**Appendix E**

**Security and Vendor Questions**

**Agencies:** The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. The Bureau of Information and Telecommunications (BIT) recommends that you utilize your BIT Point of Contact (POC) to set up a planning meeting to review the project and these questions. Understanding the background and context of the questions greatly improves realizing the purpose of the questions. Again, the purpose of the questions is to ensure the product/service being procured will meet the technology and security standards of the state.

If you do not know the details of the technologies the vendor will propose, it is best to keep the question set as broad as possible. If there is a detailed knowledge of what will be proposed, a narrowed set of questions may be possible. Vendors are invited to mark any question that does not apply to their technology as NA (Not Applicable).

**Vendors:** The following questions help the state determine the best way to assess and integrate your product or service technology with the state’s technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). The questions are divided into sections to help identify the point of the questions.

Use the last column as needed to explain your response. Also note, many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been grayed out. **If the vendor answers a question by referencing another document or another part of the RFP response, the vendor must provide the page number and paragraph where the information can be found.**

The “BIT” column corresponds to the division within BIT that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact the BIT division on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contract.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **System/Product:**  **The following questions are relevant for all vendors or third parties engaged in this hardware, software, application, or service.** | | | | | | |
| **Response** | | | | | | |
| **#** | **BIT** | **Question** | **Select all that apply** | | | |
| **1** | DC | Does the proposed solution include the use of email? | Yes  No | | | |
|  |  |  |  | | | |
| **Section A. System Security** | | | | | | |
| **The following questions are relevant for all vendors or third parties engaged in this hardware, application, or service and pertain to relevant security practices and procedures.** | | | | | | |
| **Response** | | | | | | |
| **#** | **BIT** | **Question** | **YES** | **NO** | **NA** | **Explain answer as needed** |
| **A6** | DC TEL  x | The protection of the State’s system and data is of upmost importance. Security scans must be done if:   * An application will be placed on the State’s system. * The State’s system connects to another system. * The contractor hosts State data. * The contractor has another party host State data the State will want to scan that party.   **The State would want to scan a test system; not a production system and will not do penetration testing.**  The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes.  Are either of these an issue? If so, please explain. |  |  |  |  |
| **A8** | POC  x | Will organizations other than the State of South Dakota have access to our data? |  |  |  |  |
| **A18** | DC | Does your company have an executive-level officer responsible for the security of your company’s software products and/or processes? |  |  |  |  |
| **A21** | DC | What is your background check policy and procedure? Are your background checks fingerprint based? |  |  |  |  |
| **A22** | DEV | Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain. |  |  |  |  |
| **A24** | DC  TEL | Do you have an automated Security Information and Event Management system? |  |  |  |  |
| **A25** | DC  TEL | What types of event logs do you keep and how long do you keep them? |  |  |  |  |
|  |  | 1. System events |  |  |  |  |
|  |  | 1. Application events |  |  |  |  |
|  |  | 1. Authentication events |  |  |  |  |
|  |  | 1. Physical access to your data center(s) |  |  |  |  |
|  |  | 1. Code changes |  |  |  |  |
|  |  | 1. Other: |  |  |  |  |
| **A26** | DC | How are security logs and audit trails protected from tampering or modification?  Are log files consolidated to single servers? |  |  |  |  |
| **A27** | DEV | 1. Are security specific regression tests performed during the development process? |  |  |  |  |
|  |  | 1. If yes, how frequently are the tests performed? |  |  |  |  |
| **A28** | TEL | What type of firewalls (or application gateways) do you use? How are they monitored/managed? |  |  |  |  |
| **A29** | TEL | What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed? |  |  |  |  |
| **A30** | DC  TEL | What are your procedures for intrusion detection, incident response, and incident investigation and escalation? |  |  |  |  |
|  |  |  |  |  |  |  |
|  | | | | | | |
| **Section B. Hosting**  **Not applicable for this RFP** | | | | | | |

|  |
| --- |
| **Section C: Database**  **Not applicable for this RFP** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Section D: Contractor Process**  **The following questions are relevant for all vendors or third parties engaged in providing this hardware, application, or service and pertain to business practices. If the application is hosted by the vendor or the vendor supplies cloud services those questions dealing with installation or support of applications on the State’s system can be marked “NA”.** | | | | | | |
| **Response** | | | | | | |
| **#** | **BIT** | **Question** | **YES** | **NO** | **NA** | **Explain answer as needed** |
| **D1** | DC  POC | Will the vendor provide assistance with installation? |  |  |  |  |
| **D2** | DC  DEV  POC  TEL | Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date? |  |  |  |  |
| **D9** | DEV | What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options? |  |  |  |  |
| **D21** | DC  TEL | Do you perform regular reviews of system and network logs for security issues? |  |  |  |  |
| **D37** | DC  TEL | How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated? |  |  |  |  |
| **D38** | DC  DEV | Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom.  Include training specifically given to your developers on secure development. |  |  |  |  |
| **D40** | POC  TEL  x | Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions.  At the State’s discretion, a contractor’s answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the contractor selection criteria. Is this acceptable? |  |  |  |  |

|  |
| --- |
| **Section E: Software Development**  **Not Applicable for this RFP** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **F. Infrastructure**  **The following questions are relevant to how your system interacts with the State’s technology infrastructure. If the proposed technology does not interact with the State’s system, the questions can be marked “NA”.** | | | | | | |
| **Response** | | | | | | |
| **#** | **BIT** | **Question** | **YES** | **NO** | **NA** | **Explain answer as needed.** |
| **F4** | TEL  x | Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines? |  |  |  |  |
| **F5** | DC  x | It is State policy that all systems must be compatible with BIT’s dynamic IP addressing solution (DHCP). Would this affect the implementation of the system? |  |  |  |  |
| **F17** | DC  TEL | Provide a system diagram to include the components of the system, description of the component, and how the components communicate with each other. |  |  |  |  |
| **F24** | DC  TEL | What physical access do you require to work on hardware? |  |  |  |  |
| **F25** | DC | How many of the vendor’s staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Section G: Business Process**  **The following questions pertain to how your business model interacts with the State’s policies, procedures, and practices. If the vendor is hosting the application or providing cloud services, questions dealing with installation or support of applications on the State’s system can be marked “NA”.** | | | | | | |
| **Response** | | | | | | |
| **#** | **BIT** | **Question** | **YES** | **NO** | **NA** | **Explain answer as needed.** |
| **G9** | DC | Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome. |  |  |  |  |
| **G11** | DC | Please summarize your company’s history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected). |  |  |  |  |
| **G12** | DC | Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident? |  |  |  |  |
| **G14** | DC  TEL | Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located? |  |  |  |  |
| **G15** | DC | Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk, and transcription services)? |  |  |  |  |
| **G16** | DC | Is the controlling share (51%+) of your company owned by one or more non-U.S. entities? |  |  |  |  |
| **G17** | DC | What are your customer confidentiality policies? How are they enforced? |  |  |  |  |
| **G21** | DC  TEL | What do you see as the most important security threats your industry faces? |  |  |  |  |