RSTATE OF SOUTH DAKOTA
INFORMATION TECHNOLOGY (IT) RFP
South Dakota Department of Health
615 East 4th Street
Pierre SD 57501

Electronic Disease Surveillance System (EDSS) RFP

PROPOSALS ARE DUE NO LATER THAN 10/19/2026 11:59 p.m. CST

RFP #: 27-0908002-001 STATE POC: *Elizabeth Burdick* EMAIL: *Informatics.RFP@state.sd.us*

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____

ADDRESS:_____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO:_____

ZIP (9 DIGITS):_____ FAX NO:_____

E-MAIL:_____

PRIMARY CONTACT INFORMATION

CONTACT NAME: _____ TELEPHONE NO: _____

FAX NO: _____ E-MAIL: _____

---

1. General Information

1.1. Purpose of Request for Proposal (RFP)

The State of South Dakota, through the South Dakota Department of Health (SD DOH) and in coordination with the Bureau of Information and Technology (BIT), is issuing this Request for Proposal (RFP) to solicit proposals from qualified offerors for a secure, configurable, interoperable, and supportable Electronic Disease Surveillance System (EDSS) solution and associated implementation services. The selected offeror will provide the software or platform, configuration, integration, data migration, reporting and analytics enablement, testing, training, go-live, transition, and ongoing support services necessary to replace or modernize the State's current EDSS system.

The future EDSS must support statewide communicable disease surveillance and related public health operations, including case intake and triage, disease investigation, workflow and task management, laboratory and clinical data exchange, data quality and reconciliation, federal and State reporting, reporting and analytics, user administration, role-based access, auditability, and secure access for authorized internal and external users. Detailed functional, technical, security, reporting, integration, implementation, and support requirements will be provided in this RFP and its attachments.

1.1.1 Background:

The South Dakota Department of Health currently relies on a Maven Electronic Disease Surveillance System (EDSS) environment as a core component of its communicable disease surveillance and public health reporting operations. The current environment supports case intake and triage, investigation workflows, case assignment, laboratory and diagnostic result review, disease classification, deduplication, data correction, program reporting, and federal and State reporting. SD DOH users and partners rely on EDSS data to support routine surveillance, outbreak response, program administration, partner communications, public health analytics, and required reporting to CDC.

The current EDSS operates within a broader public health technology ecosystem. Depending on the program area and workflow, that ecosystem may include integration middleware such as Rhapsody, ELR and HL7 interfaces, eCR/AIMS/RCKMS-related workflows, CDC/NNDSS/MMG reporting pathways, SQL or reporting databases, data warehouse or State data repository environments, Power BI or equivalent analytics platforms, SAS, Excel, Azure cloud services, SFTP and file exchange processes, APIs or web services, terminology and reference data sources such as LOINC, SNOMED, and PHVS, and external public health, clinical, tribal, local, contractor, subrecipient, and federal reporting partners.

Stakeholder discovery indicates that the current environment continues to support important core surveillance operations but also requires modernization to reduce risk and improve operational efficiency. Current-state workflows often require users to supplement EDSS functionality with manual entry, external spreadsheets, SQL/SAS/Power BI workflows, email coordination, manually maintained files, custom-coded reporting or configuration processes, and case-by-case reconciliation. Operational pain points include data quality and validation burden, high-volume laboratory triage, sender and terminology mapping changes, incomplete or ambiguous incoming reports, duplicate or fragmented person/case/program records, limited self-service reporting, difficult visibility into workflow status, and the need to preserve auditability and data lineage across manual entry, interfaces, imports, reporting extracts, and administrative configuration changes.

The future EDSS procurement is intended to provide SD DOH with a sustainable and configurable platform that can support event-based communicable disease surveillance while also accommodating program-specific workflows that may require longitudinal person/client tracking, service documentation, relationship and contact management, geospatial and jurisdictional support, external data exchange, and analytics-ready data outputs. The State expects the implementation to account for current operations, migration of historical and active data, continuity of critical reporting and interfaces, testing and validation across environments, user training, change management, and post-go-live stabilization.

The Background section is intended to provide context only. Detailed vendor obligations, response instructions, evaluation methods, and acceptance criteria will be stated in the scope of work, security/vendor questionnaires, cost proposal instructions, and contract attachments.

1.1.2 Goals and Objectives:

The State's primary goal is to procure and implement a modern EDSS solution that supports SD DOH's statewide public health surveillance mission while improving operational efficiency, interoperability, data quality, reporting, security, and long-term maintainability. The solution should provide a sustainable foundation for communicable disease surveillance and related public health program operations, while allowing SD DOH and BIT to manage future change without excessive reliance on custom code, one-off reporting workarounds, or disconnected external tools.

The State's goals for the future EDSS include the following:

- Support core surveillance operations, including case intake, triage, investigation, person/client and event records, workflow management, laboratory and clinical data review, outbreak support, program-specific work, and authorized internal and external user access.

- Improve usability and efficiency for epidemiology, investigation, informatics, program, reporting, administrative, and technical users by reducing duplicate entry, manual reconciliation, unnecessary navigation, spreadsheet-dependent tracking, and other avoidable workarounds.

- Strengthen interoperability with public health data sources and destinations, including ELR/HL7, eCR-related workflows, CDC/NNDSS/MMG and other federal reporting pathways, integration middleware, APIs, SFTP/file exchange, reporting databases, data warehouse or State data repository environments, BI tools, terminology services, and external public health partners where authorized.

- Improve data quality, traceability, and governance through validation, reconciliation, deduplication support, source attribution, audit trails, configuration control, clear data lineage, and consistent reporting-ready data structures.

- Provide secure, role-appropriate access to sensitive public health data, including PHI and PII, with identity management, access controls, auditability, data-governance boundaries, and support for State security and BIT technical review requirements.

- Enable reporting, analytics, dashboards, extracts, and self-service query capabilities that support operational management, program reporting, federal and State reporting, partner reporting, leadership visibility, and approved downstream

analytics.

- Support governed configuration of forms, questionnaires, workflows, rules, reference data, terminology, templates, user roles, and reporting-related structures with appropriate testing, validation, versioning, promotion, rollback, and change-control safeguards.

- Maintain performance, reliability, availability, operational monitoring, error handling, scalability, environment separation, and supportability appropriate for high-volume laboratory processing, outbreak response, routine surveillance, federal reporting cycles, and State technology operations.

- Support implementation, migration, testing, training, change management, go-live readiness, stabilization, documentation, and ongoing operations in a manner that protects continuity of surveillance and reporting during transition from the current EDSS environment.

The State's objectives for the resulting contract are to obtain a solution and implementation partner that can configure and deploy the EDSS; migrate or make available required historical data; preserve or replace critical interfaces and reporting pathways; support user acceptance testing, security review, training, and cutover; provide post-go-live stabilization; and deliver support, maintenance, documentation, and knowledge transfer sufficient for sustainable operations.

These goals and objectives are intended to guide offerors' understanding of the procurement and the State's desired outcomes. Detailed vendor obligations, response requirements, evaluation methods, and acceptance criteria will be stated in the Scope of Work, IT Requirements, Security and Vendor Questionnaire, Cost Proposal instructions, and related attachments.

1.1.3 Description of Components or Phases:

For purposes of this RFP, the State describes the work in terms of major solution and service components and anticipated implementation phases. Components describe the major capabilities, technology areas, and vendor services that must be addressed by the proposed solution. Phases describe the expected sequence for planning, configuring, validating, deploying, and supporting the future EDSS. The State may refine the final phasing approach during contract negotiation and project planning, and offerors may propose alternate sequencing when it reduces implementation risk, protects public health operations, or better supports the State's objectives.

The major components of the EDSS procurement are expected to include the following:

- **EDSS application and platform component.** A configurable EDSS application or platform that supports disease surveillance, person/client and case/event records, investigation workflows, outbreak tracking, contact tracing, and clinical history management.

- **Integration and interoperability component.** Interfaces, APIs, file exchange, message processing, and related integration services needed to preserve or replace critical inbound and outbound public health data exchange, including ELR/HL7, eCR-related workflows, CDC/NNDSS/MMG or other federal reporting pathways.

- **Data migration, conversion, and historical access component.** Services and tools needed to analyze, convert, migrate, reconcile, validate, archive, or otherwise

make available required data from the current EDSS environment and related source systems, including audit, lineage, reporting, and retention considerations.

- **Reporting, analytics, and data access component.** Operational reporting, dashboards, extracts, self-service query, reporting-ready datasets, BI or data warehouse integration, approved downstream analytics, and governance controls for internal and external reporting needs.

- **Security, identity, privacy, and audit component.** Role-based access control, user provisioning and deprovisioning, single sign-on or identity integration where applicable, external user access controls where approved, PHI/PII protections, audit trails, logging, monitoring, and evidence needed for BIT/security review.

- **Hosting, environments, operations, and support component.** The hosting model or models proposed by the offeror; production, non-production, testing, training, and support environments; performance, reliability, backup, disaster recovery, monitoring, maintenance, upgrade, service desk, and support arrangements; and documentation and knowledge transfer needed for sustainable operations.

- **Implementation and transition services component.** Project management, discovery, requirements validation, configuration, design, interface planning, testing, user acceptance support, training, change management, cutover planning, go-live support, stabilization, transition assistance, and vendor support required to place the future EDSS into production safely.

The State anticipates that implementation will include the following phases, subject to refinement through the selected offeror's proposal, contract negotiation, and approved project plan:

- **Phase 1 - Project initiation and planning.** Confirm governance, communication channels, project management processes, staffing, schedule, risk management, decision management, deliverables, and acceptance processes.

- **Phase 2 - Discovery, validation, and solution design.** Validate current-state workflows, program needs, technical architecture, data sources, interfaces, reports, security requirements, user roles, data migration needs, and requirements traceability; produce the baseline design and implementation plan.

- **Phase 3 - Configuration, build, and integration preparation.** Configure the EDSS solution; establish environments; prepare integrations, reporting structures, data migration processes, security controls, and administrative configuration; and maintain traceability to RFP requirements and approved design decisions.

- **Phase 4 - Data migration, interface development, and reporting enablement.** Execute and validate data conversion or historical access activities; develop, configure, or connect required interfaces; establish reporting and analytics pathways; and validate critical federal, State, partner, and program reporting outputs.

- **Phase 5 - Testing, security review, training, and go-live readiness.** Complete system, integration, regression, performance, accessibility, security, user acceptance, migration, reporting, and operational readiness testing; train users and administrators; finalize cutover and support plans; and confirm go-live decision criteria.

- **Phase 6 - Go-live, stabilization, and transition to operations.** Place the solution into production; support cutover; monitor workflows, interfaces, reporting, performance, security, and user adoption; resolve defects; complete knowledge transfer; and transition to ongoing operations and maintenance.

- **Phase 7 - Ongoing maintenance, support, and continuous improvement.** Provide post-implementation support, maintenance, upgrades, release management, documentation updates, service-level reporting, and optional enhancements or phased program refinements as authorized by the State.

The phases above are intended to help offerors organize their proposals and implementation approach. The State does not intend this section to prevent offerors from proposing an iterative, agile, hybrid, program-phased, interface-phased, or other risk-managed delivery model, provided the proposal explains how all required components, deliverables, testing, migration, reporting, security review, training, go-live, and stabilization obligations will be satisfied.

1.1.4 Scope of Components or Phases:

The scope of this RFP includes the products, services, labor, configuration, documentation, licenses or subscriptions, hosting or environment services, integrations, data migration, testing, training, go-live, stabilization, and ongoing support necessary to deliver a production-ready EDSS for SD DOH. The scope applies across all solution components and implementation phases described in this RFP and its attachments.

Offerors must address scope at both the solution level and the implementation level. Offerors must identify all assumptions, dependencies, State responsibilities, third-party products or services, required interfaces, optional items, exclusions, and known scope limitations.

EDSS solution scope includes, at a minimum, the following capability areas.

- **Case, person, client, event, and outbreak records.** Core record management for persons, clients, cases, events, episodes, contacts, exposures, outbreaks, clusters, deduplication, merge/unmerge, record search, lifecycle status, assignment, jurisdiction, and case-linking needs.

- **Workflow, task, and work queue management.** Configurable work queues, triage, routing, assignment, exception handling, alerts, notifications, bulk actions, high-volume review, workflow transparency, user override, and operational status tracking.

- **Program-specific and longitudinal workflows.** Program enrollment, eligibility, services, treatment, interventions, funding attribution, longitudinal program history, contact investigation, partner services, and related program documentation where included in the approved procurement scope.

- **Data capture, forms, questionnaires, and structured documentation.** Configurable forms, structured and narrative fields, required/preferred/optional fields, questionnaires, temporary or event-specific data elements, external survey or form integration where approved, and efficient manual-entry workflows.

- **Laboratory, diagnostic, and clinical data management.** ELR, HL7, manual lab entry, supplemental diagnostic data, eCR-related clinical data, test interpretation, condition-specific reportability logic, lab association, message identifiers, historical

lab visibility, missing-data follow-up, and review of updates to existing or closed cases.

- **Inbound integration, message processing, and external data ingestion.** Inbound ELR, eCR, HL7, API, file-based import, interface-engine, sender onboarding, message validation, parsing, mapping, quarantine, error handling, reprocessing, and external data source integration.

- **Outbound reporting and public health data exchange.** CDC/NNDSS/MMG, HRSA or other federal and program reporting where applicable, pre-submission validation, transmission status, correction, resubmission, reporting snapshots, partner exchange, and other authorized outbound data-sharing workflows.

- **Reporting, analytics, dashboards, and governed data access.** Operational reports, dashboards, self-service query, exports, reporting-ready datasets, BI/data warehouse or reporting-layer integration, scheduled reports, public or leadership dashboards where approved, and authorized analytic access through tools such as Power BI, SAS, SQL, R, Excel, or equivalents.

- **User experience, navigation, and role-based views.** Usable role-specific views, consolidated displays, minimized screen switching, search and lookup, high-volume navigation, clear lab and case visibility, workload/status awareness, and accessible user interface behavior.

- **Data quality, validation, reconciliation, and cleanup.** Validation rules, data completeness checks, duplicate detection, data correction, exception management, field standardization, transformation documentation, reporting-database consistency, reconciliation, and safeguards for administrative or model changes.

- **Audit, traceability, provenance, and lineage.** Auditable history of record changes, data source, interface/import provenance, user and administrative actions, reporting lineage, prior/new values where applicable, and traceability needed for compliance, operational troubleshooting, and reporting validation.

- **Configuration, governance, rules, and change control.** Configurable disease logic, forms, workflows, model/rule management, reference data, terminology, template lifecycle controls, testing before production, versioning, promotion, rollback, separation of duties, and change documentation.

- **Security, privacy, identity, and access control.** Role-based access, least-privilege controls, user provisioning and deprovisioning, SSO or identity integration where applicable, external-user controls where approved, PHI/PII protections, audit reporting, incident-support evidence, and security review support.

- **Documents, templates, uploads, imports, and file management.** Document generation, templates, attachments, structured uploads, import preview/validation, bulk import where approved, secure storage, access controls, versioning, audit history, and transition of required documents or file-based records.

- **Terminology and reference data.** LOINC, SNOMED, PHVS, NDC, value sets, disease/condition mappings, sender-specific mappings, medication or formulary reference data where applicable, effective dating, retirements, historical mapping preservation, and governance workflows.

- **Performance, reliability, scalability, and operational continuity.** Stable remote access, high-volume case and message processing, operational monitoring, error handling, alerting, backup and recovery, service availability, disaster recovery, release management, and continuity through implementation and post-go-live operations.

- **Infrastructure, architecture, implementation, and support.** Hosting or environment architecture, integration architecture, data pipeline compatibility, multiple environments, technical administration, documentation, training environments, vendor support, transition assistance, and sustainable operations support.

Implementation services scope includes, at a minimum, the following activities and deliverables:

- **Project governance and planning.** Project management, schedule, communications, risk and issue management, decision tracking, deliverable management, status reporting, and acceptance processes.

- **Current-state discovery and validation.** Review of current workflows, user roles, program requirements, data structures, interfaces, reports, dashboards, security controls, operational procedures, and known pain points.

- **Requirements traceability and solution design.** Traceability from the RFP to the proposed design, configuration, testing, demonstrations, acceptance evidence, and future operational documentation.

- **Configuration, build, and environment setup.** Configuration of the EDSS solution, establishment of required environments, administrative controls, role profiles, reference data, forms, workflows, reports, and technical configuration needed for testing and production use.

- **Interface and reporting inventory.** Identification, design, prioritization, testing, cutover, and stabilization of required inbound interfaces, outbound reports, partner exchanges, reporting datasets, dashboards, and data access patterns.

- **Data migration and historical access.** Profiling, mapping, conversion, validation, reconciliation, retention, archival, reporting continuity, historical lookup, and acceptance of data migrated or otherwise preserved from the current EDSS and related sources.

- **Security, architecture, and compliance review.** Architecture documentation, security questionnaire responses, vulnerability and remediation support, identity/access design, audit evidence, privacy controls, hosting review, and BIT/security approval activities.

- **Testing and acceptance.** System, configuration, integration, data migration, reporting, regression, performance, accessibility, security, user acceptance, operational readiness, and defect-resolution testing with documented acceptance criteria.

- **Training, documentation, and change management.** Role-based training, administrator training, training materials, job aids, release notes, knowledge transfer, communication support, and readiness activities for internal and authorized

external users.

- **Cutover, go-live, stabilization, and transition to operations.** Cutover planning, production readiness, go-live support, issue triage, performance and interface monitoring, stabilization support, transition documentation, operational handoff, and post-implementation support.

- **Maintenance, support, and continuous improvement.** Ongoing maintenance, support desk model, incident and enhancement processes, updates/upgrades, release management, service-level reporting, documentation updates, and optional future-phase services authorized by the State.

Scope boundaries and optional/future-phase handling. The State expects offerors to address the following boundary areas clearly in their proposals, even where final classification as base scope, optional scope, future phase, or excluded scope remains subject to State decision before release or during procurement: Ryan White and subrecipient workflows; tribal data exchange, including Winter Count or equivalent tribal EDSS integration; city, county, tribal, provider, contractor, or other external user access; public-facing forms or survey workflows; public or leadership dashboards; GIS/geocoding and spatial analytics; analytics sandbox, data warehouse, or reporting-layer access; replacement of disconnected external tools; and decommissioning or archival support for the current Maven-based EDSS environment.

Unless expressly authorized elsewhere in the RFP or resulting contract, this procurement does not require the selected offeror to replace unrelated State systems, make independent policy or data-sharing decisions, assume authority reserved to State procurement/legal/security/governance offices, or deploy production data exchange with external partners without approved agreements and State authorization. Offerors may, however, be required to support analysis, documentation, migration, interfaces, reporting, testing, or transition activities that involve those systems, partners, or governance decisions.

A component or phase will not be considered complete merely because software has been installed or configured. Completion should require accepted deliverables, demonstrated or tested requirements, approved security and architecture evidence where applicable, accepted data migration and reporting validation, operationally ready interfaces, trained users and administrators, completed documentation, resolved priority defects, and State acceptance under the contract and project plan.

Any proposed exclusion, substitution, dependency on State resources, third-party product, or optional item must be clearly identified so the State can evaluate risk, cost, schedule, and contractual impact.

1.2. Issuing Office and RFP Reference Number

The Department of Health (“Agency”) is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota (“State”). The reference number for this transaction is RFP# 27-0908002-001. This reference number must be referred to on all proposals, correspondence, and documentation relating to this RFP. For purposes of this RFP, the State’s centralized IT agency, the Bureau of Information and Technology (“BIT”), must approve all IT related purchases.

1.3. Schedule of Activities (Subject to Change)

All deadlines in the Schedule of Activities are due by 11:59 p.m. CST. The Schedule

of Activities for this RFP is as follows:

RFP Publication	8/24/2026
Deadline for Letter of Intent to Respond	9/8/2026
Deadline for Submission of Written Inquiries	9/14/2026
Deadline for Responses to offeror Questions	9/28/2026
Deadline for Request for SFTP Folder	10/5/2026
Deadline for Proposal Submission	10/19/2026
Discussions / Technical Review	11/1/2026-11/13/2026
Demonstrations and presentations (if required)	11/16/2026
Proposal Revisions (if required)	12/7/2026
Anticipated Award Decision/Contract Negotiation	12/31/2026

1.4. Letter of Intent

All interested offerors must submit a **Letter of Intent** to respond to this RFP.

The Letter of Intent must be submitted to the Agency via email at Informatics.RFP@state.sd.us by the date and time indicated in ***Section 1.3 Schedule of Activities***. Please place the following in the subject line of your email: **"Letter of Intent for RFP# 27-0908002-001"**.

1.5. Submitting a Proposal

All proposals must be completed and received by the Agency by the date and time indicated in ***Section 1.3 Schedule of Activities***.

Proposals received after the Deadline for Proposal Submission will be late and ineligible for consideration.

All proposals must be signed, in ink or electronically, by a representative of the offeror who is legally authorized to bind the offeror to the proposal. Proposals that are not properly signed may be rejected. The offeror's proposal must be prepared pursuant to the requirements of ***Section 6 Proposal Submission Requirements*** of this RFP.

Proposals must be submitted as PDFs via Secured File Transfer Protocol (SFTP). Offerors must request an SFTP folder by the date and time indicated in ***Section 1.3 Schedule of Activities*** by emailing Elizabeth Burdick at Informatics.RFP@state.sd.us with the subject line of "RFP# 27-0908002-001 SFTP Request". The email should contain the name and the email of the person who will be responsible for uploading the document(s).

Please note, the offeror will need to work with its own technical support staff to set up SFTP compatible software on the offeror's end. While the State can answer questions, the State is not responsible for the software required to access the SFTP folder.

No proposal will be accepted from, or no contract or purchase order will be awarded to, any person, firm, or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.6. Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion – Lower Tier Covered Transactions

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the offeror shall attach an explanation to its offer.

1.7. Non-Discrimination Statement

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin, or disability.

1.8. Restriction of Boycott of Israel

For contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.9. Certification Relating to Prohibited Entity

For contractors, vendors, suppliers, or subcontractors who enter into a contract with the State of South Dakota by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Codified Law § 5-18A. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination and would be cause to suspend and debar a business under SDCL § 5-18D-12.

1.10. Modification or Withdrawal of Proposals

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.11. Questions Regarding RFP

All written questions should be sent to: Informatics.RFP@state.sd.us, only emailed questions will be accepted.

Each offeror may submit up to 50 questions via email concerning this RFP to obtain clarification of requirements. No questions will be accepted after the date and time indicated in the above schedule of activities. Email questions to the email address listed above with the subject line “RFP# 27-0908002-001”. The questions and their answers will be sent to all offerors that submitted Letters of Intent, submitted questions, or requested the questions and answers via email before the proposal submittal date and will be sent by the date and time indicated in the above calendar of events. Offeror may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP that have not originated from the SD RFP Project Contact. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and exclusion from specific procurements.

1.12. Proprietary Information

The proposal of the successful offeror(s) becomes public information. Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. An entire proposal may not be marked as proprietary. Offerors must clearly identify in the Executive Summary and mark in the body of the

proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

1.13. Length of Contract

The length of the contract will be for a term of 4 year(s). The State will have the opportunity to renew the contract annually for up to 1 one-year time extensions. The extension(s) will not be automatic.

1.14. Governing Law

This RFP will be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this RFP will be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

1.15. Site Visit

If site visits are required, they will be scheduled before the submission of the proposal. Site visits will be made at the offeror's expense.

1.16. Presentations/Demonstrations

At the State's discretion, the State may require a presentation or demonstration by an offeror to clarify a proposal. However, the State may award a contract based on the initial proposals received without a presentation or demonstration by the offeror. If presentations or demonstrations are required, they will be scheduled after the submission of proposals. Presentations and demonstrations will be made at the offeror's expense.

1.17. Discussions

At the State's discretion, the offeror may or may not be invited to have discussions with the State. The discussions can be before or after the RFP has been submitted. Discussions will be made at the offeror's expense.

1.18. Technical Review

At the State's discretion, the State may require a technical review of the offeror based on the offeror's proposal and response to the Security and Vendor Questionnaire.

1.19. Negotiations

This process is a Request for Proposal/Competitive Negotiation process. Each proposal will be evaluated, and each respondent will be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any component of every proposal submitted. From the time the proposals are submitted

until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2. Standard Contract Terms and Conditions

Any contract or agreement resulting from this RFP will include the State's standard terms and conditions as listed below, the State's standard Information Technology ("IT") contract terms listed in Appendix A, and any additional terms and conditions as negotiated by the parties. The offeror must indicate in its response any issues it has with specific contract terms. If the offeror does not indicate that there is an issue with a specific contract term, then the offeror will be deemed to have accepted the contract terms as written.

2.1. The Contractor will perform those services described in the Scope of Work, attached hereto as Section 3 of the RFP and by this reference incorporated herein.

2.2. The Contractor's services under this Agreement will start on _____, and end on _____, unless terminated sooner pursuant to the terms of the Agreement.

2.3. The Contractor will not use State equipment, supplies, or facilities. The Contractor will provide the State with its Employer Identification Number, Federal Tax Identification Number, or Social Security Number upon execution of this Agreement.

2.4. The State will make payment for services upon satisfactory completion of the services. The TOTAL CONTRACT AMOUNT is an amount not to exceed $____. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL chapter 5-26.

2.5. The Contractor agrees to indemnify the State of South Dakota, its officers, agents, and employees, from and against all claims or proceedings for actions, suits, damages, liabilities, other losses or equitable relief that may arise at least in part as a result of an act or omission in performing services under this Agreement. The Contractor will defend the State of South Dakota, its officers, agents, and employees against any claim, including any claim, action, suit, or other proceeding related to the claim. The Contractor's obligation to indemnify includes the payment of attorney fees and other costs of defense. In defending the State of South Dakota, its officers, agents, and employees, the Contractor will engage other professionals, subject to the written approval of the State which will not be unreasonably withheld. Notwithstanding the foregoing, the State may, in its sole discretion and at the expense of the Contractor, engage attorneys and other professionals to defend the State of South Dakota, its officers, agents, and employees, or to assist the Contractor in the defense. This section does not require the Contractor to be responsible for or defend against claims or proceedings for damages, liabilities, losses, or equitable relief arising solely from errors or omissions of the State, its officers, agents, or employees.

2.6. During the term of this Agreement, the Contractor will obtain and maintain in force insurance coverage of the types and with the limits as follows:

2.6.1 Commercial General Liability Insurance:

The Contractor will maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $1 million for each occurrence. If such insurance contains a general aggregate limit it will apply separately to this Agreement or be no less than two times the occurrence limit. The insurance policy will name the State of South Dakota, its officers and employees, as additional insureds, but liability coverage is limited to claims not barred by sovereign immunity. The State of South Dakota, its officers and employees do not hereby waive sovereign immunity for discretionary conduct as provided by law.

2.6.2 Professional Liability Insurance or Miscellaneous Professional Liability Insurance:
The Contractor will procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1 million.

2.6.3 Business Automobile Liability Insurance:
The Contractor will maintain business automobile liability insurance or equivalent form with a limit of not less than $1 million for each accident. Such insurance will include coverage for owned, hired, and non-owned vehicles.

2.6.4 Workers' Compensation Insurance:
The Contractor will procure and maintain workers' compensation and employers' liability insurance as required by South Dakota or federal law.

Before beginning work under this Agreement, Contractor will furnish the State with properly executed Certificates of Insurance which will clearly evidence all insurance required in this Agreement. In the event a substantial change in insurance, issuance of a new policy, cancellation, or nonrenewal of the policy, the Contractor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Contractor will furnish copies of insurance policies if requested by the State.

2.7. While performing services under this Agreement, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

2.8. The Contractor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to the person or property of third parties, or which may otherwise subject Contractor or the State to liability. The Contractor will report any such event to the State immediately upon discovery.

The Contractor's obligation under this section will only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. The Contractor's obligation to report will not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section will not excuse or satisfy any obligation of the Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.

2.9. This Agreement may be terminated by either party hereto upon thirty (30) days' written

notice. In the event the Contractor breaches any of the terms or conditions of this Agreement, this Agreement may be terminated by the State at any time with or without notice. If termination for a breach is affected by the State, any payments due to the Contractor at the time of termination may be adjusted to cover any additional costs to the State because of the Contractor's breach. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. If after the State terminates for a breach by the Contractor it is determined that the Contractor was not at fault, then the Contractor will be paid for eligible services rendered and expenses incurred up to the date of termination.

2.10. This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of law or federal funds reductions, this Agreement will be terminated by the State upon five (5) business days' written notice. The Contractor agrees that termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State or any officer, agent, or employee of the State, and the Contractor waives any claim against the same.

2.11. This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing will be expressly identified as a part of this Agreement and be signed by an authorized representative of each of the parties to this Agreement.

2.12. This Agreement will be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction's substantive law. Venue for any lawsuit pertaining to or affecting this Agreement will be in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

2.13. The Contractor will comply with all federal, tribal, state, and local laws, regulations, ordinances, guidelines, permits, requirements, and other standards applicable to providing services pursuant to this Agreement and will be solely responsible for obtaining current information on such requirements. Nothing herein will constitute a waiver by the State to any defense to jurisdiction nor will anything under this Agreement constitute an acknowledgement by the State that any tribe has or exercises any jurisdiction over this Agreement or the parties.

2.14. The Contractor may not use subcontractors to perform the services described in this Agreement without the express prior written consent of the State. The Contractor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Contractor will cause its subcontractors, agents, and employees to comply with applicable federal, tribal, state, and local laws, regulations, ordinances, guidelines, permits, and other standards and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Contractor will assist in the vetting process.

2.15. The State reserves the right to reject any person from performing services under this Agreement who the State believes would be detrimental to the services, presents insufficient skills, presents inappropriate behavior, or is considered by the State to be a security risk.

2.16. The Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement will belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s), and other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State.

2.17. The Contractor certifies that neither Contractor nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. Contractor further agrees that it will immediately notify the State if during the term of this Agreement Contractor or its principals become subject to debarment, suspension, or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

2.18. By signing this Agreement, the Contractor certifies and agrees that is has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to the subject matter of this Agreement, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to terminate this Agreement. During the term of this Agreement, if the Contractor no longer complies with this certification, the Contractor agrees to provide immediate written notice to the State and agrees such noncompliance may be grounds for termination of this Agreement.

2.19. Pursuant to South Dakota Codified Law § 5-18A, by entering into this Agreement with the State of South Dakota, the Contractor certifies and warrants that the Contractor is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Codified Law § 5-18A.

The Contractor agrees that if this certification is false, the State may terminate this Agreement with no further liability to the State. The Contractor further agrees to provide immediate written notice to the State if during the term of the contract it no longer complies with this certification, and the Contractor agrees such noncompliance

may be grounds for contract termination and would be cause to suspend and debar a business under SDCL § 5-18D-12.

2.20. Any notice or other communication required under this Agreement will be in writing and sent to the address set forth above. Notices will be given by and to_____ ___on behalf of the State, and by and to _____, on behalf of the Contractor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties will be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination will be sent by registered or certified mail, or, if personally delivered, when received by such party.

2.21. In the event that any court of competent jurisdiction will hold any provision of this Agreement unenforceable or invalid, such holding will not invalidate or render unenforceable any other provision of this Agreement.

2.22. All other prior discussions, communications, and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided in this Agreement, this Agreement constitutes the entire agreement with respect to the subject matter.

2.23. The waiver by either party of a breach or violation of any provisions of this Agreement will not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provision of this Agreement.

2.24. Nothing in this Agreement is intended to constitute a waiver of sovereign immunity by or on behalf of the State of South Dakota, its agencies, officers, or employees.

2.25. Neither party will disclose the contents of the Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that party's rights under this Agreement. The Contractor acknowledges that the State of South Dakota and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws, including, without limitation, posting this Agreement on the website pursuant to SDCL § 1-27-46.

3. Scope of Work

The selected Contractor must provide a complete Electronic Disease Surveillance System (EDSS) solution and the associated implementation, transition, and support services necessary to meet the State's public health surveillance, reporting, data exchange, security, and operational needs. The Scope of Work includes all software, licensing or subscription services, configuration, implementation services, integration, data migration or historical access, reporting and analytics enablement, testing, training, documentation, go-live support, stabilization, and ongoing maintenance and support activities required to implement and operate the future EDSS.

The Contractor must perform the work in coordination with the South Dakota Department of Health (SD DOH), the Bureau of Information and Technology (BIT), program stakeholders, informatics and reporting staff, security reviewers, integration partners, external data

exchange partners, and other State-designated representatives. The Contractor must provide an approach that preserves continuity of critical disease surveillance operations while transitioning from the current EDSS system to the future-state solution.

This Scope of Work establishes the minimum contract-level work obligations for the procurement. Offerors must clearly identify all assumptions, dependencies, exclusions, third-party products or services, State responsibilities, optional services, and scope limitations in their proposals.

3.1. EDSS solution and platform

The Contractor must provide, configure, implement, and support an EDSS solution capable of supporting statewide communicable disease surveillance and related public health operations. The solution must support core surveillance and program activities, including person/client and case/event records, investigation workflows, contact and exposure relationships, outbreak support, program-specific workflows, structured data capture, laboratory and clinical data review, data quality, reporting, analytics, user administration, role-based access, auditability, configuration management, and operational support.

The Contractor must describe how the proposed EDSS solution supports the capability areas identified in this RFP, including but not limited to case/person/client record management; workflow, task, and work queue management; program enrollment, services, treatment, and interventions; data capture, forms, and structured documentation; laboratory, diagnostic, and clinical data management; inbound and outbound data exchange; reporting and analytics; user experience; data quality; audit and provenance; configuration and change management; security and identity; document, template, file, and upload handling; terminology and reference data; performance and reliability; and infrastructure, implementation, and support.

3.1.1. General Case Management & User Interface

3.1.1.1. The system SHALL allow appropriately permissioned users to create, copy, edit, lock, close, reopen, merge, unmerge, deduplicate, and delete case records based on configurable security controls.

3.1.1.2. The system SHALL allow authorized users to review, manage, and correct case data, including notes, patient information, surveillance data, case details, and cases requiring correction before surveillance reporting.

3.1.1.3. The system SHALL support streamlined data entry workflows that allow users to access and enter relevant case data with minimal unnecessary navigation and without relying on external tracking.

3.1.1.4. The system SHALL allow authorized users to view and navigate prior reportable diseases, historical records, related cases, related events, outbreaks, and reportable history associated with the same person.

3.1.1.5. The system SHALL support cross-condition and co-infection analysis across reportable conditions, including authorized viewing and reuse of relevant prior testing, prior condition history, prior treatment, and cross-condition person history, while maintaining condition-specific confidentiality, access restrictions, source attribution, and effective-date context.

3.1.1.6. The system SHALL provide a configurable, rule-based routing engine that automatically directs inbound public health data streams and internal workflow tasks to the appropriate program, jurisdiction, user role, or review queue based on predefined, system-configured criteria.

3.1.1.7. The system SHALL support both automated, rule-based case assignment (driven by case attributes, conditions, or jurisdictions) and manual case assignment or sign-out by authorized users

3.1.1.8. The system SHALL allow authorized users to perform bulk case actions, including bulk case creation, linkage, updates, closure, classification, and permitted edits to case attributes from workflow lists or equivalent case sets.

3.1.1.9. The system SHALL allow authorized epidemiology users to document notes, guidance, and recommendations for DIS or regional staff within the relevant case or workflow context.

3.1.1.10. The system SHALL maintain audit trails for access to disease case data.

3.1.1.11. The system SHALL support configurable program-defined rules for determining whether a case is complete, incomplete, ready for review, ready for closure, or otherwise eligible for workflow progression.

3.1.1.12. The system SHALL store case-associated geography data and preserve relationships among case records, addresses, coordinates, county assignment, census geography, tribal attribution, and geocode processing status.

3.1.1.13. The system SHALL store and report geocode confidence, geocode type, geocode source, geocode status, processing timestamps, and traceability between submitted coordinates and returned geography values where available.

3.1.1.14. The system SHALL support standardized handling of mailing versus physical address data and workflows for identifying and correcting misattributed jurisdiction cases, including tax-address versus true-residency issues.

3.1.1.15. The system SHALL support workflows for determining whether a case is reportable or relevant based on residency, mailing address, testing location, jurisdictional rules, and out-of-state indicators.

3.1.1.16. The system SHALL allow authorized users to disposition unknown records by routing them to the correct disease condition, configuring future handling of similar records, skipping or marking non-reportable records, holding records for further review, deleting records where appropriate, or escalating records to informatics or ELR staff.

3.1.1.17. The system SHALL provide program oversight views that allow authorized program managers or program leads to monitor workload, assignment coverage, case activity, user activity, workflow status, timeliness, and reporting status for their program area.

3.1.2. Contact Tracking & Flexibility

3.1.2.1. The system SHALL support the creation and management of contacts and related persons who can be tracked independently while retaining linkage to source cases, exposure investigations, partner services, or other relevant public health workflows.

3.1.2.2. The system SHALL capture contact investigation information as structured, visible, reportable, and analyzable data rather than storing reportable contact details only in uploaded paper forms, Word documents, PDF attachments, or other attachment-only artifacts.

3.1.2.3. The system SHALL allow programs whose unit of work is not contact tracing to operate without requiring contact investigation fields or event disposition logic where those fields are not applicable.

3.1.2.4. The system SHALL provide a visual relationship map that shows how source cases, contacts, linked persons, and related events are connected, supports directional relationship indicators, allows filtering by condition, investigation, date range, relationship type, and program area, and allows authorized users

to navigate to underlying records.

3.1.3. Outbreak and Cluster Management

3.1.3.1. The system SHALL allow authorized users to create, configure, maintain, modify, retire, group, and link cases to outbreak, cluster, exposure, or investigation workspaces, including outbreak-specific data elements, situational questionnaires, exposure variables, line-list fields, summary views, and high-volume or institutional outbreak scenarios.

3.1.3.2. The system SHALL generate outbreak summaries, rapid snapshots, epidemic curves, basic visualizations, and outbreak reports from system data without requiring external manipulation in SAS, Excel, or Word.

3.1.3.3. The system SHALL support configurable cluster, anomaly, and trend review capabilities that help authorized users identify possible clusters, abnormal trends, unusual disease activity, geographic clustering, temporal clustering, and other program-defined surveillance anomalies using configurable thresholds, rules, dashboards, visual indicators, and notifications where configured.

3.1.3.4. The system SHALL support linkage among human cases, exposed persons, animal events, environmental exposures, exposure events, outbreak events, farm or workplace locations, and related laboratory results where relevant.

3.1.4. Advanced Person and Case Record Deduplication and Merging

The system SHALL provide a comprehensive and configurable capability to manage duplicate person and case records. This capability must include:

3.1.4.1. Identification: A configurable matching algorithm to identify potential duplicates based on demographic and other criteria, including support for State-approved rules for automated, high-confidence merges.

3.1.4.2. Human-in-the-Loop Workflow: An intuitive workflow for authorized users to review potential duplicates. This workflow must include a side-by-side comparison view that allows users to select which data elements to retain from each source record before committing a merge.

3.1.4.3. User-Driven Actions: The ability for trained users to merge records, unmerge records that were incorrectly merged (with a full audit trail), and mark records as known non-duplicates to prevent them from appearing in future reviews (e.g., for twins or individuals with similar names).

3.1.4.4. Auditing and Lineage: A complete and immutable audit trail for all merge, unmerge, and non-duplicate decisions, capturing the "before" and "after" state, the user who performed the action, and the timestamp. Data lineage from the original source records must be preserved.

3.1.4.5. Exception Handling: A process to safely handle and persist user decisions for high-risk identity scenarios, such as twins, siblings, or individuals with shared addresses.

3.1.5. Core Data Model & Record Structure

3.1.5.1. Person-Centric Model: The system SHALL maintain a person-centered data model with a persistent person identifier that is distinct from condition-specific case, event, investigation, and contact identifiers while preserving links to those records.

3.1.5.2. Non-Person Workflows: The system SHALL support rabies, zoonotic, animal-positive, farm or location, exposed worker, DIS facility review, facility-based,

and other animal- or location-context workflows without forcing those events into person-only case structures.

3.1.5.3. Data Linkage & Lineage: The system SHALL link case records to associated laboratory results, message identifiers, and original reporting sources.

3.1.5.4. Case Data Storage: The system SHALL store source-case, contact, exposure, and person relationship data in a structured form that can support visualization.

3.1.5.5. Case Audit: The system SHALL capture and report audit details for case-level and field-level changes, including change source, responsible user or process where available, change date/time, previous value, new value, and security or compliance review indicators.

3.1.5.6. Data Accessibility: The system SHALL make EDSS-derived data available in retrievable structures that support analysis, reporting, outbound messaging, and downstream processing.

3.1.5.7. Architectural Separation: The system SHALL maintain clear separation between transactional case management workflows and governed downstream reporting or analytics workflows to ensure system performance.

3.1.6. Configurable Workflow and Task Management Engine

3.1.6.1. The system shall provide an intuitive, low-code/no-code administration interface that enables authorized, non- technical users to iteratively configure, test, and deploy program-specific workflow queues, actionable worklists, entry and exit criteria, and compact dashboards tailored to display relevant work items and roles.

3.1.6.2. The system SHALL support rule-based automation for routine workflow tasks and transitions, including case auto-closure, case classification updates, jurisdictional status updates, and high-volume case closure where program-approved criteria are met.

3.1.6.3. The system SHALL allow authorized users to perform configurable bulk workflow operations or updates on multiple cases or workflow items without opening each record individually or requiring administrative intervention.

3.1.6.4. The system SHALL support configurable inactivity alerts by disease, program, workflow, case status, or assignment type and notify appropriate users when cases have had no activity for the configured timeframe.

3.1.6.5. The system SHALL support configurable threshold alerts or reporting when workflow volumes, operational thresholds, geocoding error volumes, county mismatch volumes, or failed geocode counts meet or exceed configured limits.

3.1.6.6. The system SHALL alert users or display user-facing indicators when required data elements are missing before reporting, closure, or other configured workflow milestones.

3.1.6.7. The system SHALL display user-facing explanations for automated routing, closure, hold, rejection, manual review placement, workflow entry, workflow exit, or failure to leave a workflow.

3.1.6.8. The system SHALL provide geocoding exception workflows or work queues that allow authorized users to review, assign, resolve, rerun or reprocess, accept, reject, and audit errors, missing coordinates, failed geocode attempts, county mismatches, pending geocoding, rejected geocodes, geocode status discrepancies, and records requiring manual review.

3.1.6.9. The system SHALL identify closed, negative, non-case, or previously

dispositioned records that receive new lab results, ECR data, or other updated information requiring re-review, and route them to re-review queues where configured.

3.1.6.10. The system SHALL provide a configurable, rule-based routing engine that automatically directs all inbound data streams and internal workflow tasks to the appropriate program, jurisdiction, user role, or review queue based on predefined criteria. This capability must include support for both automated and manual case assignment and trigger event-driven notifications, such as new task alerts and inactivity warnings, through configurable channels like in-system dashboards or email to ensure timely user awareness and action.

3.1.6.11. The system SHALL function as a configurable data quality gate, automatically identifying and diverting records with missing, incomplete, inconsistent, or invalid data—such as messages with unmapped or non-standard codes—into dedicated exception-handling workflows. Within these review queues, the system must provide authorized users with the necessary context and tools to efficiently dispose and resolve the identified data quality issues before the records can proceed.

3.1.6.12. The system SHALL support do-not-contact, communication-suppression, or equivalent flags that prevent automated communications from being sent to designated person records, cases, contacts, organizations, or other communication recipients according to configured program policy.

3.1.7. Program Enrollment, Services, Treatment & Interventions

3.1.7.1. Unified Longitudinal Program Management

3.1.7.1.1. The system SHALL support the management of clients in long-term public health programs through a client-centered, longitudinal record-keeping module. This module must be capable of tracking an individual's journey over multiple years and across various program-specific events (e.g., enrollments, eligibility changes, treatments, and services) while maintaining a clear and auditable history.

3.1.7.1.2. The system SHALL support effective-dating for all time-sensitive attributes (e.g., eligibility, income, residence) and allow all reporting to be generated based on the client's status during any defined historical reporting period, rather than solely their current status.

3.1.7.2. Configurable Service and Intervention Tracking

The system SHALL allow for the structured documentation and tracking of all program-specific services, treatments, and interventions. This includes the ability to configure distinct tracking models for:

Ryan White Program Services: Including medication assistance (ADAP), insurance premium assistance, outpatient ambulatory health services, and other service categories with full transaction-level funding attribution (linking costs to specific funding sources and grant years).

STI/TB Treatment and Interventions: Including medication regimens, Directly Observed Therapy (DOT), treatment start/stop dates, outcomes, side effects, and follow-up activities.

3.1.7.3. Program-Specific Reporting and Analytics

The system SHALL provide configurable reporting and analytics capabilities to meet all federal and state program reporting requirements. This capability must include, but is not limited to:

Ryan White Federal Reporting: Native support for generating the Ryan White Services Report (RSR) and the ADAP Data Report (ADR), with full data lineage and traceability from aggregate summary numbers back to the underlying source client and service records.

Programmatic Reporting: Tools to generate reports on case classifications, treatment status and outcomes, reinfection indicators, and other key programmatic performance metrics.

Performance and Disparity Analysis: The ability to generate performance measures and analyze health disparities across all programs based on demographic, clinical, service, and outcome data dimensions.

3.1.8. User Experience, Navigation & Accessibility

3.1.8.1. Role-Optimized and Efficient Workspaces

The system SHALL provide an intuitive, configurable, and role-based user experience that optimizes common public health workflows. The user interface must be designed to minimize clicks, reduce unnecessary screen navigation, and consolidate tasks onto unified dashboards and work queues.

3.1.8.2. Intuitive Data Navigation and Discovery

3.1.8.2.1. The system SHALL provide a clear person-level reporting view and intuitive navigation between a person record and associated cases, condition events, contacts, source cases, related program records, and visual relationship views where required for contact investigation or partner services.

3.1.8.2.2. The system SHALL enable users to easily navigate and explore relationships between different data entities. This includes, but is not limited to, seamlessly moving from a person's record to their laboratory results, contact investigations, and historical events.

3.1.8.2.3. The system SHALL provide powerful, user-friendly search and filtering tools that allow non-technical users to perform ad-hoc queries and create custom case lists based on any combination of data elements.

3.1.8.2.4. The system SHALL allow authorized users to configure saved search views and result columns where permitted.

3.1.8.3. High-Volume Data Processing and Review

3.1.8.3.1. The system SHALL be designed to support the efficient review and disposition of high volumes of records, particularly for tasks like laboratory result triage and case assignment. This includes features such as configurable list views, compact display options, and effective pagination or scrolling mechanisms that allow users to process hundreds of records without performance degradation or workflow interruptions.

3.1.8.3.2. The system SHALL minimize the number of steps, screens, clicks, and module changes required to complete common tasks, move between related data elements, access longitudinal data, and navigate condition-specific case-management information.

3.1.8.4. Accessibility and Usability Standards

The system SHALL be accessible and usable for all staff, including those who use assistive technologies.

3.1.9. Performance, Scalability, Reliability & Operations

3.1.9.1. System Performance and Scalability

3.1.9.1.1. The system SHALL be architected to provide a responsive user experience and process high-volume public health data without degradation.

3.1.9.1.2. The offeror must describe how their solution achieves low-latency user interactions for both routine case management and data-intensive operations (e.g., complex queries, large report generation).

3.1.9.1.3. The system's architecture must be scalable to handle significant and sudden increases in data volume and user load, such as those experienced during a large outbreak or a pandemic, without requiring emergency hardware changes or resulting in system failure.

3.1.9.2. System Reliability and Availability

3.1.9.2.1. The system SHALL be highly reliable and available for all users. The offeror must describe their approach to ensuring high availability, minimizing unplanned downtime, and reliably persisting all user inputs and transactional data without loss.

3.1.9.2.2. The system SHALL provide clear validation feedback and actionable error messages to prevent partial or inconsistent processing outcomes for all critical workflows, including data imports, configuration changes, and reporting database updates.

3.1.9.3. Operational Continuity and Disaster Recovery

3.1.9.3.1. The system SHALL support disaster recovery and continuity of operations planning by maintaining and testing DR/COOP procedures, providing or supporting backup and recovery tools for applications and data, describing backup frequency and restore-testing practices, periodically validating automated full backups, addressing recovery of lost State data, identifying and mitigating single points of failure, supporting reliable backup storage media and geographically disparate or otherwise secure backup storage where applicable, preserving or queuing inbound messages and files during outages for supported inbound message and file channels, and restoring service within agreed SLAs during data center outages, access disruptions, or other continuity events.

3.1.9.3.2. The system SHALL support configurable recovery objectives and service commitments, including recovery point objective and recovery time objective targets defined by the State or agreed SLA, and SHALL support evidence that restoration targets can be met after planned, unplanned, or disaster-related service interruptions.

3.1.9.4. Governed Configuration and Change Management

3.1.9.4.1. The system SHALL support safe and reliable change management for all system configurations, including data models, workflows, and reporting structures.

3.1.9.4.2. The solution SHALL provide a governed, multi-environment pathway (e.g., Dev, Test, Prod) for promoting and deploying changes. This process must include safeguards such as pre-deployment validation, impact analysis, and the ability to roll back faulty configurations without requiring a full database restoration or causing extended downtime.

3.2. Project management, governance, and planning

The Contractor must provide project management and governance services appropriate for a statewide public health technology implementation. At a minimum, the Contractor must

establish and maintain a project management plan, integrated project schedule, risk and issue logs, decision log, communication plan, status reporting process, change-control process, stakeholder engagement approach, meeting cadence, escalation process, and deliverable review and approval process.

The Contractor must coordinate with State project leadership and designated workgroups to manage scope, schedule, risks, dependencies, decisions, deliverables, interface readiness, data migration readiness, testing progress, training readiness, security review, go-live readiness, and post-implementation stabilization. The Contractor must identify State decisions, dependencies, resources, access, data, environments, technical inputs, and third-party participation needed to perform the work.

3.3. Discovery, validation, and solution design.

The Contractor must conduct discovery and validation activities sufficient to confirm the future-state design, implementation approach, configuration approach, integration approach, reporting and analytics approach, security approach, migration approach, testing approach, training approach, and operational support model. Discovery must include review of current workflows, program-specific needs, data exchange pathways, reporting obligations, user roles, access-control expectations, data governance constraints, current-state technical dependencies, and acceptance criteria.

The Contractor must maintain a requirements traceability approach that connects the scope of work, proposal commitments, design decisions, configuration/build activities, test cases, demonstration evidence, defects, acceptance criteria, and final deliverables. The Contractor must identify where requirements will be satisfied through standard product functionality, configuration, integration, reporting-layer capability, third-party services, customization, operational process, or future release functionality.

3.4. Configuration, build, and workflow enablement.

The Contractor must configure, build, or otherwise enable the EDSS capabilities approved for implementation. This includes configuring workflows, forms, questionnaires, data-entry screens, rules, validation logic, work queues, task routing, notifications, dashboards, reports, role-based views, user roles, permissions, reference data, terminology, templates, documents, imports, exports, and administrative functions necessary to support the agreed implementation scope.

The Contractor must use a governed configuration and change-management approach that supports review, testing, versioning, impact assessment, promotion between environments, rollback or remediation where appropriate, and documentation. The Contractor must not rely on undocumented manual changes or unapproved production changes for routine implementation or support activities.

3.4.1. Configurable Forms, Change Management, and Configurations

3.4.1.1. The system SHALL provide a low-code/no-code form builder that allows authorized administrators to create, version, and deploy program-specific questionnaires, clinical forms, and interview instruments.

3.4.1.2. The engine SHALL support advanced form logic, including conditional branching (skip logic), calculated fields, cascading drop-downs, and data validation rules to ensure efficient and accurate data collection across varying disease programs and outbreak scenarios.

3.4.1.3. The system SHALL distinguish among missing, unknown, not asked, not applicable, and intentionally blank data values.

3.4.1.4. The system SHALL allow authorized program staff to configure and identify required fields by condition or case workflow.

3.4.1.5. The system SHALL provide impact analysis for question changes, including

removed, renamed, reconditioned, or reassigned questions and affected workflows, reports, templates, MMG outputs, and imports.

3.4.1.6. The system SHALL prevent accidental removal of data-bearing fields without explicit warning and authorized approval.

3.4.1.7. The system SHALL allow authorized users to review and test question changes and related configuration changes before saving, publishing, promoting, or using them in production.

3.4.1.8. The system SHALL allow authorized users to export, review, and technically inspect questionnaire configuration in XML or an equivalent structured format where applicable.

3.4.1.9. The system SHALL provide in-system validation tools to review question logic, field and question identifiers, naming or spelling consistency, model binding, form/workflow associations, placeholder-to-model relationships, and model configuration before deployment and confirm that model changes are complete, appropriate, limited to the requested scope, bound to the correct model, workflow, or form definitions, and do not break expected system behavior.

3.4.1.10. The system SHALL provide versioning, comparison, change history, and rollback capabilities for configuration changes.

3.4.1.11. The system SHALL support segmented program-area configuration and governance controls that prevent configuration changes or modules for one program from creating unintended cross-program impacts.

3.4.1.12. The system SHALL support disease-specific outbreak data collection, including outbreak-specific question packages, forms, and data elements that vary by condition, exposure type, or reporting requirement.

3.4.1.13. The system SHALL support configurable program models that can accommodate Ryan White reporting and workflow needs without forcing the program into unrelated contact tracing, disease investigation, or event disposition structures or requiring extensive custom redevelopment for routine reporting changes.

3.4.1.14. The system SHALL preserve historical Ryan White client information using effective-dated attributes so users can determine eligibility, insurance, income, employment, enrollment, residence, service status, and active/inactive status for a defined reporting period.

3.4.1.15. The system SHALL support multiple secure pathways for data capture including intuitive manual data entry workflows for public health staff and secure, respondent-facing web forms (e.g., via secure links or portals) for patients or external partners.

3.4.1.16. The system SHALL support mapping or importing responses from external survey tools, static forms, or separately administered data collection instruments into structured EDSS fields for the applicable workflow.

3.4.1.17. The system SHALL ensure that all externally submitted data is securely queued, validated, and linked to the correct internal person or case records upon ingestion.

3.4.1.18. The system SHALL provide built-in test case execution and regression testing capabilities for MMG and CDC reporting configuration changes.

3.4.1.19. The system SHALL allow authorized administrators or technical users to configure geocoding workflows, accepted geocode types, confidence

thresholds, rerun criteria, and exception handling rules.

3.4.1.20. The system SHALL support controlled updates to custom geography layers and reference data without requiring unsupported database changes.

3.4.1.21. The system SHALL support configuration of task schedules using a schedule builder, plain-language or form-based scheduling options.

3.4.1.22. The system SHALL support advanced scheduling syntax for technical users where necessary and display the next scheduled runtime.

3.4.1.23. The system SHALL display the next scheduled runtime and validate the schedule syntax before allowing a user to save a scheduled task.

3.4.1.24. The system SHALL audit changes to task schedules.

3.4.1.25. The system SHALL provide documentation, description fields, or inventory records for configuration elements, customizations, enhancements, interfaces, custom reports, routes, scripts, and other locally maintained system assets so future administrators can understand their purpose and operational impact.

3.4.1.26. The system SHALL restrict import configuration and import execution capabilities by role or group.

3.4.2. Documents, Forms, Files & Uploads

3.4.2.1. The system SHALL support program-specific templates that can be attached to or generated from a case record.

3.4.2.2. The system SHALL allow users to navigate from a case context to related case details, lab results, eCR documents and attachments, person history, notes, and workflow status through in-application document navigation that supports high-volume review, including sortable and filterable attachment lists, previews, jump links, source/date indicators, and return-to-case workflow continuity where applicable.

3.4.2.3. The system SHALL provide secure embedded viewing for rendered electronic case reports and related case documents within the case context without requiring repeated local download.

3.4.2.4. The system SHALL support capture, storage, and auditability of digital signatures for forms, records, documents, or workflows where digital signature collection is required by program policy or State business process.

3.4.2.5. The system SHALL support document management for Ryan White program records, including uploaded applications, supporting eligibility documentation, insurance records, pharmacy records, service documentation, and attachment of application documents to the correct client or program record.

3.4.2.6. The system SHALL allow authorized users to attach supplemental lab results, including whole genome sequencing results, to existing cases where appropriate.

3.4.2.7. The system SHALL support configurable multilingual content for external-facing forms, questionnaires, notices, instructions, and other stakeholder-facing communications where required by State program policy, accessibility needs, or public health response context.

3.4.2.8. The system SHALL support upload, maintenance, and generation of RTF or equivalent dynamic print templates for letters, forms, and correspondence, including templates that can automatically populate with available case, person, user, program, and organization data where configured.

3.4.2.9. The system SHALL support bulk import or bulk upload of structured case, program, pharmacy, and other approved data using configurable templates and formats such as CSV, Excel, JSON, or equivalent structured files.

3.4.2.10. The system SHALL support import into repeatable service, medication, funding, case management, question-group, and other repeating program data structures.

3.4.2.11. The system SHALL allow authorized users to correct upload and import errors in bulk, including medication, funding source, reporting period, service category, client matching, pharmacy invoice, and other affected line-level data without manually editing each affected line one by one.

3.4.2.12. The system SHALL allow authorized users to preview upload or import results before records are committed, including pharmacy invoice imports and other structured upload workflows.

3.4.2.13. The system SHALL validate uploaded files and imported records before committing data, including schema, completeness, required fields, duplicate, invalid, incomplete, improperly mapped, malformed, empty, or destructive-content checks as applicable to the upload type.

3.4.2.14. The system SHALL provide row-level, field-level, and file-level error reporting and review screens for failed imports, upload errors, reporting validation errors, duplicate warnings, and batch upload success or failure results.

3.4.2.15. The system SHALL maintain source attribution and data lineage for imported, uploaded, manually entered, interfaced, corrected, and automatically generated data, including identifying which upload, external source, or manually entered value contributed to each reportable value.

3.4.2.16. The system SHALL support authorized and audited rollback, reversal, bulk deletion, or duplicate-upload reversal for erroneous uploads and imports.

3.4.2.17. The system SHALL support bulk upload and management of multiple administrative files across administrative sections without requiring repetitive file-by-file upload steps.

3.4.2.18. The system SHALL allow authorized users to select a target administrative section, destination, program, or template category before uploading multiple administrative or template files to that destination.

3.4.2.19. The system SHALL allow authorized users to preview or confirm administrative batch upload results before committing changes where appropriate.

3.4.2.20. The system SHALL maintain audit trails for upload submission, validation, import, correction, rollback, reversal, bulk deletion, and administrative file upload activity.

3.4.2.21. The system SHALL support maintenance and upload of approved geospatial boundary and reference files, including GeoJSON, shapefiles, post office reference locations, tribal boundaries, county boundaries, census geography, and other approved GIS layers.

3.4.3. Reference Data, Terminology & Code Management

3.4.3.1. The system SHALL allow authorized users to add, edit, retire, replace, and validate terminology codes through both single-code updates and bulk terminology updates.

3.4.3.2. The system SHALL allow authorized users to export terminology data in user-selectable structured formats, including CSV, Excel, XML, JSON, or equivalent

formats supported by the system.

3.4.3.3. The system SHALL provide reliable search of large terminology tables using prefix, contains, exact-match, and filtered search options without requiring users to page manually through large code tables to locate values.

3.4.3.4. The system SHALL validate terminology code changes against configured completeness, structural, and mapping rules before committing change.

3.4.3.5. The system SHALL maintain audit trails and governance details for reference-code, terminology, and routing changes, including the changed value, responsible user, date and time, and source of the change where available.

3.4.3.6. The system SHALL allow authorized users to configure reference-code routing rules using LOINC, SNOMED, test name, result value, organism, sender, and related lab attributes to determine record creation, disease routing, attachment to existing records, skip logic, or exception queue routing.

3.4.3.7. The system SHALL support user-maintainable reference-code routing logic for routine code additions and updates without requiring custom development.

3.4.3.8. The system SHALL provide tools to identify redundant, conflicting, outdated, or unused reference-code routing rules.

3.4.3.9. The system SHALL maintain standardized codes and terminology values in centralized reference data for code sets managed by the system, including centrally managed LOINC and SNOMED code sets.

3.4.3.10. The system SHALL preserve historical medication and NDC mappings used for prior reporting periods and clearly distinguish current reference values from historical values.

3.4.3.11. The system SHALL support grouping multiple NDCs under a single medication concept.

3.5. Integration, interoperability, and data exchange.

The Contractor must analyze, design, configure, develop, test, document, and support required inbound and outbound integrations and data exchange workflows. The integration scope may include ELR, HL7, eCR-related workflows, AIMS/RCKMS-related workflows, laboratory and clinical data sources, integration middleware such as Rhapsody or an equivalent interface engine, CDC/NNDSS/MMG reporting, HRSA or other federal reporting pathways, APIs, SFTP or file exchange, reporting databases, data warehouse or BI platforms, terminology or reference-data sources, external partner systems, and other State-approved data exchange needs.

The Contractor must participate in interface inventory, source/target mapping, message or file specification review, sender/receiver onboarding, transport design, validation, error handling, reconciliation, monitoring, cutover planning, and post-go-live stabilization. The Contractor must identify which integrations are included in base scope, which are optional or future phase, which depend on third-party participation, and which require State-provided infrastructure, access, credentials, specifications, data use agreements, or technical resources.

3.5.1. Laboratory, Diagnostic & Clinical Data Management

3.5.1.1. The system SHALL provide a robust inbound data processing engine capable of securely ingesting, parsing, validating, and mapping various healthcare data formats (including HL7 v2.x, FHIR, XML, JSON, CSV, and flat files) via standard secure protocols (e.g., SFTP, RESTful APIs, Direct Secure Messaging).

3.5.1.2. The data processing engine SHALL support automated vocabulary translation

(e.g., LOINC, SNOMED CT, ICD-10, RxNorm) and the intelligent routing of Electronic Laboratory Reporting (ELR) and Electronic Case Reporting (eCR) to the appropriate person records, workflows, or exception review queues based on configurable business rules.

3.5.1.3. The system SHALL support validation or testing workflows for ECR-related expressions, mappings, and data extraction logic.

3.5.1.4. The system SHALL apply configurable disease-specific and test-specific reportability, case-creation, case-association, and time-boxing logic.

The following SHALL be used lab collect date, disease condition, organism/subtype, test type, result value, specimen source, reporting facility, jurisdiction, CSTE or CDC case definitions where applicable, and program-defined criteria to distinguish:

reportable from non-reportable results, identify potentially incorrect classifications, determine whether incoming results create new cases or update existing cases, and route ambiguous results for review.

3.5.1.5. The system SHALL support review, batch review, and exception routing of supplemental laboratory results, including whole genome sequencing results and broadly named batch results that cannot be automatically classified to a single disease condition.

3.5.1.6. The system SHALL automatically associate laboratory and supplemental results with appropriate existing cases when criteria are met, display related historical laboratory results and updates relevant to case determination,

3.5.1.7. The system SHALL preserve specimen/test-level provenance including collecting source, sending or intermediary source, performing laboratory, test type, accession/specimen identifiers where available, and multiple tests performed on the same specimen.

3.5.1.8. The system SHALL support manual and non-ELR laboratory reporting pathways, including faxed, out-of-state, provider-reported, reportable website, and other non-electronic sources when partners cannot submit complete ELR or ECR data for all conditions.

3.5.2. Outbound Reporting, Federal Submission & Data Exchange

3.5.2.1. The system SHALL provide standards-based API and web-service integration capabilities for data access, data exchange, endpoint querying, and justified direct interfaces with external systems.

3.5.2.2. The system SHALL support the configuration, creation, validation, and secure transmission of outbound data extracts and messages to federal partners (e.g., CDC, HRSA) and other authorized health information exchanges. This must include native capability to generate, validate, and transmit CDC National Notifiable Diseases Surveillance System (NNDSS) HL7 Message Mapping Guide (MMG) compliant messages, support for legacy NETSS formats where required, and automated data extraction for federal grant reporting.

3.5.2.3. The system SHALL support integration with external federal systems required for program reporting workflows, including eHARS where applicable.

3.5.2.4. The system SHALL support Ryan White federal reporting outputs, including ADR, RSR, and related federal or grant reporting submissions, using required client, service, medication, insurance, funding, clinical, demographic, and reporting-period data.

3.5.2.5. The system SHALL provide traceability from ADR/RSR aggregate outputs back

to the client and service records contributing to each output.

3.5.2.6. The system SHALL validate Ryan White ADR/RSR and related federal report data before submission, including missing, inconsistent, duplicate, out-of-period, or otherwise invalid data.

3.5.2.7. The system SHALL support authorized one-way outbound, inbound, and bidirectional data exchange with tribal epidemiology partners and other trusted external partners according to applicable policy, governance, validation, review, update-approval, reconciliation, and data-sharing agreements.

3.5.3. Data Quality, Validation & Reconciliation

3.5.3.1. The system SHALL feature a configurable data quality engine that automatically applies State-approved validation rules, formatting standards, and terminology mappings (e.g., LOINC, SNOMED) at the point of data entry and ingestion. The engine must actively prevent the submission of critically malformed data, standardize common fields (e.g., address standardization/geocoding), and flag incomplete or inconsistent records for review.

3.5.3.2. The system SHALL provide authorized administrators with a centralized interface management dashboard to monitor the health, throughput volume, and status of all inbound and outbound data feeds in real-time. This capability must include dedicated error-handling queues for reviewing and reprocessing failed, unmapped, or malformed messages, automated alerts for interface outages or volume anomalies, and built-in tools to support the testing, validation, and onboarding of new data senders or receivers.

3.5.3.3. The system SHALL provide dedicated workflows and review queues for data reconciliation, allowing authorized users to efficiently identify, investigate, and resolve data quality exceptions. This includes tools for managing conflicting information from multiple reporting sources, remediating unmapped laboratory results, and performing safe, audited bulk data updates or corrections.

3.5.3.4. The system SHALL ensure strict data integrity by maintaining complete provenance and lineage for all records. This includes maintaining an immutable, time-stamped audit trail of all data modifications, user actions, and automated rule executions.

3.6. Data migration, conversion, archival, and historical access.

The Contractor must provide a data migration, conversion, archival, or historical-access approach that supports the State's transition from the current EDSS environment. The approach must address data profiling, source-to-target mapping, transformation rules, data quality issues, reconciliation, test conversions, validation, exception handling, data-retention expectations, historical access, attachments and documents, audit and provenance considerations, reporting impacts, cutover sequencing, fallback or contingency planning, and final migration acceptance.

The Contractor must clearly describe what data will be migrated into the future EDSS, what data will remain available through archive or reporting access, what data will be excluded, what State remediation or mapping decisions are required, and how migration completeness and accuracy will be demonstrated before go-live.

3.7. Reporting, analytics, dashboards, and data access.

The Contractor must provide reporting, analytics, dashboard, extract, and data-access capabilities necessary to support operational management, investigation workflows, program reporting, federal and State reporting, data quality monitoring, leadership reporting, partner reporting, and authorized analytic use. The Contractor must describe how the solution will

support both in-application reporting and governed access to EDSS-derived data through approved reporting-layer, data warehouse, BI, API, extract, or equivalent mechanisms.

The Contractor must support reporting-ready data structures, data definitions, transformation documentation, lineage, scheduling or refresh processes, security controls, row-level or role-based restrictions where applicable, validation against source records, and sustainable maintenance of reports and datasets over time. The Contractor must identify any limitations on direct data access, database access, API access, export formats, refresh frequency, data volume, or downstream BI tool use.

3.7.1. Self-Service Analytics and Querying

3.7.1.1. The system SHALL empower authorized, non-technical users with intuitive, self-service querying tools. Users must be able to visually build complex, ad-hoc queries filtering across any combination of demographic, clinical, laboratory, and program-specific data elements to generate custom line lists, identify trends, and export results in standard formats (e.g., CSV, Excel) without requiring SQL or specialized programming knowledge.

3.7.1.2. The system SHALL include a native reporting and dashboarding module capable of generating operational metrics, performance tracking, and program-specific summaries. Authorized users must be able to create, save, and share interactive dashboards and scheduled reports that provide real-time visibility into workflow statuses, outbreak metrics, and key public health indicators.

3.7.1.3. The system SHALL provide drill-down from aggregate report counts to underlying case lists and, where authorized, from case lists to individual source records or client/service data used in the reported output.

3.7.1.4. The system SHALL allow data extracts, reporting tables or equivalent analytic access methods to include person-level identifiers, case/event-level identifiers, and joins between person-level data and multiple condition-specific records without relying on demographic matching alone.

3.7.1.5. The system SHALL support Ryan White active-client reporting by allowing users to define reporting periods and generate active-client counts by date range, service category, insurance status, eligibility status, funding source, subrecipient, and comparable reporting periods.

3.7.1.6. The system SHALL support forecasting-oriented visualizations or analytic outputs where configured, including charts, trends, or projections that help authorized public health users anticipate likely future case, outbreak, workload, or resource patterns.

3.7.2. Governed Data Access Layer

3.7.2.1. The system SHALL provide a secure, governed data access layer designed specifically for advanced analytics and Business Intelligence (BI). This layer must present a well-documented, reporting-optimized (denormalized) data structure that allows seamless, secure integration with State-approved enterprise BI and analysis platforms (e.g., Microsoft Power BI, Tableau, SAS, R) via standard connectivity (e.g., ODBC/JDBC, APIs) without impacting the performance of the transactional surveillance system.

3.8. Security, privacy, identity, and audit.

The Contractor must design, implement, document, and support security, privacy, identity, and audit controls appropriate for sensitive public health data, including PHI, PII, confidential communicable disease data, and any other protected or restricted data handled by the EDSS. The Contractor must support role-based access, least-privilege permissions, user provisioning and deprovisioning, single sign-on or identity-provider integration where

required, multi-factor authentication where required, session management, external-user access controls where approved, field- or record-level restrictions where required, audit logging, administrative access controls, and data-governance boundaries.

The Contractor must participate in BIT and State security, privacy, architecture, accessibility, vulnerability, risk, and compliance review processes. The Contractor must provide requested security documentation, diagrams, reports, evidence, remediation plans, incident response information, disaster recovery and continuity information, data protection controls, and other materials required by this RFP, the Security and Vendor Questionnaire, the IT Requirements section, and the final contract.

3.8.1. Audit, Traceability & Data Provenance

3.8.1.1. The system SHALL provide or integrate with data lineage and impact-analysis capabilities that allow authorized technical, reporting, and data-governance users to understand relevant upstream/downstream data relationships, source dependencies, and potential downstream impacts of planned changes.

3.8.1.2. The system SHALL identify the source of incoming data, including ELR, manual entry, fax, disease reporting website, survey import, vital records, reporting facility, intermediary system, interface source, or other available source channel.

3.8.1.3. The system SHALL provide traceability from supported inbound data sources through stored EDSS values to reporting-layer tables and downstream reporting outputs.

3.8.1.4. The system SHALL record and retain disease-history provenance needed to distinguish reinfection, ongoing disease history, and routine titer-check context.

3.8.1.5. The system SHALL maintain audit trails for person merges, known non-duplicate decisions, deduplication review actions, and unmerge capability.

3.8.1.6. The system SHALL provide lineage from aggregate or submitted report outputs back to the contributing client, service, medication, funding, clinical, demographic, file, upload, external source, and source-record values.

3.8.1.7. The system SHALL preserve reporting logic and source data snapshots used for submitted reports and allow authorized users to reproduce prior reports using the same reporting-period logic and data state.

3.8.1.8. The system SHALL maintain audit controls for funding-source changes and for correction, voiding, reversal, or reclassification of service records.

3.8.1.9. The system SHALL enforce access controls that distinguish aggregate data access from case-level data access and restrict person-level cross-condition history, condition relationships, contact relationships, tribal datasets, sensitive program datasets, compartmentalized program areas, dashboards, exports, APIs, and reporting-layer data according to role, program responsibility, jurisdiction, and approved business need.

3.8.1.10. The system SHALL support administrative security and governance reporting on user access, permissions, user actions, audit events, sensitive-data access, inactive users, elevated privileges, external users, and access requiring review.

3.8.1.11. The system SHALL support logical deletion or deletion-flagging of records where deletion is permitted, prohibit unauthorized hard deletion of records, and preserve audit trails and recovery controls for deleted or inactive records, including deletion status, user, timestamp, reason, affected record identifiers, and restoration outcome where restoration is permitted.

3.8.1.12. The system SHALL maintain change history for unknown workflow

dispositions, reference-code routing changes, and administrative configuration changes.

3.8.1.13. The system SHALL support governed data retention, archival, purge, secure destruction, backup-retention, log-retention, and disposition evidence processes for State data, audit logs, and backup copies in accordance with State policy, law, regulation, and approved retention schedules.

3.8.1.14. The system SHOULD support download of audit log information for storage into the state's Security Information and Event Management.

3.8.2. Security, Privacy, Access Control & Compliance

3.8.2.1. The system SHALL provide administrators with clear visibility and troubleshooting tools to determine which users can access specific conditions, regions, workflows, reports, imports, administrative functions, and required permissions for specific tasks.

3.8.2.2. The system SHALL support granular administrative permissions that restrict individual administrative functions and avoid reliance on all-or-nothing super-user access.

3.8.2.3. The system SHALL distinguish users who can view administrative configuration from users who can modify, deploy, or otherwise change administrative configuration.

3.8.2.4. The system SHALL support separation of duties between administrative tasks and, where required, between configuration development, testing, approval, and production deployment.

3.8.2.5. The system SHALL support approval workflows for sensitive administrative actions.

3.8.2.6. The system SHALL maintain audit trails for administrative security changes and technical configuration changes, including the user who made each change and the date and time of the change.

3.8.2.7. The system SHALL enforce role-based access controls for person records, case records, workflows, questionnaires, reporting functions, administrative functions, and program-specific data based on assigned user role and approved program responsibility.

3.8.2.8. The system SHALL restrict user access by condition, program, and region so users cannot view or act on unrelated condition data or data outside their approved responsibilities.

3.8.2.9. The system SHALL support least-privilege access while allowing authorized cross-program backup, support, mapping, and multi-workflow responsibilities without granting unnecessary operational or administrative privileges.

3.8.2.10. The system SHALL support modular, group-based, and hierarchical permission sets that can be assigned by job function, program, condition, region, and administrative responsibility, with clear and predictable cumulative behavior when multiple roles are assigned.

3.8.2.11. The system SHALL support user account lifecycle controls, including inactivation, expiration, optional end dates, duration-based access, deactivation, periodic access review, access termination, and role-change access removal.

3.8.2.12. The system SHALL support secure access for authorized internal users, external users, subrecipient users, external partner users, public users where

applicable, and other non-state users with role-appropriate restrictions, lifecycle controls, and standards-based identity federation such as OpenID Connect or SAML where required by the selected hosting and identity model.

3.8.2.13. The system SHALL support multifactor authentication for user access and provide administrative controls for managing MFA enrollment, account administration, and lifecycle changes.

3.8.2.14. The system SHALL support standards-based single sign-on.

3.8.2.15. The system SHALL control access to reporting databases, reporting-ready tables, dashboards, Power BI datasets, public dashboard datasets, CDC reporting outputs, and data extracts based on user role, approved business need, dataset sensitivity, and reporting purpose.

3.8.2.16. The system SHALL apply governed access controls to geocoded case data, mapping outputs, precise coordinates, aggregate geography-level reporting, and geography-based reporting data based on case privacy, small-number suppression, program policy, tribal data-sharing agreements, legal requirements, and approved business need.

3.8.2.17. The system SHALL apply lifecycle controls for confidential-data transfer locations, including time-limited availability, automatic deletion or cleanup of transfer folders where required, and controls that reduce unnecessary persistence of confidential data in transfer staging locations.

3.8.2.18. The system SHALL enforce secure transport for user and system access, including HTTPS/SSL or equivalent secure web transmission where applicable, use approved encryption for confidential data at rest, in transit, and on portable media where permitted, and support secure file-transfer cryptography aligned with applicable HIPAA, NIST, and State security standards.

3.8.2.19. The system SHALL support emergency break-glass access workflows where authorized by State policy, including elevated access justification, time limitation where applicable, audit logging, post-access review, and appropriate administrative oversight.

3.8.2.20. The system SHALL support security event monitoring, intrusion detection or equivalent unauthorized-access detection, recording and review of attempted unauthorized access or modification, and defined notification and escalation workflows for security events.

3.8.2.21. The system SHALL support applicable State security review, risk assessment, approval, and documentation requirements for the selected hosting model, including vendor-hosted, state-hosted cloud, state-hosted on-premises, SaaS, or hybrid deployment approaches.

3.9. Hosting, environments, operations, and supportability.

The Contractor must provide or support the approved hosting and environment strategy for the future EDSS. The Contractor must describe all proposed hosting models, environments, infrastructure dependencies, cloud or on-premises components, network dependencies, State responsibilities, vendor responsibilities, monitoring, backup, disaster recovery, release management, patching, upgrade management, deployment processes, performance management, and operational support processes.

At a minimum, the implementation must include appropriate non-production and production environments to support configuration, testing, training, security review, migration rehearsal, reporting validation, interface validation, defect resolution, and operational readiness. The Contractor must maintain environment separation and must document controls for production access, data refresh, test data, mock cases, configuration promotion, rollback, and release

management.

3.9.1. Infrastructure, Architecture, Implementation & Support

3.9.1.1. The system SHALL support controlled and auditable movement of approved configuration changes, release artifacts, and appropriate validation data between environments, including phased staging-to-production promotion and production-to-test transfer where appropriate.

3.9.1.2. The system SHALL support separate production, staging/test, and training environments for configuration, testing, deployment, validation, and training activities.

3.9.1.3. The system SHALL clearly identify the environment in which each user is working.

3.9.1.4. The system SHALL provide administrative observability for system configuration, security, reporting database exposure, scheduled jobs, and template deployment.

3.9.1.5. The system SHALL support governed APIs, integration services, interface endpoints, or equivalent integration access patterns that allow authorized systems to exchange or access case data according to approved security and data governance controls.

3.9.1.6. The system SHALL support integration with State-required cloud, geospatial, mapping, census, and equivalent architecture services.

3.9.1.7. The system SHALL support migration of existing EDSS data into the selected deployment architecture while preserving data integrity, historical context, source traceability, reporting continuity, and validation evidence needed for go-live readiness.

3.9.1.8. The system SHALL support the deployment model selected by the State, including SaaS, vendor-hosted cloud, state-hosted cloud, state-hosted on-premises, or hybrid deployment approaches approved for the procurement.

3.9.1.9. The system SHALL support standards-based authentication and secure integration with enterprise identity management tools.

3.9.1.10. The system SHALL support flexible data models capable of representing person-level, event-level, zoonotic, location, exposed-person, outbreak-related, non-infectious disease, clinic, program-specific, and other State-defined public health records where included in scope.

3.9.1.11. The system SHALL support documented infrastructure lifecycle responsibilities for each approved deployment model, including operating system, application platform, database administration, patching, upgrades, monitoring, backup, recovery, maintenance, and related operational support responsibilities.

3.9.1.12. The system SHALL support integration with SQL Server or equivalent reporting database environments and enterprise reporting architecture, including BI tools and reporting databases.

3.9.1.13. The system SHALL preserve South Dakota DOH’s ability to support required CDC, federal, tribal, and external data submission pathways during transition and cutover.

3.9.1.14. The system SHALL support configurable, low-code, or no-code tools for routine administrative functions and routine changes, reducing dependence on custom overlays, custom Java development, or direct XML editing.

3.9.1.15. The system SHALL support implementation approaches that account for

limited program staff capacity, including configuration, testing, migration, validation, and phased refinement for complex program areas.

3.9.1.16. The system SHALL provide modular, upgrade-safe extension and configuration mechanisms that minimize upgrade-blocking customization and unsafe direct manipulation of production-impacting configuration files.

3.9.1.17. The system SHALL support configurable alerting architecture for inactivity, source-volume monitoring, and workflow thresholds.

3.9.1.18. The system SHALL support creation and use of test or mock cases to validate workflows, demonstrations, and training without affecting production data.

3.9.1.19. The system SHALL support parallel validation of required reporting datasets before go-live.

3.10. Testing, quality assurance, and acceptance.

The Contractor must plan, coordinate, execute, support, and document testing activities sufficient to demonstrate readiness for production use. Testing must include, as applicable, configuration testing, system testing, integration testing, interface testing, migration testing, reporting and extract validation, user acceptance testing, regression testing, security testing or remediation validation, performance and volume testing, accessibility testing, cutover rehearsal, and operational readiness validation.

The Contractor must maintain a defect and issue management process, support State review and acceptance of test results, provide evidence that requirements and deliverables have been satisfied, and correct deficiencies before acceptance. A scope item or phase will not be considered complete solely because software has been installed or configured; completion requires accepted deliverables, demonstrated capabilities, resolved or accepted defects, approved documentation, and State acceptance according to the final contract and project governance process.

3.11. Training, change management, and documentation.

The Contractor must provide training, change-support, and documentation sufficient for State users, program users, administrators, technical staff, reporting users, support staff, and approved external users to use, manage, and support the future EDSS. Training may include role-based training, administrator training, technical training, reporting or analytics training, train-the-trainer support, quick reference materials, job aids, recorded sessions, release notes, configuration documentation, interface documentation, and support knowledge-transfer materials.

The Contractor must support readiness activities before go-live, including training completion tracking, user provisioning coordination, help desk or support model preparation, communication materials, business process transition support, and documentation of known changes from current workflows.

3.12. Go-live, cutover, stabilization, and transition to operations.

The Contractor must develop and execute a go-live and cutover approach that protects continuity of surveillance operations. The approach must address final configuration, final migration or archival steps, interface switchover, reporting readiness, user access, downtime or freeze windows, communications, go/no-go criteria, contingency or rollback procedures, issue triage, command-center or hypercare support, and post-go-live stabilization.

The Contractor must support transition to steady-state operations by resolving stabilization issues, completing accepted deliverables, transferring knowledge to State and support teams, confirming support procedures, documenting known limitations, and establishing ongoing maintenance, enhancement, release, and support processes.

3.13. Maintenance, operations, and continuous improvement.

The Contractor must provide ongoing maintenance and support services for the EDSS according to the final contract, service levels, security requirements, and support model. Ongoing services may include incident response, service desk or escalation support, defect correction, patching, security updates, release management, product upgrades, configuration support, interface support, reporting support, performance monitoring, operational monitoring, documentation updates, administrative support, training updates, and support for approved enhancements or change requests.

The Contractor must describe how customizations, configurations, integrations, reports, data structures, security settings, and operational procedures will be maintained over time, including how upgrades and version changes will be assessed, tested, communicated, and implemented without disrupting critical public health operations.

4. Project Deliverables/Approach/Methodology

The offeror must describe in detail how its proposed deliverables will meet the needs of the State as described in Section 3. At its sole discretion, the State may consider a solution that includes any of these deliverables or consider deliverables not originally listed.

An offeror must highlight any requirement in Section 3 or Section 4 that the offeror's proposed deliverables cannot comply with, and the offeror must provide any suggested "work-around" to the requirement in question or a future date that the offeror will be able to comply with the requirement.

4.1. The offeror's proposal must include a:

- Project Management Plan
- Project Schedule
- Risk Management Plan
- Data Conversion Plan, if applicable
- Requirements Traceability Matrix
- Communication Plan
- Testing Plan
- Training Plan
- Go-Live/Cutover Plan
- Post-Implementation Support (or Maintenance and Operations Plan)

In addition, the offeror's proposal must include how its proposed deliverables will meet the following IT requirements (General, State Hosted, and Vendor Hosted). ***If the offeror's proposed solution can be hosted by the offeror or in the State's cloud environment, the offeror must provide a separate response for each proposed solution and how each solution will meet the requirements in Sections 3 and 4.***

4.2. GENERAL IT REQUIREMENTS

4.2.1 Artificial Intelligence Use

The offeror must provide an explanation of its use of Artificial Intelligence, both in its proposed solution and the development lifecycle of the proposed solution.

This requirement includes the offeror's use of Generative AI (GenAI) tools/products. For GenAI tools/products, the offeror must provide the following:

- GenAI model name,
- product owner,
- product description (including purpose, functionality, and key characteristics),
- use case (or goal e.g. image recognition, natural language processing, text summarization),
- the intended information use (context for how information is used in the model) for the GenAI included in the offeror's proposal,
- the geographical location of the tool, and
- how the offeror monitors and audits the tool's compliance on use restrictions, data restrictions, legal compliance (non-discriminatory outputs), and biases in the tool's outputs.

4.2.2 Hosting and Data Access Requirements

The State will own all data tables created as a result of the Agreement. The State must have the ability to manipulate data, run reports as needed, pull code tables, access raw data, and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau, and associated platforms.

The offeror's proposal must describe how the State can access data housed within the proposed solution for ingestion into a state data repository, encompassing available methodologies (e.g., application programming interface (API), flat file), data formatting, frequency of updates, and any inherent constraints. Additionally, the offeror's proposal must provide a high-level architecture diagram, as part of the solution diagram as required by ***Section 6.7***, explaining the proposed solution's data provision mechanism.

If available, the offeror must provide separate, complete proposals for the offeror's proposed solution to be hosted by the offeror, by the State on its internal infrastructure, and on the State's Azure cloud hosted tenant as a PaaS solution. If any of the hosting options is not available, the offeror must clearly state that in the offeror's proposal and provide an explanation as to why the hosting option is not available.

4.2.3 Single Sign-On Requirements

If the offeror's proposal includes a deliverable with a login component, the proposal must describe how the deliverable will integrate with the State's standard identity management service single sign-on (SSO).

The State's SSO supports the industry standard OAuth 2.0 protocol. This identity management will handle password recovery and multi-factor authentication (MFA). MFA is required for all application Administrators and may be required for other users. The State's SSO requirement and links to Microsoft's official documentation can be found at:
https://www.sd.gov/bit?id=bit_standards_single_sign_on

If the offeror is not able to fulfill this identity management standard, the offeror's proposal will be rejected from consideration.

4.2.4 SSO Logout Initiation Requirements

- The offeror's deliverable must provide users with a clear and easily accessible logout mechanism (e.g., a "Logout" button/link).
- The logout functionality of the offeror's deliverable must trigger a session-based logout process utilizing the sign-out endpoint found in the metadata document provided during implementation.

4.2.5 Session Timeout Requirements

- The offeror's deliverables must allow for a customizable, State-defined inactive user session timeout period.
- The offeror's deliverables must notify users of impending session expiration five minutes before the timeout occurs, providing users with the option to extend the session.

4.2.6 Session Termination on Browser Close Requirement

The offeror's deliverables must clearly notify users that closing the browser window or tab is not a valid logout because the SSO session may remain active. The notice must further notify users that they are responsible for explicitly logging out to ensure complete session termination.

4.2.7 Onboarding/Provisioning of Users Requirement

The offeror's proposal must describe how new users are onboarded or provisioned into the deliverable. The offeror must provide an automated process for onboarding and offboarding users or must provide a process that requires minimal manual steps.

4.2.8 Interfaces and Integration Requirements

The offeror's proposal must describe how the deliverables can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, the offeror must make available or expose software services that would enable third-party developers to interface other business applications. The offeror must publish documentation for the software services in question. The offeror's proposal must include a detailed description of system capability.

4.2.9 Web Application Vulnerability Scan Requirements

Any web-based deliverable must undergo a web application vulnerability scan ("Vulnerability Scan"). The Vulnerability Scan must identify misconfigurations or vulnerabilities such as those found in the OWASP Top Ten and must detail the certainty level of each finding.

Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of deliverables that will pass Vulnerability Scans. If the State determines that any aspect of the deliverable has security vulnerabilities that must be corrected, the State will inform the offeror of the nature of the issue and the offeror will be required to respond in writing regarding mitigation plans for the security vulnerabilities. If the deliverable does not pass the initial Vulnerability Scan or the offeror cannot provide a satisfactory Vulnerability Scan report, additional scans may be required to confirm the deliverable is secure.

***State Hosted*:** For state hosted web-based deliverables, the Vulnerability Scan will be performed by the State and the offeror's proposal should take that into consideration when responding to this RFP. As a condition of the resulting contract, the state hosted web-based deliverable will have to successfully pass the Vulnerability Scan prior to the deliverable being allowed to go in a production environment. Any offeror who responds to this RFP must accept such a contract term and must factor this security requirement into the offeror's proposal.

***Vendor Hosted*:** For vendor hosted web-based deliverables, any offeror who makes it to the "Tech Review" stage of the RFP process must provide the State a copy of the full report of the deliverable's most recent Vulnerability Scan, a summary will not be accepted. The offeror should mark the vulnerability report as "Confidential" if it treats such a report as confidential information. If the offeror requires a Non-Disclosure Agreement (NDA) to be in place before the State may review the Vulnerability Scan report, the offeror must notify the State of such a requirement and resolve the signing of an NDA with enough time to respond to this RFP within the timeframe.

The offeror's Vulnerability Scan report must consist of, at a minimum:

- The system that was evaluated,
- The categories that were evaluated (examples: SQLi, XSS, or RCE),
- What were the general findings,
- Technical detail of each issue found,
- Remediation status of enumerated issues (if any).

The cost of any Vulnerability Scans done by the offeror or the offeror's costs associated with the State performing Vulnerability Scans must be part of the offeror's cost proposal. Failure of a deliverable to satisfactorily pass a Vulnerability Scan may result in the offeror's proposal being rejected.

4.2.10 Test System Requirement

The offeror must include a test system for its application deliverables to be used at the discretion of the State. All resource costs, including licensing costs, associated with keeping the test system available must be detailed in

the offeror's cost proposal. If the offeror does not include the test system costs in the offeror's proposal, then the offeror will bear the costs. The offeror will maintain the test system as a mirror image of the production system code base.

4.2.11 Internal Processes and Procedures Requirement

The offeror must use industry standard processes and procedures, such as a software development lifecycle, when planning the development, configuration, implementation, and support of a proposed deliverable. The offeror must outline their internal processes and procedures in their proposal, including, but not limited to, alerting key stake holders (such as: Operations, Systems Support staff, Desktop Support staff, Administrators, Help Desk personnel, Client Representatives, and others) of changes that will be occurring within State or offeror resources or systems.

4.2.12 Email Domain Name Requirement

If the offeror's proposal includes a website or a web application that generates email and is hosted by the offeror or in the State's cloud, the proposed website or web application cannot use state email domains as the originating domain name.

4.2.13 Banned Entity Requirement

The offeror's proposed deliverables cannot include any hardware or hardware components manufactured by Huawei Technologies Company, Nuctech, or ZTE Corporation or any subsidiary or affiliate of such entities. This includes hardware going on the State's network as well as the offeror's network if the offeror's network is accessing the State's network or accessing State data. This includes Infrastructure as a Service, Platform as a Service, or Software as a Service situations. Any company that is considered to be a security risk by the government of the United States of America under the International Emergency Economic Powers Act, in a United States appropriation bill, an Executive Order, or listed on the US Department of Commerce's Entity List will be included in this ban.

4.2.14 Access Management Requirement

If the offeror's proposed deliverables require accounts allowing access to State systems, then the offeror must indicate the number of the offeror's staff or subcontractors that will require access, the level of access needed, and if these accounts will be used for remote access. These individuals will be required to use Multi-Factor Authentication (MFA). The State's costs in providing these accounts will be a consideration when assessing the cost of the offeror's proposal. All costs associated with providing an account to the offeror will be borne by the agency.

4.2.15 Testing Requirements

The following testing may be required:

4.2.15.1 Regression Testing – Regression testing is the process of testing changes to computer programs to make sure that the older programming still works with the new changes.

4.2.15.2 Integration Testing – Integration testing is a software development process which program units are combined and tested as groups in multiple ways. In this context, a unit is defined as the smallest testable part of an application. Integration testing can expose problems with the interfaces among program components before trouble occurs in real-world program execution. Integration testing is also known as integration and testing (I&T).

4.2.15.3 Functional Testing – Functional testing is primarily used to verify that a piece of software is meeting the output requirements of the end-user or business. Typically, functional testing involves evaluating and comparing each software function with the business requirements. Software is tested by providing it with some related input so that the output can be evaluated to see how it conforms, relates or varies compared to its base requirements. Moreover, functional testing also checks the software for usability, such as ensuring that the navigational functions are working as required. Some functional testing techniques include smoke testing, white box testing, black box testing, and unit testing.

4.2.15.4 Performance Testing – Performance testing is the process of determining the speed or throughput of an application. This process can involve quantitative tests such as measuring the response time or the number of MIPS (millions of instructions per second) at which a system functions. Qualitative attributes such as reliability, scalability and interoperability may also be evaluated. Performance testing is often done in conjunction with load testing.

4.2.15.5 Load Testing – Load testing is the process of determining the ability of an application to maintain a certain level of effectiveness under unfavorable conditions. The process can involve tests such as ramping up the number of users and transactions until the breaking point is reached or measuring the frequency of errors at your required load. The term also refers to qualitative evaluation of factors such as availability or resistance to denial-of-service (DoS) attacks. Load testing is often done in conjunction with the more general process of performance testing. Load testing is also known as stress testing.

4.2.15.6 User Acceptance Testing – User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications. UAT is one of the final and critical software project procedures that must

occur before newly developed or customized software is rolled out. UAT is also known as beta testing, application testing or end user testing. In some cases, UAT may include piloting of the software.

4.2.16 Website Requirements

Any website must meet the Web Standards listed in this RFP and as found in the following:

https://www.sd.gov/bit?id=bit_standards_web
https://www.sd.gov/bit?id=bit_standards_vendor_client_sec_req

4.2.17 Web Content Accessibility Guidelines Requirement

The offeror's proposed deliverables must conform to the Web Content Accessibility Guidelines 2.1 Level AA.

4.2.18 Browser Compatibility

The offeror's proposed deliverables must be compatible with supported versions of Edge, Chrome, Safari, and Firefox browsers.

4.3. STATE HOSTED SOLUTIONS (ON-PREM OR STATE CLOUD) REQUIREMENTS

4.3.1 Virtualized Environment Requirement

The offeror should state whether its proposed solution will operate in a virtualized environment. The offeror must identify and describe all differences, restrictions, or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment. This information must be included with the system diagram.

4.3.2 Network Vulnerability Scan Requirement

All deliverables hosted by the State will be subject to a network vulnerability scan by the State.

4.3.3 Load Balancing Requirement

The offeror must state if its proposed deliverables can be load balanced across multiple servers, which is a requirement for an application to operate within the State's computing environment.

4.3.4 Use of Abstraction Technologies Requirement

The offeror must describe how its proposed deliverables use abstraction technologies, which is defined as the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

In addition, the offeror must affirmatively state that its proposed deliverables

do not use hard-coded references.

4.3.5 Non-Standard Hardware and Software Requirement

State standard hardware and software should be utilized unless there is a reason not to. If the offeror's proposal recommends using non-standard hardware or software, the proposal must very clearly indicate what non-standard hardware or software is being proposed and why it is necessary to use non-standard hardware or software to complete the project requirements. The costs of such non-standard hardware or software should be reflected in the offeror's cost proposal. See https://bit.sd.gov/bit?id=bit_standards_overview, for lists of the State's standard hardware and software. The offeror's proposal must include a link to the offeror's hardware and software specifications if one is available or explain why a link is not available. BIT must approve the use of any non-standard hardware or software before a contract can be awarded.

4.3.6 Vendor to State Hosted Transition

If, as part of the proposed project plan, the offeror intends to set up or configure a deliverable outside of State's IT infrastructure, even in part, and then move said deliverable to the State's infrastructure, then the offeror must provide a complete and detailed project plan on how that transition will occur. The offeror's proposal should include any additional time and money considerations for the transition.

4.4. VENDOR HOSTED SOLUTION REQUIREMENTS

4.4.1 General Vendor Hosted Requirements

In the offeror's proposal, the offeror must describe its:

- Data loss prevention methodology;
- Data sanitization methodology and procedures;
- Identity and access management;
- Security intelligence;
- Annual security training and awareness;
- Manual procedures and controls for security;
- Perimeter controls;
- Security certifications and audits.
- Ability to meet HIPAA compliance with a signed business associate agreement

4.4.2 Import and Export of Data Requirement

The offeror's proposed deliverables must allow the State the ability to import or export the State's data piecemeal or in its entirety at the State's discretion without interference from the offeror. The data must be able to be exported in a non-proprietary format and must include information such as metadata (data structure descriptions, data dictionary, and data). The offeror's proposal must describe how this functionality works within its deliverables.

5. Resources

Historically, the most successful projects are those that use the team approach. The team approach utilizes a combination of consultant staff, BIT staff, and Agency staff. Below is a description of how the team will be structured.

5.1 Team Organization: Provide the following information.

5.1.1 Project Organization Chart

List names, job titles (designate vacancies), and the city and state in which individual will work on this project.

5.1.2 List of all Consultants and Subcontractors

List all entities to be used for performance of the services described in this RFP. In the work plan, describe which responsibilities will be assigned to consultants or subcontractors and the city and state in which the consultants or subcontractors are located.

5.2 Project Staffing Roles

The overall project team may be comprised of the following potential project roles. These roles will be based on the size and complexity of the project.

Consultant Project Manager
Who: an employee of the offeror.

Role: Some of the duties performed by the Consultant Project Manager are:

- Plan, organize, and execute the tasks needed to meet project requirements. Identifying and documenting project goals and scope
- Planning and documenting project tasks and schedule
- Planning project kickoff meeting
- Ensuring deliverables are delivered on-time
- Managing project resources
- Effectively communicating with stakeholders
- Eliminating blockers and potential risks
- Documenting project's process using various project management tools
- Ensuring top-quality results and project success
- Responsible for test and training strategies, System Integration Testing, and UAT
- Responsible for Cutover and Transition Plans
- Responsible for Change Management and training documentation

Reports to: The Agency Project Sponsor as part of the project status meetings. When issues arise, this person must be able to make recommendations to the team regarding amendments and changes to the deliverables, schedule, or budget.

Project Security Lead
Who: an employee of the offeror.

Role: Some of the duties performed by the Project Security Lead are:

- Certify in writing the security of each deliverable
- Responsible for the security of the application development, management, and update process throughout the contract period.

Reports to: The Agency Project Sponsor as part of the project status meetings. When issues arise, this person must be able to make recommendations to the team regarding amendments and changes to the deliverables, schedule, or budget.

Agency Project Sponsor

Who: an employee of the Agency for whom the project is undertaken and who is the primary stake holder and the primary risk taker.

Role: Some of the duties performed by the Agency Project Sponsor are:

- Resolves agency resource and priority conflicts
- Approves the Project Charter and/or Plan
- Approving project changes that affect scope, time, and budget
- Holds subordinate managers accountable for their performance
- Direct communication and reporting relationship with the Agency Project Manager.
- Chief advocate for the project
- Keeps the agency team focused on appropriate goals
- Keeps the agency updated with new information
- Holds the project team accountable planning and executing the project
- Holds the team accountable for delivering agreed-upon results

Reports to: Agency leadership.

Agency Project Manager

Who: an employee of the Agency appointed by the Project Sponsor.

Role: Some of the duties performed by the Agency Project Manager are:

- Plans, organizes, and executes the Agency's tasks needed to meet project requirements
- Provides day to day oversight of the project
- Approves consultant payments based on contract language
- Provides direction to Agency employees as well as the Project Steering Team
- Keeps Agency Project Sponsor informed on a weekly basis regarding progress and status of the project

Reports to: The Agency Project Sponsor. When issues arise, this person must be able to make recommendations to the team regarding amendments and changes to the deliverables, schedule or budget.

Project Steering Team

Who: This team consists of at least one member from each impacted departmental area and may include an offeror representative.

Role: Some of the duties performed by the Project Steering Team are:

- Oversee the project in terms of the contract and work order agreements. Specific items of oversight include:
  - What are the deliverables for the State, and are they being met?
  - Is the project on schedule? If not, what are the consequences?
  - Should or can the project be put back on schedule and how will that be done?
  - What expenditures have been made? Is the project on budget? If not, what are the circumstances surrounding it?
- Recommend approval of any scope changes or any changes that affect cost and schedule based on cost benefit to the State

Reports to: Agency leadership.

Authority: Each Project Steering Team member should have authority to make decisions for the member's respective departmental area.

BIT Project Manager
Who: an employee of BIT

Role: Some of the duties performed by the BIT Project Manager are:

- Plan, organize, and execute the BIT tasks needed to meet project requirements
- Coordinate or collaborate with the Agency and Consultant Project Managers to develop a project plan and schedule for the BIT project deliverables
- Manage and report on BIT project deliverables
- Work with BIT management to ensure necessary BIT resources are available to execute the project
- Develop a project communication plan to project stakeholders for BIT project deliverables
- Be in close communication with Agency stakeholders and, when applicable, the Agency and Consultant Project Managers to ensure that all deliverables are met
- Document and communicate BIT project risks, issues, decisions, actions, and change requests with project stakeholders
- Provide executive level project reporting on the BIT project deliverables

Reports to: BIT manager and provides project reporting on BIT project deliverables to stakeholders and others as specified in the communication plan.

5.3 Staff Resumes and References

Resumes and references of key personnel are required as part of the offeror's proposal. Key personnel are considered to be those who are accountable for the completion of one or more major deliverables, has the responsibility of any or all of the total project management, or is responsible for the completion of the project. Provide resume details for all key personnel, including any subcontractors' project leads, by listing the following in the order in which it appears.

- Name
- Title
- Contact Information (telephone number(s), e-mail address)
- Work Address

- Project Responsibilities (as they pertain to this project)
- Percentage of time designated to this project
- Brief listing of work experience in reverse chronological order over the last five years (only provide company name, job title(s)/position(s) held, date started, and date left each position, brief description of job duties, responsibilities, and significant accomplishments)
- RFP Project Experience
- Technical Background relative to this project
- Experience in Similar Projects
- Names of the Similar Projects they were involved in
- Role the person played in the projects similar to this project
- Project Management Experience
- Technical Knowledge
- Education
- Relevant Certifications
- Three Professional References (name, telephone number, company name, relationship to employee)

6. Proposal Submission Requirements

The offeror's proposal should be prepared simply and economically and provide a direct, concise explanation of the offeror's proposal and qualifications. Elaborate brochures, sales literature, and other presentations unnecessary to a complete an effective proposal should not be submitted.

The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories. The State of South Dakota is under no obligation to solicit any information that is not included with the proposal. The offeror's failure to submit all requested information in this RFP may cause an adverse impact on the evaluation of the offeror's proposal. The offeror should respond to each point in Sections 3 and 4 in the order they were presented.

6.1 Use of State Seal Restriction

The offeror's proposal should refrain from using the State of South Dakota State Seal in its proposal. Offerors are cautioned that use of the State Seal in any of its documents is illegal as per South Dakota Codified Law § 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota, or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.*

6.2 Format of Proposal

6.2.1 The offeror's proposal must be submitted pursuant to the requirements of Section 1.5 of this RFP.

6.2.2 The offeror's proposal should be page numbered and should have an index or a table of contents referencing the appropriate page number. Each of the sections listed in Section 6.2.3 should be tabbed or bookmarked.

6.2.3 The offeror's proposal should be prepared using the following headings and, in the order that they are presented below. Please reference the section for details on what should be included in your proposal.

- Statement of Understanding of the Project
- Deliverables
- Project Plan
- IT Requirements
- Required Diagrams (If not a separate document)
- Security and Vendor Questionnaire (If not a separate document)
- Response to the State's Contract Terms
- Corporate Qualifications
- Project Experience and References
- Team Organization and Staff Resumes
- Background Investigations
- Cost (If not a separate document)
- Audited Financial Statement (Upon request)

6.3 Statement of Understanding of the Project

The offeror's proposal must summarize the offeror's understanding of the State's needs as enumerated in Section 3 and the work required to meet those needs ("Executive Summary"). The Executive Summary should include, but not be limited to, the offeror's understanding of the purpose and scope of the project, critical success factors and potential problems related to the project, and the offeror's understanding of the deliverables. The offeror must include their specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements. The Executive Summary should be limited to no more than two pages.

6.4 Deliverables

The offeror's proposal must include a Deliverables section which constitutes the major portion of the work to be performed. The offeror's Deliverables section must include a complete narrative detailing the assessment of the work to be performed, approach and methods to provide the requirements of this RFP, the offeror's ability to fulfill the requirements of this RFP, the offeror's approach, the resources necessary to fulfill the requirements, project management techniques, specialized services, availability to the project locale, familiarity with the project locale, and a description of any options or alternatives proposed. The offeror's Deliverables section should address each evaluation requirement enumerated in Section 8. If the offeror has an alternative methodology or deliverable it would like to propose to meet the needs of the State,

please include a detailed description of the alternative methodology or deliverables and how the alternative options will meet or exceed the requirements of this RFP.

6.5 Project Plan

The offeror's proposal must provide a project plan that indicates how the offeror will complete the required deliverables and services and addresses the following:

- Proposed project management techniques
- Number of offeror's staff needed
- Tasks to be performed (within phase as applicable)
- Number of hours each task will require
- Deliverables created by each task
- Dates by which each task will be completed (dates should be indicated in terms of elapsed time from project inception)
- Resources assigned to each task
- Required state agency support
- Show task dependencies
- Training (if applicable)

Microsoft Project is the standard scheduling tool for the State of South Dakota. The schedule should be a separate document, provided in Microsoft Excel, and submitted as an attachment to your proposal.

6.6 IT Requirements

The offeror's proposal must highlight any requirement in Section 4 that the offeror's proposed deliverables cannot comply with, and the offeror must provide any suggested "work-around" to the requirement in question or a future date that the offeror will be able to comply with the requirement.

6.7 Required Diagrams

6.7.1 ***System Diagram***. The offeror's proposal must include a system diagram which must provide specific details so that the State can understand the components, the system flow, and system requirements. The offeror must provide a system diagram for each hosting option. It is preferred that the diagram be provided as a separate document or attachment. The file must be named "(Your Name) System Diagram and Requirements." If the offeror elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

6.7.2 ***Solution Diagram.*** The offeror's proposal must include a solution diagram which must provide specific details on how the offeror's proposed deliverables will meet the requirements of this RFP. The solution diagram must include integration with the State's infrastructure; existing systems that will integrate with the proposed deliverables; how data would flow between systems; all components, tools, and products the proposed deliverables will utilize, the technology stack of the proposed deliverables including any dependencies;

and include, but not be limited to, user onboarding/provisioning and SSO.

6.8 Security and Vendor Questionnaire

The offeror must submit a completed Security and Vendor Questionnaire, which is attached to this RFP as Appendix B, for each proposed deliverable. The offeror must complete a Security and Vendor Questionnaire for each hosting option proposal. The Security and Vendor Questionnaire will be used in the proposal evaluation. The offeror must complete the Security and Vendor Questionnaire in the Microsoft Word format as it is provided to the offeror.

6.9 Response to the State's Contract Terms

The offeror's proposal must indicate any issues the offeror has with specific contract terms found in Section 2 and Appendix A. If the offeror does not indicate that there is an issue with a specific contract term, then the offeror will be deemed to have accepted the contract terms as written.

6.10 Corporate Qualifications

6.10.1 Offeror Company Information

The offeror's proposal must include responses to the each of the following questions:

- What year was your firm established?
- What is your firm's website?
- Has your firm ever done business under a different name and if so, what was the name?
- How many employees does your firm have?
- How many employees in your firm are involved in this type of project?
- How many of those employees are involved in on-site project work?
- Has your firm ever done business with other governmental agencies? If so, please provide references.
- Has your firm ever done business with the State of South Dakota? If so, please provide references.
- Has your firm ever done projects that are exactly like or similar to this project?
- How many clients are currently using your proposed solution? How many of those clients are public sector: local, state, and federal?

6.10.2 Offeror Parent Company

If the offeror has a parent company, the offeror's proposal must include responses to the following questions:

- What is the name of your parent company?
- What year was your parent company established?
- What is your parent company's website?
- What is the business of your parent company?
- What is the total number of employees in the parent company?

- What are the total revenues of your parent company?
- How many employees of your parent company have the skill set to support this effort?
- How many of those employees are accessible to your organization for active support?
- What percent of your parent company's revenue (if applicable), is produced by your firm?

6.11 Project Experience and References

The offeror's proposal must provide details about the four most recent projects that the offeror was awarded and managed through to completion. If the offeror cannot provide four examples, the offeror must explain why it cannot provide four examples and must provide as many examples as possible. These most recent projects will serve as references. Project examples must include the following information (if available):

- Client Name
- Client Address, including City, State and Zip Code
- Client Contact(s), including ***Name***, ***Title***, ***Telephone Number***, and ***E-mail Address***.
- Project Start Date and Completion Date
- Estimated Project Timeframe and Actual Project Timeframe (if actual timeframe is greater than estimated, please provide an explanation)
- Project Description and Goals
- Offeror's Role in Project
- Offeror's Responsibilities
- Offeror's Accomplishments
- Description of How Project Was Managed
- Estimated Project Cost and Actual Project Cost (if actual costs exceed estimated costs, please provide an explanation)
- Description of special project constraints, if applicable
- Description of offeror's ability and proven history in handling special project constraints
- Description of all changes to the original plan or contract that were requested (describe which changes were completed)
- Description of how change requests were addressed or completed by offeror
- Was there any litigation or adverse contract action regarding contract performance? (If "Yes" provide explanation)
- Feedback on offeror's Work by Client
- Offeror's Statement of Permission for the State to contact the Client and for the Client's contact(s) to release information to the State

6.12 Team Organization and Staff Resumes

In this subsection, the offeror's proposal must provide the requested information and identify the individuals who will fulfill the roles for the offeror found in ***Section 5 Resources***.

6.13 Background Investigations

The offeror must include the following statement in its proposal:

(Company name here) acknowledges and affirms that it understands that the (company name here) employees who have access to production Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), any information defined under state or federal statute as confidential or have access to secure facilities will have fingerprint-based background investigations. These background investigations will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation's records. (Company name here) acknowledges and affirms that this requirement will extend to include any subcontractors, agents, assigns, and affiliated entities.

6.14 Cost

In this subsection, the offeror's proposal must provide the requested information in ***Section 7 Cost Proposal***.

The project plan and the costs stated in ***Section 7 Cost Proposal*** must include service desk and support, since BIT can only guarantee best effort support for on-prem vendor proposed solutions. If any software development may be required in the future, hourly development rates must be stated in the offeror's proposal and ***Section 7 Cost Proposal***. The project plan must include the development and implementation of a disaster recovery plan since vendor hosted solutions will not be covered by the State's disaster recovery plan and must be reflected in the costs.

6.15 Audited Financial Statements

Upon the State's request, the offeror may be required to submit a copy of its most recent audited financial statements.

7. Cost Proposal

Cost will be evaluated independently from the technical proposal. The offeror must submit a cost proposal for each hosting proposal. Each of the offeror's proposals must include all costs related to the required services, including all third-party software licenses the State is expected to pay. If available, the offeror must submit a cost proposal for a vendor-hosted solution, a cost proposal for a state-hosted on-prem solution, and a cost proposal for a State cloud-hosted PaaS solution if applicable, or a combination of the three hosting options.

The offeror must submit a statement in the offeror's proposal that attests the offeror's willingness and ability to perform the work described in this RFP for the price being offered.

The cost proposal must provide complete, transparent, and comparable pricing for the offeror's proposed EDSS solution and related services. The cost proposal must align with the offeror's technical proposal and Vendor Questionnaire, project plan, staffing plan, hosting response, interface and integration response, data migration approach, reporting and analytics approach, support model, proposed exceptions, assumptions, and proposed contract terms.

The offeror must include all costs necessary to deliver, operate, support, maintain, and transition the proposed solution for the base scope described in this RFP. Costs that are required to meet the offeror's proposed solution, required services, security obligations, implementation approach, environments, integrations, migration, reporting, training, testing, go-live, stabilization, maintenance, support, or transition obligations must not be omitted from the base cost unless clearly identified as optional or separately priced scope.

The offeror must clearly identify fixed costs, recurring costs, one-time implementation costs, subscription or license costs, hosting or infrastructure costs, third-party costs, optional costs, travel costs, hourly or rate-card costs, and any assumptions or dependencies that may affect total cost. The offeror must state whether pricing is fixed, not-to-exceed, time-and-materials, usage-based, volume-based, transaction-based, tiered, optional, or subject to escalation.

If, as part of the project, the State will be acquiring the right to use vendor or third-party software, the offeror's proposal must clearly state if the software license is perpetual or a term license. If both are options, the offeror's proposal should clearly say so and state the costs of each type of license separately.

7.1. Staffing

The cost proposal must identify professional services costs by role, phase, activity, estimated hours, labor category, rate, and pricing basis. Staffing costs must align with the proposed project organization, staffing matrix, implementation schedule, deliverables, interface and migration workload, reporting and analytics workload, training approach, security review, go-live support, stabilization period, and ongoing support model.

If the offeror proposes subcontractors, specialty consultants, offshore or remote resources, shared resources, optional subject-matter experts, or surge staffing, those costs must be identified clearly. The offeror must identify which rates apply to implementation work, post-implementation support, enhancement work, additional interfaces, reporting requests, configuration changes, emergency support, and future development or change-order work.

Name	Role	Total Hours on Project	Total Hours on Site	Hourly Rate	Total
				Total:	

7.2. Travel and Expenditure Table

Name	Method of Travel	Cost per trip	Number of Trips	Total Cost
			Total:	

Name	Lodging Cost per night	Number of Nights	Lodging Cost	Per diem	Number of Days	Per diem Cost	Total Cost
Totals:							

NOTE: The State asks that vendors accept state per diem. Lodging and per diem rates can be found at https://bhr.sd.gov/files/travelrates.pdf.

Travel costs must be identified separately from labor, licensing, hosting, and other services. The offeror must state whether travel is included in fixed implementation pricing, proposed as not-to-exceed reimbursement, excluded unless separately authorized, or subject to State travel policies. Travel assumptions must identify anticipated on-site activities, number of trips, number of travelers, duration, purpose, and whether travel is required for discovery, design, testing, training, demonstrations, go-live, stabilization, governance meetings, or executive briefings.

7.3. Other Costs

Show any other costs such as: software, hardware, ongoing costs, etc.

If costs vary based on user counts, roles, organizations, jurisdictions, programs, diseases/conditions, message volume, case volume, storage volume, environments, interfaces, APIs, reports, dashboards, data feeds, external users, support tiers, service levels, or hosting model, the offeror must describe the pricing metric, assumptions, included thresholds, overage charges, and escalation triggers.

	One Time	Year 1	Year 2	Year 3	Totals
Hardware					
Software					
Maintenance					
License Fees					
Training					
Other					
Totals					

7.4. Additional Work

The offeror may be expected to perform additional work as required by any of the State signatories to a contract. This work can be made a requirement by the State before allowing the application to go into production. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third-party technologies, or excessive resource consumption. The cost for additional work should be included in the offeror's proposal.

8. Proposal Evaluation and Award Process

8.1. After determining that a proposal satisfies the mandatory requirements stated in this RFP, the State will use subjective judgment in conducting a comparative assessment of all qualified proposals by considering each of the following criteria:

8.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;

8.1.2 Ability of the offeror and the offeror's deliverables to meet all applicable IT requirements, as outlined in Section 4;

8.1.3 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

8.1.4 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

8.1.5 Availability to the project locale;

8.1.6 Familiarity with the project locale;

8.1.7 Proposed project management techniques;

8.1.8 Ability and proven history in handling special project constraints;

8.1.9 Approval by BIT, who provides an "approved" or "disapproved" assessment of an offeror's proposal; and

8.1.10 Cost.

8.2. Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

8.3. The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

8.4. The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

8.5. Award. The State and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

8.5.1 If the State and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the State, the State shall, either orally or in writing, terminate negotiations with the offeror. The State may then negotiate with the next highest ranked offeror.

8.5.2 The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached, or the agency terminates the contracting process.

9 Best and Final Offers

The State reserves the right to request best and final offers; best and final offers cannot be initiated by an offeror. Best and final offers may not be necessary if the State is satisfied with the proposals received.

If best and final offers are sought, the State will document which offerors will be notified and provide them an opportunity to submit best and final offers. Requests for best and final offers will be sent stating any specific areas to be covered and the date and time in which the best and final offer must be returned. Conditions, terms, or price of the proposal may be altered or otherwise changed, provided the changes are within the scope of the RFP and instructions contained in the request for best and final offer. If an offeror does not submit a best and final offer or a notice of withdrawal, the offeror's previous proposal will be considered that offeror's best and final offer. After best and final offers are received, final evaluations will be conducted.

Appendix A – Included I/T Contract Terms and Conditions

Appendix B – Security and Vendor Questions