**RFP 21-1788 Clarification**

**INSTRUCTIONS**

***Instructions:*** *Please provide responses to the clarification question(s)/prompt(s) below. Information provided in the clarification responses will be considered as part of the respondent’s proposal. Where appropriate, supporting documentation may be referenced by specific page and/or paragraph number(s). If any of the responses contain confidential information, as defined by IC 5-14-3, please reference the attached confidential material and separate from the rest of this response document. Otherwise, a redacted version of this clarification document will need to be submitted.*

**DUE DATE: September 8, 2020 BY 3:00 PM EDT**

| **Section/Topic** | **Clarification Question** | **Respondent Response** |
| --- | --- | --- |
| Attachment F, Mandatory Requirement 1 | In order to allow your company and the DOR to further evaluate your level of compliance with CAT1 STIG requirements, the State is requesting that you complete and return the attached DISA STIG requirement spreadsheet, compiled and prepared based on your response to Clarification 1. Please be sure to complete all of the tabs in the spreadsheet that pertain to the solution in your proposal.  If you discover that you failed to include any infrastructure or server environment information in your response to Clarification 1, please reach out to us and we will provide those STIGs to you.  Instructions for filling out the DISA STIG requirement spreadsheet:   1. Review attached STIGS for your environment and fill out the spreadsheet tabs pertaining to your proposed solution and environment 2. Do NOT delete or re-order columns (hide them if you wish). You may add columns. 3. Please be aware that DOD Data or sensitive data is just PII/FTI data (SSN, CC#, DOB, for example) 4. Please answer all applicable questions in the spreadsheet, regardless of severity. Answers to all questions must be one of the following and entered in the comments column of the STIG spreadsheet:  |  |  | | --- | --- | | **Status** | **Description/details** | | **Open** | This means you do not strictly comply with the check. | | **Not a Finding** | This means you strictly comply with the check. For example, if you have a password complexity algorithm but it does not meet ALL of the password complexity checks you should mark it Open; NOT "Not a Finding". | | **N/A** | This means that the check does not apply. Any check marked "N/A" requires an explanation in an "N/A Comments" column that you add. Valid reasons for "N/A" include (but are not limited to):  o   Not using DoD root certificate  o   Not implementing PKI  o   Not using IPV6 |  1. If your application or infrastructure is in a cloud, please fill out the attached State IOT Cloud Provider Questions spreadsheet also   **The** **DISA STIG requirement spreadsheet and State IOT Cloud Provider Questions spreadsheet (if applicable) must be completed and returned to the State no later than 3:00 PM EDT on September 8, 2020.** | Fairfax Software has provided the completed DISA STIGS requirement spreadsheet and have included it as part of this Clarification response.  Since our proposal solution is for an on-premise approach, we have not provided the State IOT Cloud Provider Questions spreadsheet. |