STATE OF SOUTH DAKOTA
BUREAU OF INFORMATION AND TELECOMMUNICATIONS
700 GOVERNOR'S DRIVE
PIERRE, SOUTH DAKOTA 57501

Acquisition of IT Cloud Platform Technology Services

PROPOSALS ARE DUE NO LATER THAN
March 6, 2023 (5:00PM CST)

RFP #: 23RFP8393
BUYER: Bureau of Information and Telecommunication (BIT)
EMAIL: harold.bruce@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:

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

1.2.1 Background:

The State of South Dakota uses, or will use, Cloud Platform technologies to meet the business needs of State Agencies. The Cloud Platform technologies include but are not limited to: Platform as a Service (PaaS), Software as a Service (SaaS), Integration Platform as a Service (iPaaS) and Infrastructure as a Service (IaaS).

1.2.2 Goals and Objectives:

On behalf of the State of South Dakota, the Bureau of Information and Telecommunications (BIT) is initiating this RFP to obtain a list of qualified vendors who can expand and enhance the State's existing cloud platform technologies by providing consulting and implementation services and by providing additional cloud platform technologies. BIT anticipates that as a result of this RFP, there will be multiple winning vendors. The selected winning vendors will sign a Master Service Agreement with BIT. As IT cloud platform technology services are needed by state agencies, the state agency may request a cost proposal from a qualified vendor or bids from several qualified vendors for the needed services. The selected qualified vendor will enter into a job specific Statement of Work (SOW) with the state agency for the needed services.

1.2.3 Description of Components:

The cloud platform technology services required partner certification/designation levels, modules/services, and skills/rolls potentially desired are listed in the following tables:

Cloud Platform: ServiceNow **Partner Designation: Premier, Elite, or Global Elite Partner**
Products to include, but are not limited to: • App Engine • Automation Engine • Customer Service Management • Enterprise Asset Management • Field Service Management • Financial Services Management • Governance, Risk, and Compliance • Healthcare and Life Sciences Service Management • HR Service Delivery • Integration Hub • IT Assess Management • IT Operations Management

- IT Service Management
- Legal Service Delivery
- Manufacturing Connected Workforce
- Operational Technology Management
- Order Management
- Order Management for Technology Providers
- Order Management for Telecommunications
- Procurement Service Management
- Public Sector Digital Services
- Security Operations
- ServiceNow Platform Encryption
- ServiceNow Vault
- Strategic Portfolio Management
- Supplier Lifecycle Management
- Technology Provider Service Management
- Telecommunications Network Inventory
- Telecommunications Service Management
- Telecommunications Service Operations Management
- Workplace Service Delivery

Skills and/or Roles to include, but are not limited to:

- Engagement Manager
- Scrum/Project Manager
- Business Analyst
- User Experience and Graphics Specialist
- ServiceNow Technical Consultant
- ServiceNow Solution/Technical Architect
- ServiceNow Developer
- ServiceNow Technical Trainer
- ServiceNow Security Engineer/Architect

Cloud Platform: Azure and Power Platform
Partner Competencies: Gold Competencies related to items below

- Microsoft Dynamics 365
- Microsoft Power Apps
- Microsoft Power Automate
- Microsoft Power BI Services
- Microsoft Azure Services

Skills and/or Roles to include, but are not limited to:

- Engagement Manager
- Scrum/Project Manager
- Business Analyst
- Microsoft Dynamics 365 Developer
- Microsoft Power Apps Developer
- Microsoft Power Automate Developer
- Microsoft Power BI Development
- Azure Data Engineer
- Azure Platform Architect
- Azure Platform Security Engineer
- Azure Platform Automation Architect

The total dollar amount for all SOWs entered into as a result of this RFP Cannot Exceed **$25 million**.

There is no guarantee of work. Specific SOWs to acquire professional services for cloud platform technology services with job specific terms and conditions and scopes of work will be created on an as needed basis.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

BIT is the issuing office for this document and all subsequent addenda relating to it. The reference number for the transaction is RFP# 23RFP8393. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.3 LETTER OF INTENT

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

The Letter of Intent may be submitted to Harold Bruce via email at harold.bruce@state.sd.us. Please place the following in the subject line of your email: **"Letter of Intent for RFP# 23RFP8393"**.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication **01/30/2023**
Letter of Intent Response Due (5:00PM CST) **02/13/2023**
Deadline for Submission of Written Inquiries (5:00PM CST) **02/20/2023**
Responses to Offeror Questions (5:00PM CST) **02/27/2023**
Proposal Submission (5:00PM CST) **03/06/2023**
Evaluation of Proposals **04/03/2023**
Anticipated Award Decision/Contract Negotiation **04/10/2023**

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received by BIT by the date and time indicated in the Schedule of Activities.

Each Offeror must provide BIT an electronic version of the proposal. The electronic version should be provided in MS WORD or in PDF format to harold.bruce@state.sd.us. The email, including attachments, must be limited to 10MB in size.

All proposals must be signed by an officer of the Offeror, legally authorized to bind the Offeror to the proposal. Proposals that are not properly signed may be rejected. To facilitate the electronic signature of proposals, Offerors shall provide the email address of the officer legally authorized to bind the Offeror to the proposal **by 5:00PM CST, March 3, 2023**. If Offerors do not wish to sign electronically, the first page of the RFP must accompany the proposal submission, completed, and signed.

No proposal shall be accepted from, or no contract or purchase order shall 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 are 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 bidder shall attach an explanation to their 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 its proposal, the Offeror certifies it does not discriminate in its employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin, or disability.

1.8 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.

1.9 OFFEROR INQUIRIES

All written questions should be sent to: harold.bruce@state.sd.us. Only emailed questions will be accepted.

Offeror may submit email questions 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# 23RFP8393". The questions and their answers will be provide via the State of South Dakota's Bureau of Administration Central Bid Exchange website before the proposal submittal date and will be sent by the date and time indicated in the above Schedule of Activities. 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.

1.10 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. Service elements are not considered proprietary. 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.

1.11 LENGTH OF CONTRACT

The contract will begin on the date the last signature is applied a MSA.
The contract will end on June 30, 2025.
The State has the right to extend the terms of the contract for a period of two years. There is the possibility of up to four (4) extensions. Any extension of the contract will not be automatic.

1.12 RESTRICTION OF BOYCOTT OF ISRAEL

For contractors, vendors, suppliers, or subcontractors with five or more employees who enter into a contract with the State of South Dakota that involves the expenditure of $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.

1.13 RESTRICTION OF 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 Executive Order 2023-02. 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.

1.14 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.

1.15 NEGOTIATIONS

This process is a Request for Proposal/Competitive Negotiation process. Each proposal shall be evaluated, and each Offeror must be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any component of each 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.

2.0 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, along with any additional terms and conditions as negotiated by the parties. The Offeror should indicate in its response any issues it has with specific contract terms if the Offeror does not indicate that there are any issues with any contract terms then the State will assume those terms are acceptable to the Offeror.

2.1 The State hereby enters into this MSA for services with the Vendor in consideration of and pursuant to the terms and conditions set forth in this MSA.

Section I. Scope of Work

A. During the Term of the Agreement, the Vendor agrees provide services to the State of South Dakota and its agencies to maintain and enhance the State's existing technical staff and expertise. On an as needed basis, the Vendor may enter into a Statement of Work (SOW) with a state agency to augment the State's existing technical staff to meet the agency's maintenance and development needs. A project's SOW will include the scope of work for that unique project and it will include additional terms and conditions based upon the unique nature of the project.

B. Additional exhibits within this MSA attached to this MSA and incorporated by reference include:

1. **Appendix A: Certificate of Media Sanitation for Offsite Data**
2. **Appendix B: Information Technology Security Policy – BIT Version**
3. **Appendix C: Security Acknowledgment Form**
4. **Appendix D: Certification re Prohibited Entity**

Section II. Term of Agreement

The "Term of the Agreement" will commence on the date the last signature is applied to this MSA and terminate on June 30, 2025, unless sooner terminated pursuant to Section XI. The Parties will have the option to renew this MSA for four (4) additional two-year periods under the same terms and conditions unless amended by mutual agreement of the Parties pursuant to Section XXIV. At a

minimum, renewal is contingent upon satisfactory performance of the contract by the Vendor as determined by the State. If the State wishes to renew this MSA, the State will provide a written Request to Renew to the Vendor no less than 90 days prior to the end of the current MSA term. Once a Request to Renew is provided to the Vendor, a written renewal agreement must be executed by the Parties; otherwise this MSA will terminate through expiration of its current MSA term. If the Vendor does not wish to renew this MSA or intends to increase the fees of any SOW, the Vendor must provide the State with 180 days' written notice. The preceding notice requirement is not applicable if the increase in fees was previously negotiated by the Parties.

Section III. Fees and Payment

The Vendor and the agency in need of services will negotiate fees and payment terms and conditions and incorporate them into each unique SOW. The State or its agencies will not pay the Vendor's expenses as a separate item. Payments will be made pursuant to itemized invoices submitted with a signed state voucher. Payments will be made consistent with SDCL ch. 5-26. The TOTAL AGREEMENT AMOUNT of all SOWs entered into as a result of this MSA cannot exceed $25 million.

Section IV. Employer Identification Number

The Vendor will provide the State with a Certificate of Authority issued from the South Dakota Secretary of State upon execution of this MSA. When the Vendor executes a SOW with a state agency, the Vendor agrees to provide the state agency with its Employer Identification Number, Federal Tax Identification Number, or Social Security Number.

Section V. Property

When providing services pursuant to a SOW, the Vendor may use some state equipment, supplies, and facilities. In its sole discretion, the State may provide the Vendor limited office space, meeting space, secretarial support, or phone, fax, or copying service during the term of a SOW. The terms and conditions of use of state property or services will be enumerated within a SOW.

Section VI. Indemnification

The Vendor agrees to indemnify and hold the State of South Dakota and its officers, agents, and employees harmless from and against all actions, suits, damages, liability, or other proceedings that may arise as the result of entering into this MSA and any SOW, including but not limited to any claim alleging infringement or any patent, copyright, trade secret, or other intellectual property right. This section does not require the Vendor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State or its officers, agents, or employees.

Section VII. Professional Services Quality and Originality Warranties

The Vendor represents and warrants that all professional services provided pursuant to a SOW will be performed in a professional and workmanlike manner. The Vendor further represents and warrants that the deliverables of any SOW will be its own original work, without incorporation of software, text, images, or other assets created by third parties, except to the extent that the State consents to such

incorporation in writing.

Section VIII. Remedies for Breach of Professional Services Warranties

In the event of a breach of the warranty granted in Section VII of this MSA, the Vendor, at its own expense, will promptly re-perform the professional services in question. The preceding sentence, in conjunction with the State's right to terminate this MSA and a SOW for breach where applicable, states the State's sole remedy and the Vendor's entire liability for breach of the warrant granted in Section VII.

Section IX. Independent Contractor

The Parties are independent contractors and will so represent themselves in all regards. Neither Party is the agent of the other, and either may make commitments on the other's behalf. The Parties agree that no Vendor employee or contractor will be an employee of the State. The Vendor will be responsible for all employment rights and benefits of the Vendor employees, including without limitation: federal, state, and local income and employment taxes and social security contributions; workers' compensation, health benefits, vacation pay, holiday pay, profit sharing, retirement, pension, disability benefits, and other health and welfare benefits, plans, or programs; and insurance.

Section X. Reporting

The Vendor agrees to report to the State any event encountered during the Term of the Agreement which results in injury to the person or property of any third party, or which may otherwise subject the Vendor or the State of South Dakota or its officers, agents, or employees to liability. The Vendor will report any such event to the State immediately upon discovery.

The Vendor's obligation under this section will be to report the occurrence of any event to the State and to make any other report provided for by its duties or applicable law. The Vendor'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 Vendor to report any event to law enforcement or other entities under the requirements of any applicable law.

Section XI. Termination

A. This MSA or any SOW may be terminated by either Party upon 30 days written notice.

B. If the Vendor breaches any term or condition of this MSA or any SOW, the State may terminate this MSA or applicable SOW at any time with or without notice. If the State terminates this MSA or a SOW for a breach by the Vendor, any payments due to the Vendor at the time of termination may be adjusted to cover any additional costs to the State as a result of the breach. If the State exercises its right of termination pursuant to this subsection and it is determined that the Vendor was not at fault for the breach or a breach did not occur, the State agrees to pay the Vendor for eligible services rendered and expenses incurred up to the date of termination.

C. Alternatively, the State retains the discretion to provide the Vendor the opportunity to cure a breach of this MSA or applicable SOW. If the State exercises its discretion, the State will provide the Vendor notice of its opportunity to cure the breach. If the breach remains unresolved after three days, the State may require the Vendor to send at least one qualified and knowledgeable representative to the State's site where the system in question is located. The representative will continue to work towards a resolution of the breach. The Vendor will bear all costs associated with curing the breach. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this MSA, the applicable SOW, or by law.

D. Upon termination of this MSA or a SOW, the Vendor acknowledges the State's right to take over the work or may award the work to another party.

Section XII. Confidentiality of Information

A. **Definition:** "Confidential Information" includes all information disclosed by the State to the Vendor, including but not limited to: names, social security numbers, employee numbers, addresses, other data about applicants, employees, and clients to whom the State provides services of any kind, and any other nonpublic, sensitive information disclosed by the State. Notwithstanding the foregoing, Confidential Information does not include information that:
   1. was in the public domain at the time it was disclosure;
   2. was known to the Vendor without restriction at the time of disclosure by the State;
   3. The Vendor received written approval by the State to disclose;
   4. was independently developed by the Vendor without the benefit or influence of the State's information; or
   5. becomes known to the Vendor without restrictions from a source not connected to the State.

B. **Nondisclosure:** The Vendor will not use Confidential Information for any purpose other than to facilitate the transactions contemplated by this MSA or an applicable SOW ("Purpose"). The Vendor will not disclose Confidential Information to:
   1. any employee or contractor of the Vendor unless such person needs access in order to facilitate the Purpose and executes a nondisclosure agreement with the employee or contractor with terms no less restrictive than those of this MSA or an applicable SOW; and
   2. any other third party without the State's prior written consent.

   Without limiting the generality of the foregoing, the Vendor must protect Confidential Information with the same degree of care it sues to protect its own confidential information of similar nature and importance, but with no less than reasonable care. Vendor must promptly notify the State of any misuse or misappropriation of Confidential Information that comes to the Vendor's attention. Notwithstanding the foregoing, the Vendor may disclose Confidential Information as required by applicable law or by proper legal or governmental authority. The Vendor must give the State prompt notice of any such legal or governmental demand and reasonably cooperate with the State in any effort to seek a protective order or otherwise to contest such required disclosure, at the State's expense.

C. **Injunction, Termination, and Retention of Rights:**
   1. *Injunction.* The Vendor agrees that breach of this Section XII would cause the State irreparable injury, for which monetary damages would not provide adequate compensation, and that in addition to any other remedy, the State will be entitled to injunctive relief against such breach or threatened breach, without proving actual damage or posting a bond or other security.
   2. *Return upon Termination.* Upon termination of this MSA or an applicable SOW, the Vendor will return all copies of Confidential Information to the State or certify, in writing, the destruction thereof.
   3. *Retention of Rights.* This MSA or an applicable SOW does not transfer ownership of Confidential Information or grant a license thereto. Except to the extent that another section of this MSA or an applicable SOW specifically provides to the contract, the State will retain all right, title, and interest in and to all Confidential Information.

Section XIII. State Data

A. **Data Location:** The Vendor agrees to provide its services to the State and access and storage of State data solely from data centers in the continental United States. The Vendor will not provide or allow access to State data to any person or entity outside the continental United States without prior written permission from the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

B. The Vendor will not allow its employees or subcontractors to store State data on portable devices, including personal computers, except for devices that are password protected, encrypted, and used and kept only at the Vendor's data centers. The Vendor may allow its employees or subcontractors to access State data remotely only as required to provide technical support or to fulfill the terms of this MSA or an applicable SOW. If the State data in question includes data that is legally protected or considered sensitive by the State, then remote access is only allowed if:
   1. the device used to remotely access the data must be password protected;
   2. multifactor authentication must be used;
   3. the data is encrypted to at least AES 256 both in transit and in storage;
   4. the data is not transferred to mobile media;
   5. no non-electronic copies are made of the data;
   6. the Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed; and
   7. the State's Data Sanitization policies are followed when the data is no longer needed on the device used to access the data remotely.

C. **Data Protection:** Protection of personal privacy and data will be an integral part of the business activities of the Vendor to ensure there is no inappropriate or unauthorized use of State data at any time. To this end, the Vendor must safeguard the confidentiality, integrity, and availability of State data and comply with the following conditions:
   1. The Vendor must implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI),

Federal Tax Information (FTI), or any information that is confidential under federal or state law. Such security measures will be in accordance with recognized industry practices and not less protective than the measures Vendor applies to its own non-public data.

2. At no time will any State data be copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.
3. The Vendor will not use State data for the Vendor's own benefit and will not engage in data mining of State data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.

D. **Non-Disclosure and Separation of Duties:** The Vendor will enforce separation of job duties and require non-disclosure agreements of all employees that have or can have access to State data or the hardware that State data resides on. The Vendor will limit staff knowledge to those staff whose duties require them to have access to State data or the hardware State data resides on.

E. **Securing of Data:** All facilities used to store, and process State data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Vendor warrants that all State data will be encrypted in transmission (including via web interface) and in storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

F. **Lost or Damaged Data Liability:** If State data is lost or damaged as a result of any failure by the Vendor, its employees, or its agents to exercise reasonable care to prevent such loss or damage, then the Vendor's liability will not exceed the reasonable cost of reproducing the lost or damaged data. The Parties agree this limitation of liability will trump any limitation of liability found in a SOW as it relates to lost or damaged State data.

G. **Rights and License in and to State Data:** The Parties agree all rights, including all intellectual property rights, in and to State data will remain the exclusive property of the State, and the Vendor has a limited, nonexclusive license to use the data as provided in this MSA or a SOW solely for the purpose of performing its obligations hereunder. This MSA or a SOW does not give a Party any rights, implied or otherwise, to the other's data, content or intellectual property, except as expressly stated in this MSA or the SOW.

H. **Continued Access to State Data:** The Vendor agrees it will not hinder the State's access to the State data if there is a contract dispute between the Parties, if there is a billing dispute between the Parties, or if the Vendor merges with or is acquired by another entity. In addition, the Vendor must maintain all security requirements and disaster recovery commitments of this MSA and any active SOW during such incidents.

I. **Legal Requests for State Data:** Except as otherwise expressly prohibited by law, the Vendor will:

1. immediately notify the State of any subpoenas, warrants, or other legal order, demand, or request received by the Vendor seeking State data;
2. consult with the State regarding the Vendor's response to the order, demand, or request;
3. cooperate with the State in efforts by the State to intervene and quash or modify the order, demand, or request; and

4. provide the State with a copy of the order, demand, or request and the Vendor's proposed or actual response to the order, demand, or request.

J. **eDiscovery:** The Vendor will notify the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to State data. The Vendor agrees to not respond to service of process and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

K. **Data Sanitization:** At the end of a project covered by a SOW, the Vendor is responsible for returning all State data to the State or securely disposing of all State data in all forms, which can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of National Institute of Standards and Technology (NIST) Special Publication 800-88. The Vendor must complete and provide to the State point of contact a completed Certificate of Sanitization for Offsite Data, attached to this MSA as Appendix A. The State will review the completed Certificate. If the State is not satisfied by the data sanitization, then the Vendor will use a method that does satisfy the State.

Section XIV. Security Processes

The Vendor will disclose its non-proprietary security processes and technical limitations to the State so adequate protection and flexibility can be attained between the State and the Vendor, e.g. virus checking and port sniffing.

Section XV. Password Policies

Password policies for the Vendor's employees will be documented annually and provided to the State to ensure adequate password protections are in place. Logs and administrative settings will be provided to the State upon request to demonstrate such policies are actively enforced. The process used to reset a password must include security questions or Multi-factor Authentication.

Section XVI. Adverse Event

For purpose of this MSA and any SOW, "Adverse Event" is the unauthorized use of system privileges, unauthorized access to State data, execution of malware, or physical or electronic intrusion that may include network, applications, servers, workstations, and social engineering of staff. The Vendor must notify the State point of contact within two business days if the Vendor becomes aware that an Adverse Event has occurred. If the Adverse Event was the result of the Vendor's actions or inactions, the State can require a risk assessment of the Vendor and can mandate the scope and methodology used for the risk assessment. The State can require the risk assessment to be performed by a third party at the Vendor's expense.

Section XVII. Threat Notification

For purposes of this MSA and any SOW, "Credible Security Threat" means the discovery of an exploit that a person who is considered an expert on information technology security believes could be used to breach at least one aspect of a system that is holding State data. The Vendor will notify

the State within two business days upon becoming aware of a Credible Security Threat with the Vendor's or a subcontractor's product or service being used by the State to fulfill the Vendor's obligation under this MSA or any SOW. Upon request, the Vendor will provide the State with information regarding the nature of the Credible Security Threat.

Section XVIII. Access Attempts

All access attempts, whether failed or successful, to any system connected to a system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity will be logged by the Vendor. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than seven years in a searchable database in an electronic format that is un-modifiable. At the request of the State, access must be granted to search those logs as needed to demonstrate compliance with the terms of this MSA or any SOW and any audit requirements related to the hosted system.

Section XIX. Access to Protected Data

For the purposes of this MSA and any SOW, "Protected Data" means data protected by any law, regulation, industry standard, or has been designated as sensitive by the federal or a state government. The Parties agree that if a SOW provides the Vendor access to the State's Protected Data, then the following contract clauses apply to that SOW:

A. **Security Incident Notification:** For purposes of this MSA and any SOW, "Security Incident" is a violation of any Bureau of Information and Telecommunications (BIT) security or privacy policy or contract agreement involving Protected Data or the imminent threat of a violation. The BIT security and privacy policies can be found in the Information Technology Security Policy (ITSP), attached to this MSA and fully incorporated in this MSA as Appendix B. The Vendor will implement, maintain, and update Security Incident procedures that comply with all state standards and federal and state requirements. The Vendor agrees to notify the State of a Security Incident. To the extent probes and reconnaissance scans common to the industry constitute Security Incidents, the Parties agree that this MSA constitutes notice by the Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State is required. Probes and reconnaissance scans include, but are not limited to, pings and other broadcast attacks on the Vendor's firewall, port scans, and unsuccessful log-on attempts if such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by a legal requirement, the Vendor will provide notice of the Security Incident to only the State. The State will determine if notification to the public will be made by the State or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Vendor will be distributing, broadcasting to, or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent and must approve the content of the information. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting, or otherwise releasing information on the Security Incident.

1. The Vender must notify the State point of contact within 12 hours of the Vendor becoming aware that a Security Incident has occurred. If notification to the State is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within 12 hours after law enforcement grants permission for the release of information on the Security Incident.
2. At a minimum, notification of a Security Incident state the nature of the Protected Data exposed, the time the Incident occurred, and a general description of the circumstances of the Incident. If any of the preceding information is not available within the notification time period, the Vendor must provide the State with all available information along with the reason for the incomplete notification. The Vendor must provide the missing information to the State immediately upon the information becoming available.
3. At the State's discretion, within five business days of a Security Incident, the Vendor must provide to the State all data available including: (i) contact information for the Vendor's point of contact for the Incident: (ii) date and time of the Incident; (iii) date and time the Incident was discovered: (iv) description of the Incident including the Protected Data involved, being as specific as possible; (v) the potential number of records or, if unknown, the range of records; (vi) address where the Incident occurred: and, (vii) the nature of the technologies involved. If any of the preceding information is not available within the specified time period, the Vendor must provide the State with all available information along with the reason for the incomplete information. The Vendor must provide the missing information to the State immediately upon the information becoming available.
4. The Vendor is responsible for complying with South Dakota Codified Law Chapter 22-40 when applicable to a Security Incident. This legal requirement does not replace the Vendor's obligations found in the preceding three subsections.

B. **Handling of Security Incident:** At the State's discretion, the Vendor may be required to preserve all evidence regarding a Security Incident including, but not limited to, communications, documents, and logs. In addition, the Vendor will:
   1. fully investigate each Security Incident;
   2. cooperate fully with the State's investigation and analysis of and response to the Security Incident;
   3. make a best effort to implement necessary remedial measure as soon as it is possible; and
   4. document responsive actions taken related to the Incident, including any post-Incident review of events and actions taken to implement changes in business practices in providing the services covered by the applicable SOW.

   If the State determines the Security Incident was due to the actions or inactions of the Vendor, the Vendor must pay for and use a credit monitoring service, call center, forensics company, advisors, or public relations firm to respond to the Incident; all of which services must be preapproved by the State. The State may require the Vendor to offer and pay for one year of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment of the Vendor, which the Vendor will pay for. If the State requires a risk assessment, the State will mandate the methodology and the scope of the assessment. The State reserves the right to select a third party to conduct the risk assessment.

If the Vendor is required by federal, state, or international law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within 12 hours of the investigation report being completed. If the Vendor is required by federal, state, or international law or regulation to notify the affected parties, the State must also be notified unless otherwise prohibited by law.

Notwithstanding any other provision of this MSA or any SOW, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State for investigating and remediating a Security Incident including, but not limited to, providing notification to regulatory agencies or other entities as required by law or contract. The Vendor will pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

C. **Security Acknowledgment Form:** The Vendor must sign the Security Acknowledgement Form, which is attached to this MSA as Appendix C. Before work on a SOW may begin, the signed Security Acknowledgement form must be approved by BIT and the approval must communicated to the Vendor. This form constitutes the agreement of the Vendor to be responsible and liable for ensuring that the Vendor and its employees and subcontractors participating in the work will abide by the policies found within the ITSP. Failure to abide by the requirements of the ITSP or the Security Acknowledgement form is considered a breach of this MSA and any applicable SOW. The Vendor is required to submit a new signed Security Acknowledgment Form when a new employee or subcontractor begins work on the project after the original Form is approved by the State; failure to do is a breach of this MSA and applicable SOW. The State reserves the right to require the removal of an employee or subcontractor from the project covered by a SOW if that employee or subcontractor violated any requirement of the ITSP.

D. **Background Investigations:** The State requires any person who is fulfilling the Vendor's obligations under this MSA and an appliable SOW and who writes or modifies state-owned software, alters hardware, configures software of state-owned technology resources, has access to source code or Protected Data, or has access to secure areas to undergo a fingerprint-based background investigation. The fingerprints will be used to check the criminal history records of both the State of South Dakota and the Federal Bureau of Investigation. These background investigations will be performed by the State with support from the State's law enforcement agencies. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow two to four weeks to complete this process. If work assignments change after the initiation of the project covered by an applicable SOW so that a new person will be fulfilling the Vendor's obligations for the project and that person will be writing or modifying State owned software, altering hardware, configuring software of state-owned technology resources, have access to source code or Protected Data, or have access to secure areas then a background investigation must be performed on that new person. The State reserves the right to require the Vendor to prohibit any person fulfilling the Vendor's obligations from performing work under an applicable SOW whenever the State, in its sole discretion, believes that having that specific person perform work under the SOW is detrimental to the project or is considered by the State to be a security risk based on the results of the background investigation. The State will provide the Consultant with notice of this determination.

E. **Restriction on Use of Protected Data in a Non-Production Environment:** The Vendor cannot use Protected Data in a non-production environment. Any non-production environment that is found to have Protected Data must be purged immediately and the Vendor must immediately notify the State point of contact. Upon receipt of notice, the State will determine if such an event qualifies as a Security Incident. Protected Data that is de-identified, aggregated, or hashed is no longer considered to be Protected Data.

F. **Movement of Protected Data:** All Protected Data must be kept secure. When Protected Data is moved to any of the Vendor's production systems, security must be maintained. The Vendor will ensure that the Protected Data will at least have the same level of security as it had in the State's environment, the policies for which are found in the ITSP.

Section XX. Multi-factor Authentication

The Vendor and its employees and subcontractors will not access the State's network except through the State's Multi-factor Authentication (MFA) process. For purposes of remote access to any State system on the State's domain, the Vendor will adhere to the State's requirement for MFA upon receipt of notification from the State that such requirements have been implemented. The Vendor will require adherence to the State's requirements by any of officer, employee, or subcontractor of the Vendor who will have remote access to any State system on the State's domain. The State's requirements for MFA are found in the ITSP.

Section XXI. Training Requirements

All persons fulfilling the Vendor's obligations under this MSA and any SOW must successfully complete a cyber-security training program at the time of hire and annually thereafter. The training must include, but is not limited to: legal requirements for handling data, media sanitation, strong password protection, social engineering or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and security incident response.

Section XXII. Funding Out

This MSA and all SOWs depend 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 MSA or the applicable SOW will be terminated by the State. Termination pursuant to this section is not a default by the State nor does it give rise to a claim against the State.

Section XXIII. Assignment

This MSA and any SOW may not be assigned without the express prior written consent of the State.

Section XXIV. Amendment

This MSA or any SOW may not be amended except in writing, which writing will be expressly identified as a part of this MSA or the applicable SOW and be signed by the authorized representatives of both Parties.

Section XXV. Change Management Process

The Parties may agree to modify the services provided pursuant to a SOW through a written change order specifically referencing both this MSA and the applicable SOW. Such change order will become effective and part of the applicable SOW when executed by both parties, containing the dated signatures of authorized representatives of the Parties. The services described within the change order will become part of the applicable SOW deliverables.

Section XXVI. Governing Law

This MSA and all SOWs 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. The venue for any lawsuit pertaining to or affecting this MSA and all SOWs will be in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota**.**

Section XXVII. Insurance

At all times during the Term of the Agreement, the Vendor will obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. **Commercial General Liability Insurance:** The Vendor 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 MSA or a SOW or be no less than two times the occurrence limit.

B. **Professional Liability Insurance or Miscellaneous Professional Liability Insurance:** The Vendor will maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1 million.

C. **Business Automobile Liability Insurance:** The Vendor 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.

D. **Workers' Compensation Insurance:** The Vendor will maintain workers' compensation and employer's liability insurance as required by South Dakota law.

E. **Cyber Liability Insurance:** The Vendor will maintain cyber liability insurance with liability limits in the amount of $3 million to protect all State data the Vendor receives as part of this MSA and all SOW, no matter where the State data resides. If the Vendor has a contract with a third party to host any state data, then the Vendor will require the third party to maintain a similar level of cyber liability insurance that protects the State data, no matter where the State data resides. The cyber liability insurance will cover expenses related to management of a data breach incident, the investigation, recover and restoration of lost State data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. The cyber liability insurance must stay in effect for three years after the termination of this MSA.

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

Section XXVIII. Compliance

The Vendor will comply with all federal, international, state, and local laws, regulations, ordinances, guidelines, permits, and requirements applicable to providing services pursuant to this MSA and all SOWs, and will be solely responsible for obtaining current information on such requirements. Liability resulting from noncompliance with applicable standards required by federal, international, state, and local laws, regulations, ordinances, guidelines, permits, and other requirements is assumed entirely by the Vendor.

Section XXIX. Subcontractors

The Vendor may not use subcontractors to perform services described in any SOW without the express written consent of the State. The Vendor will include provisions in its subcontracts requiring the subcontractors to comply with the applicable provisions of this MSA and the applicable SOW, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this MSA. The Vendor will require its subcontractors, agents, and employees to comply with applicable federal, state, and local laws, regulations, ordinances, guidelines, permits, and requirements. The Vendor will adopt review and inspection procedures as are necessary to ensure such compliance.

Section XXX. Rejection or Ejection of Vendor Employees and Subcontractors

The State may require the vetting of any of the Vendor's employees or subcontractors. The Vendor agrees to assist in this process as needed.

The State reserves the right to reject any person from participating in a project or require the Vendor to remove from a project any person the State believes is detrimental to the project or is considered by the State to be a security risk. Upon receipt of the Vendor's request, the State will provide the Vendor with notice of its determination and the reasons for the rejection or removal. If the State signifies that a potential security violation exists with respect to the request, the Vendor agrees it will immediately remove the individual from the project.

Section XXXI. Work Product and Ownership and Use

The Vendor represents and warrants the professional quality, technical accuracy, timely completion, and coordination of all services and products provided by the Vendor and any subcontractors, if applicable, under this MSA and all SOWs. The Vendor warrants that the services and the products provided are technically sound and in conformance with all applicable federal, international, state, and local statutes, codes, ordinances, resolutions, and other regulations. The Vendor will, without additional compensation, correct or revise any errors or omissions in its work products.

The Vendor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, agreements, Confidential Information, State data, Protected Data, any information discovered by the State, PII, data protected under FERPA, PHI, FTI, or any information defined under state statute as confidential, and all information contained therein provided to the State by the Vendor in connection with its performance under this Agreement and all SOWs will belong to and is the property of the State and will not be used in any way by the Vendor without the written consent of the State.

Papers, reports, forms, or other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State. If any copyright does not fully belong to the State, the State reserves a royalty-free, non-exclusive, non-transferable, and irrevocable license to reproduce, publish, and otherwise use and to authorize others to use on the State's behalf any such work for government purposes.

Section XXXII. Transfer of Ownership of Work Product

Upon the effective date of this MSA, the Vendor hereby assigns to the State all of the Vendor's ownership, right, title, and interest in and to any copyrights in the software and other assets created pursuant this MSA and any SOW with a state agency ("Work Product").

A. **License.** To the extent that this Section does not provide the State with full ownership, right, title, and interest in and to the Work Product, the Vendor hereby grants the State a perpetual, irrevocable, fully paid, royalty-free, worldwide license to reproduce, create derivative works from, distribute, publicly display, publicly perform, and use the Work Product, with the right to sublicense every such right.
B. **Further Assistance & Survival.** The Vendor will reasonably assist the State in obtaining and enforcing copyrights in the Work Product, at the State's expense. The rights granted in this Section will survive any termination or expiration of this Agreement and any applicable SOW or of the Vendor's engagement with the State.
C. **Transfer of Employee Rights.** Prior to the effective date of this MSA, the Vendor will ensure that all its employees and contractors who may in any way be involved in creating the Work Product are subject to written agreements with the Vendor that grant the Vendor all such employees' or contractors' present and future ownership and other rights in and to the Work Product.

Section XXXIII. Debarment

The Vendor certifies that neither the Vendor nor its principals are presently debarred, suspended, proposed for debarment or suspension, declared ineligible, or voluntarily excluded from participating in transactions by the federal government or any state or local government department or agency. During the Term of the Agreement, if the Vendor 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, Vendor agrees to immediately notify the State.

Section XXXIV. Bankruptcy Rights

When applicable, the rights and licenses granted to the State in this MSA or a SOW are licenses to "intellectual property" rights, as defined by Section 365(n) of the United State Bankruptcy Code (11 U.S.C. Sections 101, et seq.). If the Vendor is subject to any proceeding under the United States Bankruptcy Code, and the Vendor as debtor in possession or its trustee in bankruptcy reject this MSA or a SOW, the State may, pursuant to 11 U.S.C. Section 365(n)(1) and (2), retain all rights granted to it under this MSA or the SOW to the maximum extent permitted by law. This Section XXXIV will not be construed to limit or restrict any right or remedy not set forth in this Section XXXIV, including without limitation the right to retain any license or authority this MSA or a SOW grants pursuant to any provision other than the licensing provisions of this MSA or a SOW.

Section XXXV. Notice

Any notice or other communication required under this MSA will be in writing and sent to the address set forth above. For this MSA, notices will be given by and to **(Insert BIT POC for MSA), South Dakota Bureau of Information and Telecommunications,** on behalf of the State, and by **(Name of Vendor POC), (Vendor POC Title), (Vendor Company Name)**, on behalf of the Vendor, or such authorized designees as either party may from time to time designate in writing. The Parties acknowledge and agree that each unique SOW will designate an agency specific point of contact to whom notices must be given to.

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 must be sent by registered or certified mail, or, if personally delivered, when received by such party. Notices or communications to or between the parties by email will be deemed to have been delivered when sent by the sending party.

Section XXXVI. Electronic Signature

The Parties agrees that this MSA and any SOW may be electronically signed, and that any electronic signatures appearing on this MSA or a SOW are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility.

Section XXXVII. Severability

In the event that any court of competent jurisdiction rules any provision of this MSA or a SOW unenforceable or invalid, such ruling will not invalidate or render unenforceable any other provision hereof.

Section XXXVIII.Entire Agreement

This MSA sets forth the entire agreement of the Parties and supersedes all prior or contemporaneous writings, negotiations, and discussions with respect to its subject matter. Neither Party has relied upon any such prior or contemporaneous communications.

Section XXXIX. State of Israel

By signing this MSA, the Vendor certifies and agrees that it 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 the contract, 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 MSA. During the term of this MSA, if the Vendor no longer complies with this certification, the Vendor agrees to provide immediate written notice to the State and agrees such noncompliance may be grounds for termination of this MSA and any active SOW.

Section XL. Conflict of Interest

The Vendor agrees to establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Vendor expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

Section XLI. Conflicts among Attachments

In the event of conflict with an attachment to this MSA, this main body of this MSA will govern. In addition, no SOW or other attachment incorporated into this SOW or other attachment incorporated into this MSA after execution of this main body of this MSA will be construed to amend this main body unless it specifically states its intent to do so and cites the section or sections amended.

3.0 SCOPE OF WORK

The scope of work for each agency project will be determined based on the modules/services and skills/rolls required. The detailed scope of work will be provided in a detailed SOW as the need arises. These SOWs will be created in conjunction with BIT and any other state agency in need of cloud platform services for a specific engagement, and each SOW will incorporate the terms of the Agreement resulting from this RFP.

4.0 RESOURCES

BIT is the state agency that provides IT services for the State.

Any services provided as a result of this RFP will utilize 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.

4.1 TEAM ORGANIZATION: Provide the following information.

4.1.1 PROJECT ORGANIZATION CHART

In detailed SOWs for cloud platform services, names, job titles (designate vacancies), and the city and state of staff who will work on projects will be specified.

4.1.2 LIST OF ALL CONSULTANTS AND SUBCONTRACTORS

In detailed SOWs for cloud platform services, descriptions for which responsibilities will be assigned to consultants or subcontractors and the city and state in which the consultants or subcontractors are located will be specified.

4.2 STATE PROJECT STAFFING ROLES

Project staffing roles will be determined based on the scope of work found in the detailed SOW. Not all engagements will require all staffing roles. Each engagement may consist of, but is not limited to, the following roles:

Agency Project Sponsor
Agency Scrum/Project Manager
Agency Project Security Lead
Agency Application Solution Architect
Agency Platform Architect
Agency Developers
Agency Testers

4.3 STAFF RESUMES AND REFERENCES

Resumes and references of key personnel, 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 a specific engagement. In detailed SOWs for cloud platform services, resume details for all key personnel will be specified, 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 from present to 2016 (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 **relative to section 1.2.3 Description of Components**
- Technical Background **relative to section 1.2.3 Description of Components**
- Experience in Projects **relative to section 1.2.3 Description of Components**
- Names of the Similar Projects they were involved in **relative to section 1.2.3 Description of Components**
- Role they played in the projects similar to this project **relative to section 1.2.3 Description of Components**
- Project Management Experience
- Technical Knowledge **relative to section 1.2.3 Description of Components**
- Education
- Relevant Certifications **relative to section 1.2.3 Description of Components**
- Three Professional References (name, telephone number, company name, relationship to employee)

5.0 PROJECT DELIVERABLES/APPROACH/METHODOLOGY

The deliverables, approach, and methodology of an engagement will be determined based on the modules/services and skills/rolls required. These details will be provided in a detailed SOW as the need arises. These SOWs will be created in conjunction with BIT and any other state agency in need of cloud platform services for a specific engagement, and each SOW will incorporate the terms of the Agreement resulting from this RFP.

6.0 FORMAT OF SUBMISSION

All proposals 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 and effective proposal are not desired.

Offerors are required to provide an electronic copy of their proposals via email to harold.bruce@state.sd.us. The electronic copy should be provided in MS WORD or in PDF format. The email, including attachments, should be limited to 10MB in size.

The Offeror is cautioned that it is the Offeror's sole responsibility to submit information related to the evaluation categories and that the State is under no obligation to solicit such information if it is not included with the proposal. The Offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all questions or comments regarding the RFP, the evaluation, etc. to harold.bruce@state.sd.us. Offerors and their agents may not contact any state employee other than Harold Bruce regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should email harold.bruce@state.sd.us.

The Offeror may be required to submit a copy of its most recent audited financial statements upon the State's request.

The proposal should be page numbered and should have an index and a table of contents referencing the appropriate page number. Each of the sections listed below should be tabbed.

Offerors are cautioned that the use of the state seal in any of their documents is illegal pursuant to South Dakota Codified Law 1-6-3.1, which states:

> 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. (*SDCL § 1-6-3.1)*

Proposals 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.

6.1 Statement of Understanding of Project
6.4 Project Plan
6.2 Corporate Qualifications
6.3 Relevant Project Experience
6.6 Contract Terms
6.7 Background Checks
7.0 Costs

6.1 STATEMENT OF UNDERSTANDING OF PROJECT

To demonstrate your comprehension of Section 1.2.2 Goals and Objectives, please summarize your understanding of what the work will entail. This should include, but not be limited to your understanding of the purpose and scope of potential projects, critical success factors and potential problems related to potential projects. Your specialized expertise, capabilities, and technical competence as demonstrated by previous experience to delivery Platform Cloud IT Services, as specified relative to section 1.2.3 Description of Components, should be included. This section should be limited to no more than two pages.

6.2 CORPORATE QUALIFICATIONS

Please provide responses to the each of the following questions in your proposal.

A. What year was your parent company (if applicable) established?

B. What is the business of your parent company?

C. What is the total number of employees in the parent company?

D. What are the total revenues of your parent company?

E. How many employees of your parent company have the skill set to support this effort?

F. How many of those employees are accessible to your organization for active support?

G. What year was your firm established?

H. Has your firm ever done business under a different name and if so what was the name?

I. How many employees does your firm have?

J. How many employees in your firm are involved in this type of project?

K. How many of those employees are involved in on-site project work?

L. What percent of your parent company's revenue (if applicable), is produced by your firm?

M. Corporate resources available to perform the work, including any specialized services, within the specified time limits for the project. **For Microsoft Partners, please list the Microsoft Competencies for the related technologies from Section 1.2.3 and whether they are gold or silver competencies**.

N. Availability to the project locale

O. Familiarity with the project locale

P. Has your firm ever done business with the State of South Dakota? If so, please provide references.

Q. What is your Company's web site?

When providing references, the reference must include the following information:

- Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted
- Dates of the service/contract
- A brief, written description of the specific prior services performed and requirements thereof

6.3 RELEVANT PROJECT EXPERIENCE

Provide details about four recent projects that the Offeror was awarded and then managed through to completion. Project examples should include sufficient detail so BIT fully understands the goal of the project.

A. Client/Company Name

B. Client Company Address, including City, State and Zip Code

C. Client/Company Contacts(s)
    Name
    Title
    Telephone Number
    E-mail address
    Fax Number

D. Project Start Date

E. Project Completion Date

F. Project Scope of Work

G. Project Deliverables, if any

H. Offeror's Role in Project

I. Offeror's Responsibilities

J. Offeror's Accomplishments

K. Description of How Project Was Managed and Methodology Used

L. Description of Price and Cost Data from Project

M. Description of Special Project Constraints, if applicable

N. Description of Your Ability and Proven History in Handling Special Project Constraints

O. Description of All Changes to the Original Plan or Contract That Were Requested

P. Description of All Changes to the Original Plan or Contract That Offeror Completed

Q. Description of How Change Requests Were Addressed or Completed by Offeror

R. Was Project Completed in a Timeframe That Was According to the Original Plan or Contact? (If "No", provide explanation)

S. Was Project Completed Within Original Proposed Budget? (If "No" provide explanation)

T. Was There Any Litigation or Adverse Contract Action Regarding Contract Performance? (If "Yes" provide explanation)

U. Feedback on Offeror's Work by Company/Client

V. Offeror's Statement of Permission for BIT to Contact the Client/Company and for the Client's/Company's Contact(s) to Release Information to BIT

6.4 PROJECT PLAN

The project plan of an engagement will be determined based on the modules/services and skills/rolls required. The project plan will be provided in a detailed SOW as the need arises. These SOWs will be created in conjunction with BIT and any other state agency in need of cloud platform services for a specific engagement, and each SOW will incorporate the terms of the Agreement resulting from this RFP. Please describe your approach for project management techniques, and how you typically approach: staffing, tasks, deliverables, required state agency support, and training, relative to section 1.2.3 Description of Components.

6.5 DELIVERABLES

The deliverables of an engagement will be determined based on the modules/services and skills/rolls required. These deliverables will be provided in a detailed SOW as the need arises. These SOWs will be created in conjunction with BIT and any other state agency in need of cloud platform services for a specific engagement, and each SOW will incorporate the terms of the Agreement resulting from this RFP.

6.6 CONTRACT TERMS

The Offeror must state if there are any issues with the contract terms in Section 2.0. The issues should be fully described along with any proposed changes.

6.7 BACKGROUND CHECK

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 statute as confidential or have access to secure facilities will have fingerprint-based background checks. These background checks 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 Subcontractor's, Agents, Assigns and or Affiliated Entities employees.

7.0 COST PROPOSAL

Please describe your cost recovery model for the services you provide **as relative to section 1.2.3 Description of Components**.

7.1 STAFFING

Name (optional)	Role	Total Hours on Project	Total Hours on Site	Hourly Rate	Total
				Total:	

7.2 TRAVEL AND EXPENDITURE TABLE

Name (optional)	Method of Travel	Cost per trip	Number of Trips	Total Cost
			Total:	

Name (optional)	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 consultants accept state per diem. The state per diem is located Bureau of Human Resources website at https://bhr.sd.gov/files/travelrates.pdf.

8.0 PROPOSAL EVALUATION AND AWARD PROCESS

8.1

After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria:

8.1.1 Company Specialization – 30%

- Expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the resource staffing requirements.
- Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration.
- 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.
- Microsoft Competencies, if applicable, and the competency level for each (Gold or Silver).

8.1.2 Resources – 25%

- The proposed resource must have knowledge and skills identified in Section 1.2.3 Description of Components, excellent customer relations, and experience working in teams.
- Resources available to perform the work, including any specialized services, within the specified time limits for the project.
- 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 information related to the experience and qualifications, including education and training, of proposed personnel.

8.1.3 – 25%

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

8.1.4 – 5%

Availability to the project locale;

8.1.5 – 5%

Familiarity with the project locale;

8.1.6 – 5%

Proposed project management techniques; and

8.1.7 – 5%

Ability and proven history in handling special project constraints

8.2

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.

8.3 Award

BIT will place Offerors that satisfy the mandatory requirements stated in the RFP on a list of qualified vendors. When the State has a need for expanding or enhancing the State's existing cloud platform technologies or providing additional cloud platform technologies, the State

will solicit from the qualified vendor list proposals for completing the request, which will consist of a SOW.

9. BEST AND FINAL OFFERS

The State reserves the right to request a best and final offer from each Offeror chosen to enter into an Agreement pursuant to this RFP. If so, the State will initiate the request for a best and final offer; a best and final offer cannot be initiated by an Offeror. A best and final offer may not be necessary if the State is satisfied with proposals received.

If best and final offers are sought, the State will document which Offerors will be notified and provide them the 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 request for proposal and instructions contained in the request for a 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 – CERTIFICATE OF MEDIA SANITATION FOR OFFSITE DATA

Certificate of Media Santization.docx

APPENDIX B– INFORMATION TECHNOLOGY SECURITY POLICY

The Information Technology Security Policy - Contractor (ITSP) is located at: https://bit.sd.gov/docs/Information%20Technology%20Security%20Policy%20-%20Contractor.pdf

APPENDIX C – SECURITY ACKNOWLEDGEMENT FORM

Contractor Security Acknowledgement F

APPENDIX D – CERTIFICATION RE PROHIBITED ENTITY

APPENDIX D -
Certification re Proh