contribution

- Established and delivered the OCM and Training roadmap
- Developed SAP Analytics Cloud training materials across Gross Margin and

Workforce Planning
• Drove change impact validation and action planning
• Conducted trainer readiness efforts and a Train-the-Trainer workshop
• Created a proposed pre-go-live readiness checklist and post-go-live support model; coordination is underway with the client to operationalize pre-and-post-go-live measures

OCM & Training Lead

Global CPG Company | Jul 2023 - Apr 2025

Project name: Central Finance (CFIN) Project

The Global CPG Company is embarking on a multi-year journey to modernize their enterprise operating platform with SAP S4/HANA to enable the company's growth and its digital transformation. The first component of this transformation is the Central Finance project, which will modernize, standardize, and centralize key finance processes in a single global solution driving value for Controllership, FP&A, Shared Services, and other key audiences across the organization. Phase 1 focused on Central Reporting and the Financial Close, and Phase 2 launched Transaction Processing (e.g., AR and AP).

Contribution

• Developed and delivered the organizational change management and training strategies and roadmap
• Conducted client OCM and change impact workshops geared towards driving insights, determining change actions, and executing the change actions and training activities, in partnership with the client
• Managed the training curriculum design, development, and training review and approval processes for Finance, FP&A, and Transaction Processing
• Led a team of 4 consultants, who developed over 50 training work products in coordination with the Functional and Enabling teams
• Developed and delivered a global Change Network, which was comprised of Change Champions (senior influential leaders) and a Super User Network (to provide the first-line support), in coordination with the client PMO and Functional teams
• Drafted and delivered three Train-the-Trainer workshops for global client end-user trainers
• Designed and executed the Super User (SU) Captain network, which was comprised of a subset of the top Super Users who provided heightened support for end-users in their functional area. This program prepared Super User Captains for their role, and key coordination with the Hypercare team.

OCM Lead

Global CPG Company | Jan 2021 - May 2023

Project name: S/4HANA Transformation Project

The global CPG client was seeking to build a global digital foundation with harmonized business processes and data, which unleashed the power of its company and its employees, through streamlined ways of working and key capabilities to drive sustained growth. The scope of this S/4HANA SAP project included Order to Cash, Make to Deploy, Forecast to Schedule, Enterprise Asset Management, Record to Report, Procure to Pay, and Trade Promotions Management.

Contribution

As the Organizational Change Management Lead and Training Advisor, I've developed and operationalized the project's change and training roadmap across the Master Data, Finance, and Wave (Supply Chain) deployments to bring awareness, understanding, and drive adoption across tens of thousands of end-users.

Key responsibilities:
• Developed the change management and leadership engagement strategies as well as the Train-the-Trainer approach, and partnered with the client to deliver them
• Drove the change management and training programs e.g., change impacts, Change Network, engagement, training content development, and the Train-the-Trainer program
• Established the Change Network and Change Network hypercare engagement plan
• Led Change Impact workshops during Integration Sprints across Finance, Accounting, Procurement, and Supply Chain, and established change action plans throughout the deployment
• Established the change and training project plan in coordination with the client with key milestones and dependencies
• Managed a team of 15 consultants to support change management and training efforts, resulting in over 400 training assets developed

Change Management Lead

Global CPG Company, United States | Dec 2019 - Jan 2021

Project name: S/4HANA Transformation Project

The global CPG client was seeking to build a global digital foundation with harmonized business processes and data, which unleashed the power of its company and its employees, through streamlined ways of working and key capabilities to drive sustained growth.

Contribution

• Developed tailored deployment change management and leadership engagement strategies
• Served as the Change Management Lead representing the client and IBM, onboarding 6 client OCM team members until the project hired a client OCM counterpart (in May 2020)
• Developed and drove a robust project OCM Project Plan and deliverables with key dependencies and integration points across the project • Conducted ongoing coordination and integration sessions with process areas, the IBM Europe OCM / Training deployment, as well as Analytics, Deployment, and IBM Integration Leads
• Provided ongoing coaching to my client counterpart and 5 client OCM team members (new to OCM) and managed a team of two IBMers
• Led two IBM project health check surveys utilizing Qualtrics, amidst the pandemic to understand any COVID-19 related support needed from IBMers, onboarding experiences (primarily virtual), and ways of working

Rapid Discovery Change Management Lead

Global Food & Beverage Company, United States | Sep 2019 - Dec 2019

Project name: S/4HANA Rapid Discovery Phase

.

Contribution

As the Change Management Lead, I drove the development and execution of the Executive Alignment program for the S/4HANA Rapid Discovery Phase.

Key Achievements:
• Led the planning, development, approach as well as delivery of over 40 client Executive interviews in coordination with the IBM Account Leadership team •
• Conducted weekly checkpoints throughout Rapid Discovery Phase with IBM Account Leadership team on Executive interview progress, open items, initial findings, and next steps
• Coordinated with OCM Leads from other Rapid Discovery Phase projects on key lessons learned and insight to apply
• Conducted ongoing working sessions and reviews with client IT Leader and client OCM point person to socialize work-in-progress Change Summary Report, preliminary change readiness, baseline high-level change impacts, and executive interview findings
• Actively participated in Rapid Discovery Functional and Master Data workshops as well as Business Value sessions to gain an understanding of Business Capabilities and value pools

OCM Lead

Global Retail Company | Mar 2017 - Aug 2019

Project name: S/4 Fashion - Finance and Supply Chain & SAP Ariba global implementation

The client was transforming its Finance, Supply Chain, and Procurement functions globally through the launch of S/4 Fashion - Finance, Supply Chain, and SAP Ariba technology.

Contribution

For the S/4 transformation, Tracy served as the Global OCM Lead in a multi-vendor environment, leading a team of 3 resources to drive stakeholder management, communications, and readiness activities across 3 client brands, globally, and thousands of end-users.

Throughout her time on this project, Tracy has developed and delivered 7 Change Agent (CA) & Super User (SU) networks, globally for Finance, Supply Chain, and Procurement. In addition to this, she established dedicated stakeholder readiness scorecards, which served as input towards the Business Readiness section of the Project Go-Decision. Further, she has led the CA & SU Hypercare program, across 3 phases, to establish a formal go-around with accountability and real-time hypercare support between the business, IT, functional, and project team.

Tracy has served on the project's Deployment Committee, representing OCM across Cutover, Deployment, and Hypercare activities. Further, Tracy has played a hands-on role, drafting over 60 communications related to BPC, GRC, SAP Ariba, BI Reporting, and S/4 HANA (Finance & Supply Chain) including external wholesale customer messages.

Lastly, Tracy led and helped execute the OCM plan for the SAP Ariba project, across 3 brands and 8 categories, working closely with the client's Senior Director of Procurement across key stakeholder and end-user activities including Information Sessions, the development of journey maps, as well as incorporating an animated video to help ensure the key changes resonated with employees globally.

4.3.1.8 The vendor should demonstrate technical competence in designing, configuring, and implementing secure, cloud-based case management systems. The response should explain the vendor's standard project methodology, including requirements gathering, system configuration, quality assurance, data migration, and user acceptance testing. Vendors should describe how their technical approach aligns with CJIS, FedRAMP High, and HITECH compliance requirements and supports scalability, performance, and long-term system sustainability.

IBM will deliver a secure, cloud-based investigative case management solution for the **West Virginia Office of Inspector General (OIG)** using **Salesforce Public Sector Solutions (PSS)** configured for the full investigative lifecycle (intake through closure), evidence handling, approvals, auditability, and role-based reporting. The approach is designed to operate within a **FedRAMP High-authorized hosting boundary** and to support **CJIS Security Policy** and **HITECH** requirements through security-by-design, documented controls, and operational readiness practices.

Standard Methodology Aligned to WV OIG Timeline and Deliverables

IBM will execute a phased delivery consistent with the WV OIG project structure and staffing plan (23 weeks / ~5.5 months), with defined entry/exit criteria and Agency sign-offs:

Phase 1 – Foundation (Weeks 1–4): Requirements, Architecture, Security Baseline

- Confirm WV OIG investigative workflows, intake channels, evidence handling expectations, approval needs, and reporting obligations.
- Establish the security architecture (identity, access controls, audit logging, retention) and compliance mappings for CJIS/FedRAMP/HITECH.
- Provision environments and define a controlled delivery and release approach.

Phase 2 – Core Build (Weeks 5–12): Configuration-First Implementation

- Configure PSS case lifecycle processes (triage, assignment, tasking, approvals, closure) with standardized data capture and controlled routing.
- Implement workflow automation and dashboards aligned to WV OIG roles (investigator, supervisor, admin).
- Configure SSO integration approach consistent with state identity standards (Azure AD/Entra ID) and document integration patterns for up to two additional interfaces as authorized.

Phase 3 – Testing & Refinement (Weeks 13–16): QA and UAT Readiness

- Execute functional testing, security validation (role access, audit trail behavior), and regression testing.
- Support Agency-led UAT using scenario-based test scripts tied to real WV OIG investigative workflows (intake, evidence upload, approvals, reporting, closure).

Phase 4 – Training (Weeks 15–17, parallel): Train-the-Trainer and Knowledge Transfer

- Deliver in-person train-the-trainer sessions and role-based end-user training aligned to WV OIG operations.
- Provide reusable job aids, user guides, admin guides, and recorded/printable materials for onboarding and refreshers.

Phase 5 – Deployment (Weeks 18–19): Controlled Cutover

- Execute production readiness checklist, final security configuration validation, user provisioning, and go-live support.
- Conduct smoke testing and confirm critical business functions before transitioning to steady operations.

Phase 6 – Hypercare (Weeks 20–23): Stabilization and Transition to AMS

- Triage and resolve post-go-live issues, refine reports/workflows, and finalize the operational runbook and support handoff.

Optional Phase – Data Migration: Controlled, Auditable Migration

Based on responses in the Q&A process, IBM understands that data migration is not required within the current scope. However, we can provide optional data migration services including structured data mapping, transformation rules, loading, reconciliation using repeatable scripts/tools and validation criteria, as well as validation of migrated records with sampling, exception reporting, and Agency confirmation prior to final cutover. If needed, data migration scope, approach, and pricing can be discussed upon contract award during the negotiation and Statement of Work (SOW) phase.

Compliance Alignment: CJIS, FedRAMP High, and HITECH

IBM's delivery approach embeds compliance requirements into each phase rather than treating them as post-implementation tasks. This includes:

- **Encryption in transit and at rest** within the authorized hosting boundary and alignment to federal cryptographic requirements.
- **MFA and SSO controls** consistent with CJIS authentication expectations and state identity management standards.
- **Auditability and traceability** for system access and record-level actions to support CJIS oversight and investigative defensibility.
- **Incident response and notification procedures** aligned to CJIS/NIST expectations, including rapid Agency notification protocols.
- **Workforce compliance controls**, including CJIS Security Awareness Training and CJIS Security Addendum execution for personnel with system access.

Scalability, Performance, and Sustainability for WV OIG

The solution is designed to scale for additional divisions or future departments without re-platforming by:

- Using **configuration-first** patterns (Flows, OmniStudio, security model, standard objects/extensions) to minimize custom code and reduce long-term maintenance burden.
- Structuring data and reporting to support growth in case volume and concurrent usage, including multiple users working in the same case context.
- Delivering complete operational documentation, admin knowledge transfer, and a transition plan to AMS to support long-term sustainment and continuous improvement.

4.3.1.9 The vendor should describe its internal quality assurance and risk-management processes to ensure timely, high-quality delivery of services. The description should include procedures for change control, issue tracking, and escalation of critical risks to the Agency. The vendor should also describe how quality metrics are monitored, documented, and reported throughout the project lifecycle.

IBM will apply established quality assurance and risk-management controls to ensure services are delivered on time, with high quality, and with full transparency to the West Virginia Office of Inspector General (OIG). These controls are embedded throughout the project lifecycle and aligned to regulated-environment expectations (CJIS, FedRAMP High, HITECH), with clear procedures for change control, issue management, escalation, and ongoing quality reporting.

Internal Quality Assurance Approach

IBM uses a structured QA approach that combines configuration reviews, testing discipline, and formal acceptance checkpoints to validate that solution outcomes match WV OIG requirements and investigative workflows. Key practices include:

- **Requirements-to-deliverable traceability** to ensure each requirement is mapped to a configuration, test case, and acceptance criterion.
- **Configuration quality reviews** prior to promoting changes between environments, including security model checks (roles, permissions, sharing) and workflow validation (routing, approvals, SLAs).
- **Test planning and execution** including functional testing, regression testing, and UAT support using scenario-based scripts aligned to WV OIG case lifecycle activities.
- **Release readiness validation** prior to deployment, including completion of testing, defect closure thresholds, and operational readiness checks.

Risk Management and Governance

IBM will maintain a live **risk register** with defined severity, probability, mitigation actions, owners, and due dates. Risks are reviewed routinely and escalated based on impact to schedule, compliance, cost, or operational readiness. Examples of risks actively managed include data availability and quality for migration, integration access approvals, and security validation timelines.

Change Control Procedures

IBM will implement a formal change control process to prevent scope creep and ensure WV OIG maintains decision authority:

- **Change Request (CR) intake and documentation** (description, rationale, priority, dependency, compliance impact).
- **Impact analysis** covering schedule, cost, security/compliance, testing effort, and training/documentation updates.
- **Approval workflow** through WV OIG designated approvers prior to implementation.
- **Controlled release scheduling** to align changes with sprint cycles and testing windows.

Issue Tracking and Defect Management

IBM will use a centralized issue and defect tracking process with:

- Standard categories (incident, defect, configuration change, enhancement request).
- Severity levels and target resolution windows.
- Routine triage sessions with WV OIG stakeholders to prioritize and approve fixes.
- Defect lifecycle governance (open → in progress → ready for test → validated → closed), including regression validation for resolved defects.

Escalation of Critical Risks and Issues to WV OIG

IBM will define clear escalation thresholds and notification procedures, including:

- Immediate escalation for issues affecting availability, security, investigative operations, or compliance requirements.
- Defined escalation path from delivery leads to executive sponsor engagement when thresholds are exceeded.
- Regular status reporting with transparent visibility into risks, issues, decisions needed, and mitigation progress.

Quality Metrics Monitoring and Reporting

IBM will monitor, document, and report quality metrics throughout delivery. Standard metrics include:

- **Schedule health:** sprint burndown, milestone attainment, and dependency tracking.
- **Delivery quality:** defect density, severity distribution, reopen rates, and test pass rates.
- **Requirements coverage:** percentage of requirements tested and accepted.
- **Readiness indicators:** training completion status, open critical issues, and go-live readiness checklist status.

These metrics will be communicated through weekly status reports and regular governance meetings, with action items and decisions documented for WV OIG review and auditability.

4.3.1.10 The vendor should describe its customer-support model, including hours of operation, help-desk capabilities, response times, and issue-resolution procedures. The vendor should summarize its history of meeting service-level obligations under prior contracts and describe tools used for performance monitoring, ticket tracking, and reporting.

IBM will provide a structured, CJIS-aware support model designed to ensure reliable operations of the WV OIG investigative case management solution. The model includes defined hours of coverage, a staffed help desk, documented response and resolution procedures, and transparent performance reporting aligned to service-level expectations.

IBM will provide a 24/7/365 help desk located at the ***West Virginia Rocket Center near Keyser, WV*** , to begin following the conclusion of the implementation and roll-out to end users. The help desk will provide basic Level 1 support which could include items such as password resets. More complex issues such as break fixes, enhancement requests, and system changes will be documented, triaged, and queued for consideration with the OIG during the next business day and addressed by the fixed capacity development team upon mutual agreement.

The full scope of the help desk will be negotiated as part of the award including potential integration with the existing WV Office of Technology Service Desk, preferred ticketing system for documentation and number of licenses, and specific items to be addressed by the help desk both during and after business hours. Doing so will allow for IBM and the OIG to mutually identify opportunities to maximize reuse of existing resources while mitigating costs.

Hours of Operation and Coverage Model

IBM will provide two-tier support coverage:

- **Standard Support (Business Hours):** Coverage for routine incidents, service requests, reporting support, and minor configuration changes during WV OIG business hours.

- **24x7x365 Critical Incident Coverage:** On-call support for Severity 1 issues impacting system availability, security, or time-sensitive investigative operations, including after-hours escalation and coordination with Salesforce Government Cloud support as required.

Help Desk Capabilities

IBM's help desk provides:

- Centralized intake via ticketing (email/portal/phone as agreed)
- Categorization and triage (incident vs. service request vs. enhancement)
- Severity classification and prioritization (Sev 1–Sev 4)
- Escalation paths for security, integration, and platform-related issues
- Knowledge base articles and standard resolution playbooks for recurring issues

Response Times and Issue Resolution Procedures

IBM follows a structured ITIL-aligned workflow:

- **Intake and triage** (validate impact, classify severity, assign ownership)
- **Initial response** (acknowledge, communicate next steps, begin investigation)
- **Diagnosis and resolution** (fix, workaround, or escalation to vendor/platform)
- **Validation** (confirm resolution and perform regression checks as needed)
- **Closure and documentation** (root cause notes, prevention actions, KB updates)

Service levels are defined by severity and finalized with WV OIG during operational readiness. Typical SLA constructs include immediate response for critical incidents and scheduled response for standard requests.

History of Meeting Service-Level Obligations

IBM has an established track record supporting public sector case management and compliance-sensitive systems under defined SLAs, including uptime, incident response, and time-to-resolution commitments. IBM routinely provides SLA performance reporting and governance reviews as part of managed services engagements.

Tools for Monitoring, Ticket Tracking, and Reporting

IBM uses industry-standard tools and processes to ensure measurable performance and transparency:

- **Ticketing / ITSM:** ServiceNow or a comparable enterprise ticketing system (or WV OIG's preferred ITSM if required)
- **Operational dashboards:** SLA attainment reporting, backlog aging, trend analysis, recurring incident identification
- **Release and environment monitoring:** Platform health and event monitoring signals available within the hosting boundary, plus IBM operational runbooks and escalation procedures
- **Reporting cadence:** Weekly operational summaries during stabilization/hypercare and monthly/quarterly service reviews in steady state

IBM will align reporting formats and cadence to WV OIG governance expectations and will provide a clear escalation procedure and points of contact for operational and executive-level issues.

4.3.2 Mandatory Qualifications and Experience Requirements

The following mandatory qualification or experience requirements, or combination of both, must be met by the Vendor as a part of its submitted proposal. Vendor must describe how it meets the mandatory requirements and includes any area(s) where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications and experience requirements are listed below.

4.3.2.5 The vendor must provide verifiable documentation showing successful implementation of at least one (1) cloud-based system authorized at the FedRAMP High impact level, one (1) system that complies fully with CJIS Security Policy, and (1) system that complies with HITECH requirements within the past five (5) years. Documentation should include:

- Evidence of continuous monitoring and vulnerability management consistent with NIST SP 800-53 Rev. 5 controls.
- A description of the vendor's experience maintaining compliance with FedRAMP continuous monitoring, reporting, and remediation requirements.
- The vendor must also submit copies of any relevant security certifications, FedRAMP listings, audit reports, or compliance attestations supporting the proposed solution.

IBM has extensive experience implementing Salesforce Public Sector Solutions (PSS) on Salesforce Government Cloud Plus, a secure cloud environment purpose-built to meet the highest U.S. government security and compliance requirements. Salesforce Government Cloud Plus is authorized at the FedRAMP High impact level, the most stringent authorization under the Federal Risk and Authorization Management Program. FedRAMP High authorization confirms implementation of a comprehensive control baseline aligned with NIST SP 800-53 Rev. 5, including continuous monitoring, vulnerability scanning, incident response, and documented remediation processes. Salesforce Government Cloud Plus holds a FedRAMP High Provisional Authority to Operate (P-ATO) issued through the Joint Authorization Board (JAB), as reflected in publicly available Salesforce compliance documentation:
https://compliance.salesforce.com/en/categories/fedramp-high

IBM has repeatedly implemented Salesforce PSS solutions on Salesforce Government Cloud Plus for federal, state, and local government agencies, supporting secure cloud-based workloads such as case management, licensing and permitting, eligibility systems, constituent services, and investigative applications. Across these implementations, IBM has supported ongoing FedRAMP continuous monitoring activities, including vulnerability management, POA&M tracking, security reporting, and change control processes consistent with federal requirements.

In addition to FedRAMP High authorization, Salesforce Government Cloud Plus has completed an independent assessment against the FBI Criminal Justice Information Services (CJIS) Security Policy. This assessment validates that Salesforce's implemented security controls align with CJIS requirements for the protection of Criminal Justice Information (CJI), including access controls, encryption, auditing, personnel security, and incident response. Salesforce publishes CJIS assessment documentation to support agency compliance determinations:

https://compliance.salesforce.com/documents/a006e000013GLo5AAG

IBM has delivered Salesforce PSS implementations for justice, public safety, fraud investigation, and regulatory enforcement agencies that rely on CJIS-aligned security capabilities, ensuring sensitive criminal justice data is protected throughout the system lifecycle when deployed in accordance with state CJIS agreements.

Salesforce Government Cloud Plus also supports compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act and the HIPAA Security, Privacy, and Breach Notification Rules. Salesforce provides HIPAA compliance documentation, executes Business Associate Addendums (BAAs), and undergoes third-party assessments demonstrating the platform's ability to support workloads involving Protected Health Information (PHI). Salesforce's healthcare and HIPAA compliance posture is documented here:

https://compliance.salesforce.com/en/categories/hipaa

IBM has implemented Salesforce PSS solutions in healthcare-related and human services environments where PHI is processed, applying Salesforce's certified security controls together with IBM's secure configuration, governance, monitoring, and compliance management methodologies.

IBM can provide verifiable documentation supporting these implementations, including Salesforce's FedRAMP High listing, CJIS assessment documentation, relevant security certifications, audit summaries, and compliance attestations. Collectively, IBM and Salesforce Government Cloud Plus offer a proven, secure, cloud-based solution that satisfies the RFP requirements for FedRAMP High authorization, CJIS Security Policy alignment, and HITECH compliance within the past five years.

Key Assumptions

Scope Confirmation

- Final confirmation of investigative workflows, case types, evidence handling rules, report templates and integration points will occur during the Discovery Phase.
- Any work identified during discovery that falls outside the awarded scope will follow a formal change control process.

System Access

- The Agency and State IT will provide timely access to systems, environments, databases, networks and documentation needed for integration, testing and security activities.

Identity and Network Integration

- The State's identity provider, network configuration, VPN access and firewall rules will be available to support MFA, SSO and secure API connections required for CJIS-aligned authentication and remote access.

Stakeholder Engagement

- Agency subject matter experts, investigators, administrators and decision makers will participate in workshops, validation sessions, testing cycles and approval points needed to keep the project on schedule.

Licensing and Hosting

- A FedRAMP High hosting environment (such as Salesforce Government Cloud Plus or an equivalent platform) will be procured, active and available before configuration begins.
- Third-party security or compliance documents required for validation will be provided to the Agency.

Third-Party Dependencies

- External systems such as MMIS, financial systems, Google Workspace and law enforcement systems will maintain stable APIs, service availability and documentation needed for integration.
- The State or its vendors will expose required interfaces for all integrated systems.

Support and Call Center

- The vendor will provide technical system support as described in the RFP. Operational call center or end-user customer support is not included unless requested and scoped separately.

Billing and Costs

- Billing will follow contract terms and occur on a periodic basis such as monthly.
- Travel and living expenses will be billed at actuals if required by the Agency.

Platform Use and Configuration

- Out-of-box platform capabilities will be used wherever possible. Customization will be limited to RFP-required functionality or compliance needs.
- Mobile-specific interface redesigns or custom mobile applications are out of scope unless explicitly requested.

Not in Vendor Scope

- **Call center or citizen support services** such as phone, chat, or email assistance for the public or external users are not included.
- **Paper-to-digital scanning** or conversion of physical documents, evidence, or historical files will not be performed by the vendor.
- **Data migration tasks** including data extraction, data cleansing, data validation, and preparation of legacy data are the responsibility of the Agency.
- **New system interfaces** will not be developed for external systems that do not already expose APIs or documented integration methods.
- **Organizational change management** beyond training content and train-the-trainer sessions is not included.
- **Integrations with any current systems** are not included in current scope.
- **Custom mobile applications**, offline mobile functionality, or major UI redesigns are not included unless separately requested and scoped.
- **Functional enhancements or new modules** beyond what is defined in the RFP will require a change request.
- **Tier 1 support** for end-user help desk operations remains with the Agency unless separately contracted.

Solution Scope Boundaries

Case Management System Implementation

- Deploy Salesforce Public Sector Solutions Investigative Case Management on Salesforce Government Cloud.
- Configure case intake, triage, assignment, investigation, evidence management, approvals and closure.
- Use pre-built PSS ICM objects with an estimated 80% configuration and 20% customization.
- Provide role-based workspaces for investigators, supervisors and administrators.
- Support secure case activity logging, task tracking, document storage and chain-of-custody controls.
- Configure platform security including MFA, SSO, RBAC, audit logging, encryption, session controls and CJIS-aligned workflows.
- Standard Salesforce user interface will be used. No custom mobile applications are included.

Internal Portal / Interface

- Provide secure internal access for OIG staff to process complaints, referrals, subpoenas, evidence updates, notes, approvals and investigative actions.
- Access will be restricted based on defined user roles.

Integrations

- No integrations included at initial go-live.
- Any integration work will be contracted separately through a change request.

Reporting and Analytics

- Configure dashboards for investigators, supervisors, administrators and executives.

- Deliver reports for case aging, workload, evidence tracking, audit logs and trend analysis.
- Reports will be built primarily with Salesforce out-of-box features.
- Support exports to PDF, CSV and Excel.

Change Management and Training

- Deliver training using a Train-the-Trainer model.
- Provide in-person training along with reproducible materials in web-based or DVD formats.
- Deliver administrator, investigator and supervisor training.
- OIG leads broader organizational change activities.

Data and Content Migration

- No data migration is included in this scope.
- Any extraction, cleansing, validation or transformation of legacy data is the responsibility of the Agency and may be addressed through a change request.

Security and Compliance

- Configure required controls aligned to CJIS Security Policy, HITECH/HIPAA, FedRAMP Moderate platform controls and FIPS 140-3 encryption needs.
- Support MFA, SSO, logging, encryption, SIEM/DLP/IDPS connectivity and secure access models.

Hypercare Support

- Provide 30 days of post-go-live Hypercare.
- 24/7 support for Priority-1 critical issues during the Hypercare window.
- Focus on rapid investigation, triage and stabilization.

AMS Support

- Scope is limited to functionality delivered by IBM.
- Business-hours coverage (9:00 AM–5:00 PM EST, Monday–Friday, excluding State holidays).
- IBM provides on-call coverage for P1 issues only.
- No formal SLA commitments included; SLAs will be finalized with OIG in the first six months. Upper boundary for SLAs will exceed no more than 10% of monthly fees.
- Support is capacity-based and constrained to the AMS hours in the contract.
- Enhancements are not included and will require a change request.
- OIG provides Tier 1 and Tier 1.5 support.
- IBM provides Tier 2 and Tier 3 support during business hours.
- Client provides service management tools and manages ticket intake.
- Platform-level issues or defects will be handled directly between the State and Salesforce.
- Any code or configuration changes required due to platform updates will be handled through a PCR unless covered by available AMS capacity.
- Technical assistance will be delivered based on available AMS capacity.
- IBM and OIG will define AMS capacity requirements in the first six months; any adjustments will require a PCR.
- No training is included during the AMS period.

- Client is responsible for security, performance and integration testing during the AMS period.

Contract Exceptions & Clarifications

Upon the State's award of this work to IBM the parties will negotiate and sign a Statement of Work ("SOW") which will describe the scope of the work, our respective responsibilities, Charges, and other terms. The mutually signed SOW will be the final description of IBM Services and will supersede IBM's RFP Bid Response in the Order of Precedence.

RFP Section	Section	Term	Comments/Revised Language
General Terms and Conditions	1	Contractual Agreement	Vendor reserves the right to negotiate the terms of the agreement. For clarity, Vendor's signature on its bid does not signify Vendor's agreement to the terms and conditions in the RFP or contract attached to the RFP. The following table includes a list of exceptions and requested modifications that Vendor would seek to discuss if selected.
General Terms and Conditions	4	Authority to Proceed	IBM acknowledges that, if selected, an Award Document shall be issued after negotiations.
General Terms and Conditions	5	Quantities	IBM requests clarification on section 5; IBM is a 'Service' provided not a 'Quantities' based provider.
General Terms and Conditions	7	Required Documents	IBM acknowledges that no boxes are checked in this section.
General Terms and Conditions	8	Insurance	IBM carries robust coverage, if selected, IBM would request minor modification to section 8 (Insurance requirements) to align with IBM's policy language, included but not limited to removal of Cyber in lieu of IBM's Professional Liability coverage.
General Terms and Conditions	11	Liquidated Damages	IBM acknowledges that liquidated damages shall not be part of any contract under this engagement.
General Terms and Conditions	12	Acceptance	Vendor's signature on its bid does not signify Vendor's agreement to the terms and conditions in the RFP or contract attached to the RFP. This exceptions table includes a list of exceptions and requested modifications that Vendor would seek to discuss if selected, prior to any contract agreement. Therefore, Vendor would request the following restatement of section 12: "*Vendor's signature on its bid, or on the certification and signature confirms Vendor's proposed solution to the RFP and shall be valid for ninety (90) days after submission of the proposal*"
General Terms and Conditions	13	Pricing	IBM does not maintain publicly advertised pricing therefore, the last line in section 13 is not applicable and IBM would ask that it be removed. For clarity, IBM requests that the phrase "...firm for the life of the Contract' be replaced with, "...*firm for the initial term of the Contract*".

General Terms and Conditions	16	Taxes	IBM requests further discussion on section 16
General Terms and Conditions	17	Additional Fees	IBM requests that section 17 include the following exception – "*unless approved by the State of West Virginia*"
General Terms and Conditions	28	Warranty	IBM requests that section 28 be replaced with the industry standard following Warranty language: *"Vendor warrants that it shall perform the Services in a professional manner that meets or exceeds the standards of the information technology consulting industry, and that upon delivery the Deliverables shall conform in all material respects to their specifications as set forth in the applicable Statement of Work. In the event that the Services and/or Deliverables do not conform to this warranty, and provided that the Agency notifies Vendor in writing specifying the nature and extent of the non-conformity within thirty (30) days of the acceptance of the Services or Deliverables claimed to be non-conforming, Vendor shall re-perform the applicable Services or correct the applicable Deliverables at its expense to cure the non-conformity as promptly as possible, but in any event within such period as agreed upon by the parties in writing. Notwithstanding the foregoing, Vendor shall not be responsible for the remedial actions under this warranty to the extent the failure to meet the warranty is caused by or related to modifications to the Services and/or Deliverables, or to the environment in which they operate, by Agency or anyone other than the Vendor or Vendor's subcontractor. Furthermore, if Vendor re-performs Services and the non-conformity is later discovered to be attributable to, caused by or related to modifications to the Services, Deliverables or environment by the Agency or anyone other than the Vendor or Vendor's subcontractor, the Agency agrees to reimburse Vendor for the material and labor costs of the remedial measures. Notwithstanding anything in this Agreement or any Statement of Work to the contrary, Vendor does not warrant any software, application or other product provided by any third party, and Vendor shall have no responsibility or liability for defects in or failures of the Services or Deliverables that Vendor can evidence were caused solely by such software, applications or products or any modifications, upgrades or other changes thereto by such third party and were not caused by Vendor's configuration of such software, applications or products."*
General Terms and Conditions	36	Indemnification	IBM requests that the following industry accepted language replace section 36: "*Vendor will indemnify, defend at its expense, and hold harmless the Agency from all third party claims, damages, losses, and expenses (including attorneys' fees) arising from or related to: (a) IP infringement of Vendor's services or deliverables; (b) Vendor's negligence, gross negligence, or willful misconduct; (c) claims by Vendor's employees against the Agency related to such employee's employment with Agency; (d) government-imposed fines and penalties arising from Vendor's violation of laws applicable to it as an IT service provider ("Third Party Claims").; provided, however, that Vendor's obligation is limited solely to amounts finally awarded or amounts paid in settlement.*

			For any third-party claim that a Vendor Product acquired under this Agreement infringes or misappropriates a patent or copyright, Vendor will defend and indemnify the Agency at its expense and pay any amounts finally awarded by a court against the Agency or included in a settlement approved by Vendor, provided that Vendor shall have no liability for claims arising from: (1) modifications to the Product not made or authorized by Vendor; (2) combination of the Product with items not supplied by Vendor; (3) use of the Product in accordance with specifications provided by the Agency; (4) use of open-source or third-party components specifically requested or provided by the Agency; or (5) use of non-current Product versions for which Vendor has offered an update that would have avoided infringement. As Vendor's sole liability and the Agency's exclusive remedy for such claims, Vendor may, at its option: (i) procure for the Agency the rights to continue using the Product; (ii) modify or replace the Product to be non-infringing without material degradation of functionality; (iii) replace the Product with a functionally equivalent non-infringing product; or (iv) refund any fees paid for the affected Product, less reasonable allowance for prior use, and terminate the Agency's rights to the affected Product. *The Agency will promptly notify Vendor upon receiving any claim covered by indemnity. Vendor 's duty to defend arises upon assertion of claim and includes control over the defense and selection of counsel. The Agency will cooperate in the defense by providing information, access to personnel, and other reasonable assistance at Agency 's own expense. Vendor may not settle any claim without Agency 's prior written consent if such settlement would impose obligations or admissions of liability on the Agency, except for claims by governmental entities. Indemnification survives termination of Agreement.* *For purposes of this Agreement, "gross negligence" means a heightened form of negligence that: (a) involves an extreme departure from the standard of ordinary care and demonstrates reckless disregard for the safety or rights of others; (b) manifests a lack of even slight diligence or care; or (c) constitutes a conscious act or omission in deliberate disregard of a legal duty and the foreseeable consequences to another party."*
General Terms and Conditions	45	Void Contract Clauses	West Virginia Code 5A-3-62. IBM, like most companies, must maintain limits on certain liabilities.
General Terms and Conditions		Additional - Limitation of Liability	IBM requests that the following section be added to any final agreement: "IBM's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the Product and/or Services that are the subject of the claim, regardless of the basis of the claim. IBM will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings. These limitations apply collectively to IBM, its affiliates, contractors, and suppliers.

WV State Government – HIPAA Business Associate Addendum		HIPAA	IBM would like to offer its contemporary BAA in lieu of the HIPAA document included.
Software as a Service Addendum			Not Applicable