**SUBMITTAL FORM H – Infrastructure Requirements**

SPECIAL REQUIREMENTS: This Submittal Form must not contain any names that can be used to identify who the proposer is and must not identify the proposers cost/fee(reference RFP section 4.10).

**The following lists DRB’s infrastructure requirements for an on-premise and a cloud-based solution. Vendors may respond to either Infrastructure A or Infrastructure B requirements or both.**

|  |  |
| --- | --- |
| **Infrastructure A** | These requirements apply only to the on-premise solution. |
| **Infrastructure B** | These requirements apply only to the cloud-based hosting solution. |

**If the Offeror is submitting both an on-premise and a cloud-based solution, provide a brief (one page or less) description of the advantages and disadvantages to each. Indicate which hosting option you feel would be in DRB’s best interest to use.**

**For the following requirements, indicate the Degree of Customization Required in the applicable field:**

1. **Configuration**. Existing system functionality will be configured to deliver the requirement. This includes setting of parameter values, updates to factor and value tables, updating rules engines, and selection from any available configuration options within the existing software release. Configuration changes would not be expected to have any impact on future software updates.
2. **Minor Customization**. To meet the requirement, existing functionality will be modified to incorporate unique DRB customizations not within the existing software release. This includes customization within well-defined exit/entry points within the system, interface file format definitions, custom formulas, custom SQL or SQR code for queries or reports, and addition/modification of data fields. Minor Customizations would not be expected to have an impact on future software updates.
3. **Major Customization**. Existing functionality to meet the requirement does not currently exist within an existing module, feature, or system component. This includes DRB-specific extensions/enhancements/customizations to existing functionality, DRB-specific APIs, protocols, or standards, and back-porting features from another version of the system. These are customizations that would not normally be reviewed or tested by the Contractor as part of their general System release testing and validation. Special care would be required to ensure compatibility with future software updates.
4. **Other** (describe in comments). Existing functionality to meet the requirement does not currently exist and would require either a new functionality be added to the System, e.g. a new module, feature, or system component, the use of third-party technology specifically to meet DRB’s requirement, or the requirement will be met outside of the System either manually or with a standalone tool.

## Infrastructure A – On-Premise Solution

|  |
| --- |
| **Please provide a maximum 1-page narrative description of how your on-premise solution supports the Infrastructure A Technical Requirements and meets the functional requirements listed below. Provide information detailing what differentiates your solution from others in the industry and why it is the best option for Alaska DRB.** |
| **Response**: |

| **ReqID** | **Sub-category** | **Requirement Details** | **Degree of Customization Indicator** | **Meets Requirement?** |
| --- | --- | --- | --- | --- |
| T5.12 | Performance | The System must make use of F5 Front-end load balancing of web servers. |  | [ ] Yes [ ] No |
| T5.13 | Performance | The System must make use of F5 Application server load balancing capabilities. |  | [ ] Yes [ ] No |
| T5.16 | Architecture | The System must be compatible with Intrusion Detection System (IDS)/Intrusion Protection System (IPS) and solutions installed and operated on both the internal and external interfaces for state firewalls and host End Point protection is installed for malware protection. Logging of all IDS/IPS solutions must be performed at the enterprise level and sent to the State’s enterprise logging solutions. State of Alaska uses McAfee Security Platform for IPS and Cybereason for End Point Protection. The State Security Office plans to move to a new product for IPS by the end of the calendar year. |  | [ ] Yes [ ] No |
| T5.17 | Architecture | The architecture must be compatible with Stateful Packet Inspection (SPI) technology inspecting inbound and outbound traffic from bastion host environment and external networks and the State intranet environment. State of Alaska uses Cisco ASA’s for SPI but may be replaced over the next two years. |  | [ ] Yes [ ] No |
| T5.18 | Architecture | The architecture must be compatible with firewall technology separation between bastion host, external and internal (intranet) environments. State of Alaska uses Cisco ASA’s for separation and may be replaced over the next two years. |  | [ ] Yes [ ] No |
| T5.19 | Architecture | The architecture must be compatible with Forward-Proxy technology forwarding outgoing requests from a private network or intranet to the Internet. State of Alaska uses BIGIP F5’s. |  | [ ] Yes [ ] No |
| T5.20 | Policy | The System must not utilize any firewall or other security appliance that adversely affects the State’s solutions or proposed solutions for the management, monitoring, auditing, logging, or reporting within the State WAN or Local Area Network (LAN) environments. The SSO must evaluate all firewall requests on a case-by-case basis for adverse effects. |  | [ ] Yes [ ] No |
| T5.21 | Policy | The Offeror must protect and secure the operation of State networks in a manner appropriate to the sensitivity of the electronic information traversing those networks. The Offeror must not purchase or deploy firewalls or other network security solution without the approval of the State Security Office (SSO) as defined in State policy ISP-179 Firewall Use. |  | [ ] Yes [ ] No |
| T5.22 | Policy | The Offeror must use only State approved systems, software, and networks to remotely connect to State networks. |  | [ ] Yes [ ] No |
| T5.23 | Policy | The Offeror must complete a security plan and submit it to the SSO for authorization as defined in SOA policy ISP-191 Security in Systems Development. |  | [ ] Yes [ ] No |
| T5.24 | Policy | Ingress/Egress points will not be established outside the State’s Enterprise DMZ environments |  | [ ] Yes [ ] No |
| T5.25 | Policy | Ingress/Egress environments will consist of a multi-layer architecture that provides clear separation between the bastion host environment and the State Internal networks or services. |  | [ ] Yes [ ] No |
| T5.26 | Policy | All network, system, service, application, appliances, or other devices within an Ingress/Egress environment must report to a security event correlation solution. |  | [ ] Yes [ ] No |
| T5.27 | Policy | All ingress/egress environments will support application and user proxies. |  | [ ] Yes [ ] No |
| T5.28 | Policy | All ingress/egress environments will log and report to SSO specified logging devices or solutions. |  | [ ] Yes [ ] No |
| T5.29 | Policy | The SSO will be provided read-only access to all ingress/egress environments and all devices supporting environment for the purposed of ensuring security. |  | [ ] Yes [ ] No |
| T5.30 | Policy | The Offeror must not install servers, add services, connect networks, or otherwise implement systems onto or within existing State systems or networks without the specific approval of OIT Executive Management. |  | [ ] Yes [ ] No |

## Infrastructure B – Cloud-based Hosting Solution

|  |
| --- |
| **Please provide a maximum 1-page narrative description of how your hosted cloud-based solution supports the Infrastructure B Technical Requirements and meets the functional requirements listed below. Provide information detailing what differentiates your solution from others in the industry and why it is the best option for Alaska DRB.** |
| **Response**: |

| **ReqID** | **Sub-category** | **Requirement Details** | **Degree of Customization Indicator** | **Meets Requirement?** |
| --- | --- | --- | --- | --- |
| T5.31 | Compliance | The Cloud Services provider will be Federal Risk and Authorization Management Program (FedRAMP) certified at the High level. DRB reserves the right to inspect the Government Cloud Services provider’s FedRAMP Readiness Assessment Report and other such FedRAMP certification supporting documentation. |  | [ ] Yes [ ] No |
| T5.32 | Compliance | The Cloud Services provider will support HIPAA compliance and enter into a Business Associate Agreement, as required by HIPAA. |  | [ ] Yes [ ] No |
| T5.33 | Data protection | The Offeror and their subcontractors will implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of all data within its control. Such security measures will be in accordance with recognized industry practice and not less stringent than the measures the Offeror their subcontractors apply to its own data of similar kind. |  | [ ] Yes [ ] No |
| T5.34 | Data protection | All data obtained by the Offeror and their subcontractors within its control in the performance of this contract will become and remain the property of DRB. This data includes, but is not limited to, all system & infrastructure generated audit, security, error, performance, and activity logs. |  | [ ] Yes [ ] No |
| T5.35 | Data protection | At no time will any data or processes, which either belong to or are intended for the use of DRB or its officers, agents, or employees, be copied, disclosed, or retained by the Offeror and their subcontractors or any party related to the Offeror and their subcontractors for subsequent use in any transaction that does not include DRB. |  | [ ] Yes [ ] No |
| T5.36 | Data protection | The Offeror and their subcontractors will maintain and implement procedures to logically separate DRB data from the Offeror and subcontractor’s data and the data belonging to the Offeror and subcontractor’s other customers. |  | [ ] Yes [ ] No |
| T5.37 | Data protection | The Offeror and their subcontractors will not store DRB Data on any portable computing device including, but not limited to, personal data assistant (PDA), cell phone, smartphone, laptop (each a “Portable Computing Device”), unless DRB Data stored on such Portable Computing Device is encrypted. |  | [ ] Yes [ ] No |
| T5.38 | Data protection | The Offeror and their subcontractors will not store DRB Data on any removable media, such as compact disc, flash drive, tape (each a “Removable Media”), unless DRB Data stored on such Removable Media is encrypted. |  | [ ] Yes [ ] No |
| T5.39 | Data protection | The Offeror and their subcontractors will ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Confidential Data, Restricted Data, and Personal Data, unless the Offeror and their subcontractors present a justifiable position approved by DRB that data must be stored on an Offeror and subcontractors portable device in order to accomplish work as defined in the scope of work. |  | [ ] Yes [ ] No |
| T5.40 | Data protection | DRB will own all right, title, and interest in DRB Data that is related to the Cloud Services provided by this contract. The Offeror and their subcontractors will not access DRB user accounts or DRB Data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at DRB’s written request. |  | [ ] Yes [ ] No |
| T5.41 | Data protection | DRB will have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Offeror and their subcontractors. This includes the ability for DRB to import or export data to/from other service providers. |  | [ ] Yes [ ] No |
| T5.42 | Data protection | The Offeror will ensure that all data, including data stored in all databases, environments, and data backups, will be stored on-shore within the United States of America and that the data will be accessed only by personnel located within the United States of America. System access will be limited to DRB-assigned access and only those Offerors’ staff required performing services under this Contract. Staff with data access will sign a nondisclosure agreement and a security agreement with DRB. The Offeror will use the data only as necessary to perform services hereunder and not share or sell the data in any way. |  | [ ] Yes [ ] No |
| T5.43 | Data protection | The Offeror will contact DRB upon receipt of any electronic discovery, litigation holds, discovery searches, or expert testimonies related to DRB’s data under this contract, or which in any way might reasonably require access to the data of DRB. The Offeror and their subcontractors will not respond to subpoenas, service of process, or other legal requests related to DRB without first notifying DRB, unless prohibited by law from providing such notice. |  | [ ] Yes [ ] No |
| T5.44 | Data protection | In the event of an early termination of the contract, the Offeror and their subcontractors will allow DRB to retrieve its digital content and provide for the subsequent secure disposal of DRB digital content. |  | [ ] Yes [ ] No |
| T5.45 | Data protection | During any period of suspension, the Offeror and their subcontractors will not take any action to intentionally erase any DRB digital content. |  | [ ] Yes [ ] No |
| T5.46 | Data protection | In the event of early termination of any services or agreement in entirety, the Offeror and their subcontractors will not take any action to intentionally erase any DRB data until all data has been transferred to a new environment of DRB’s choice. After the transfer, the Offeror and their subcontractors will have no obligation to maintain or provide any DRB data and will thereafter, unless legally prohibited, delete all DRB Data in its systems or otherwise in its possession or under its control. In the event of termination for cause, the Offeror and their subcontractors will impose no fees for access and retrieval of digital content to DRB. |  | [ ] Yes [ ] No |
| T5.47 | Data protection | After termination of the contract and the prescribed retention period, the Offeror and their subcontractors will securely dispose of all digital content in all of its forms, such as disk, CD/ DVD, backup tape, and paper. DRB’s digital content will be permanently deleted and will not be recoverable, according to NIST-approved methods. Certificates of destruction will be provided to DRB. |  | [ ] Yes [ ] No |
| T5.48 | Disaster Recovery | The System must use, subject to DRB's approval, multiple Cloud Service provider geographically distinct regions for disaster recovery and business continuity. |  | [ ] Yes [ ] No |
| T5.49 | Disaster Recovery | The System must use, subject to DRB's approval, multiple Cloud Service provider data sites and/or availability zones for System fault tolerance. |  | [ ] Yes [ ] No |
| T5.50 | Disaster Recovery | The System must provide for a Recovery Time Objective of no greater than 24 hours |  | [ ] Yes [ ] No |
| T5.51 | Disaster Recovery | The System must provide a Recovery Point Objective (Maximum time period of lost transactions, data changes, or work-in-process) of no greater than 8 hours |  | [ ] Yes [ ] No |
| T5.52 | Logs | The Offeror and their subcontractors will provide access to system logs which include usage statistics, user access data, user access IP address, user access history, and security information. |  | [ ] Yes [ ] No |
| T5.53 | Performance | If applicable, the Offeror will have a Service Level Agreement (SLA) with their subcontractors. The SLA will be designed to support the goals contained in the SLA between the Offeror and DRB. |  | [ ] Yes [ ] No |
| T5.54 | Performance | The System must provide a Percentage uptime guarantee of 99.99%. The intervals measured shall be every 15 minutes during guaranteed periods. The time periods used for measuring uptime shall be monthly, starting each first of month at 12:01am Alaska Time Zone |  | [ ] Yes [ ] No |
| T5.55 | Performance | The System must provide a Maximum response time (for query & update functions), percentage of 98 percent within 2 seconds. The intervals measured shall be every 60 minutes during guaranteed periods. The time periods used for measuring system response time shall be monthly, starting each first of month at 12:01am Alaska Time Zone |  | [ ] Yes [ ] No |
| T5.56 | Policy | The Offeror and their subcontractors must provide annually a SOC-2, Type 2 audit report prepared by an independent certified public accounting firm under Statement on Standards for Attestation Engagements No. 18 (“SSAE 18 Report”) for each facility from which Government Cloud Services are provided. |  | [ ] Yes [ ] No |
| T5.57 | Policy | The Cloud Services provider and any implementation subcontractors responsible for infrastructure will be a distinct entity from the Offeror. |  | [ ] Yes [ ] No |
| T5.58 | Policy | The Cloud Services provider and any implementation subcontractors responsible for infrastructure must be approved by the State OIT. |  | [ ] Yes [ ] No |
| T5.59 | Policy | The Offeror will ensure that the Cloud Services will provide for sustainable and cost-effective operation of the System. The Offeror will, as applicable, will, upon request by DRB, promptly make available copies of invoices from a Cloud Services provider and any Offeror subcontractors issued to the Offeror, and all supporting materials submitted in support of same. |  | [ ] Yes [ ] No |
| T5.60 | Policy | The Offeror will require that the Cloud Services provider and any Offeror subcontractors provide that, in the event the Offeror’s services are terminated, prior to the expiration of the term set forth in this Contract, DRB will have the right to assume all of the Offeror’s rights in the Government Cloud provider and any (Sub)contractor managed environments. |  | [ ] Yes [ ] No |
| T5.61 | Policy | The Offeror and their subcontractors will include a calendar of scheduled maintenance, which will be continuously available to DRB, with all scheduled activities occurring within the Maintenance and Support periods set forth herein. The Offeror will require that any cloud hosted infrastructure subcontractors provide for the underlying cloud infrastructure, including network, servers, operating systems and storage maintenance, upgrades, and enhancements over time (“Infrastructure Maintenance”), including through the system development and testing, Warranty Period, and any optional Maintenance and Support periods DRB elects. The Offeror will further require that any cloud hosted infrastructure subcontractors provide that major upgrades to the System’s Software and Equipment must be scheduled after advanced prior notice that allows DRB an opportunity to assess the impact and make any needed changes to accommodate the new infrastructure. |  | [ ] Yes [ ] No |
| T5.62 | Policy | The State SSO will be allowed to scan for vulnerabilities against systems in which DRB has the primary responsibility for system and data confidentiality, integrity, and availability. |  | [ ] Yes [ ] No |
| T5.63 | Policy | The Offeror and their subcontractors will allow the State SSO, or its representative, to conduct forensic investigations for both criminal and non-criminal purposes. The Offeror and their subcontractors will ensure that there is no interference with the investigation and will ensure the integrity of the data is maintained throughout the investigation. |  | [ ] Yes [ ] No |
| T5.64 | Policy | Upon DRB’s request, the Offeror and their subcontractors will promptly provide DRB with such assistance and information as is required by DRB in order to comply with any legal obligations to preserve or collect DRB data or information concerning DRB’s use of the Cloud Services or to respond to or otherwise address any inquiry, access request, complaint, enforcement notice, claim, or similar action raised in relation to or made by any or all subjects of DRB data. |  | [ ] Yes [ ] No |
| T5.65 | Policy | The Offeror and their subcontractors will allow DRB to audit conformance to the contract terms. DRB may perform this audit or contract with a third party at its discretion and at DRB’s expense. |  | [ ] Yes [ ] No |
| T5.66 | Policy | The Offeror must complete a security plan and submit it to the State SSO as defined in SOA policy ISP-191 Security in Systems Development. |  | [ ] Yes [ ] No |
| T5.67 | Policy | The Offeror and their subcontractors will give advance notice to DRB of any changes (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. |  | [ ] Yes [ ] No |
| T5.68 | Sizing | The Offeror and their subcontractors will accommodate transaction rates and storage demands that accommodate DRB usage in the Warranty Period and/or during Maintenance and Support services delivery. |  | [ ] Yes [ ] No |