Delaware Health
And Social Services

DIVISION OF MANAGEMENT SERVICES

PROCUREMENT

DATE: September 1, 2015

HSS 15 052

DOG LICENSING SERVICES

FOR

DIVISION OF PUBLIC HEALTH

Date Due: October 8, 2015
11:00AM

ADDENDUM # 1

Please Note:

THE ATTACHED SHEETS HEREBY BECOME A PART OF THE ABOVE MENTIONED BID.

Technical Environment Requirements are attached.

Kieran Mohammed
PROCUREMENT ADMINISTRATOR
(302)255-9291

William Ingram
(302) 744-4706

Technical Environment Requirements

4.4 Requirement to Comply with State Policies and Standards

The proposed solution must be fully compatible with the Department of Health and Social Services' technical environment. Vendor solutions that are not fully compliant with State standards may be disallowed.

The Information Technology Publications web page http://www.dhss.delaware.gov/dhss/dms/itpubs.html has links to the DHSS and DTI policies and standards and other documentation. See the "Supportive Documentation for Bidding on Proposals" section.

The DTI Systems Architecture Standard contains information confidential to the State and is not published on the internet. However, DTI has set up an email address which will automatically send a response with this document attached. The email address is sysarch@lists.state.de.us

The application will have at least 3 tiers with the tiers configured and secured as in the sample diagram included in the DHSS Information Technology Environment Standards. Please see State of Delaware Systems Architecture Standard (instructions above) and DHSS Information Technology Environment Standards http://www.dhss.delaware.gov/dhss/dms/irm/files/dhss_it_environment.pdf for more information.

All components of the proposed solution, including third party software and hardware, are required to adhere to the policies and standards described above, as modified from time to time during the term of the contract resulting from this RFP, including any links or documents found at the above referenced web sites.

4.4.1 Authorizations

All contractor staff working on this project will be subject to a Criminal Background Check (CBC). The contractor will be solely responsible for the cost the CBC. DHSS will review the CBC results. DHSS at their sole discretion may request that a contractor staff member be replaced if their CBC result is unsatisfactory.

Contractor staff will be required to fill out DTI's Acceptable Use Policy, Biggs Data Center User Authorization Form, and the Biggs Data Center Non-Disclosure Agreement for necessary authorizations before starting work. Staff working at a secured State site will be issued a security access card by DHSS as per the State Standard.

4.4.2 Architecture Requirements

Securing and protecting data is critical to the State. This protection is required for data whether hosted **onsite or offsite**. As such it is required that the vendor include in the response to this section a proposed architectural diagram(s) in Visio format demonstrating how State data is being secured.

System architecture diagrams are a key component of the proposed system in terms of meeting State architecture requirements. As part of contract negotiations, the selected vendor will work with IRM to produce a final State approved detailed diagram for each proposed environment. These will be included

in the final contract. This will also be made part of a project business case that must be in "Recommended" status prior to contract signature. The project business case is a State responsibility.

4.4.3 State Hosting Requirements

If the proposed solution will be hosted by the State, bidder is instructed to include in their response to this section the following statement, "**Proposing a State hosted solution. Therefore the**

Cloud/Remote Hosting Requirements from section 4.4.4 do not apply and are not addressed in this proposal."

4.4.3.1 Standard Practices

The contractor(s) shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished to the State. The contractor(s) shall follow practices consistent with generally accepted professional and technical policies and standards. The contractor(s) shall be responsible for ensuring that all services, products and deliverables furnished to the State are consistent with practices utilized by, or policies and standards promulgated by, the Department of Technology and Information (DTI) published at http://dti.delaware.gov/information/standards-policies.shtml. If any service, product or deliverable furnished by a contractor(s) does not conform to State policies, standards or general practices, the contractor(s) shall, at its expense and option either (1) replace it with a conforming equivalent or (2) modify it to conform to State policies, standards or practices.

4.4.3.2 Confidentiality and Data Integrity

The Department of Technology and Information is responsible for safeguarding the confidentiality and integrity of data in State computer files regardless of the source of those data or medium on which they are stored; e.g., electronic data, computer output microfilm (COM), tape, or disk. Computer programs developed to process State Agency data will not be modified without the knowledge and written authorization of the Department of Technology and Information. All data generated from the original source data, shall be the property of the State of Delaware. The control of the disclosure of those data shall be retained by the State of Delaware and the Department of Technology and Information.

4.4.3.3 Security Controls

As computer, network, and information security are of paramount concern, the State wants to ensure that computer/network hardware and software do not compromise the security of its IT infrastructure. Therefore, the Vendor is guaranteeing that any systems or software meets or exceeds the Top 20 Critical Security controls located at http://www.sans.org/critical-security-controls/.

4.4.3.4 Cyber Security Liability

It shall be the duty of the Vendor to assure that all products of its effort do not cause, directly or indirectly, any unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by the State of Delaware. Vendor's agreement shall not limit or modify liability for information security breaches, and Vendor shall indemnify and hold harmless the State, its agents and employees, from any and all liability, suits, actions or claims, together with all reasonable costs and expenses (including attorneys' fees) arising out of such breaches. In addition to all rights and remedies available to it in law or in equity, the State shall subtract from any payment made to Vendor all damages, costs and expenses caused by such information security breaches that have not been previously paid to Vendor.

4.4.3.5 Information Security

Multifunction peripherals must be hardened when used or connected to the network. They should be configured to harden the network protocols used, management services, processing services (print, copy, fax, and scan), logging, and physical security. Care shall be taken to ensure that any State non-public data is removed from memory before service calls and/or equipment disposal. Electronic information storage devices (hard drives, tapes, diskettes, compact disks, USB, multifunction peripherals, etc.) shall be disposed of in a manner corresponding to the classification of the stored information, up to and including physical destruction.

4.4.3.6 Mandatory Inclusions for State Hosting

4.4.3.6.1 Network Diagram

The contractor must include a network diagram of the solution including any interfaces between the solution and other solutions. The diagram needs to be clearly documented (ports, protocols, direction of communication).

4.4.3.6.2 List of Software

The contractor must include a list of software (operating system, web servers, databases, etc.) that the State needs to utilize the solution. For example, a certain web browser (IE) or web service technology for an interface. The contractor will include a list of browsers and versions that are officially supported for web applications. The software list will be formatted as follows:

Product Name	Version	Vendor Name	Required for Development?	Required for M&O?

4.4.3.6.3 3rd Party Authentication

The contractor must include a list of any 3rd party authentication solutions or protocols that they support.

4.4.3.6.4 Password Hashing

The contractor must describe the method used by the solution for hashing user passwords. Include items like hash algorithm, salt generation and storage and number of iterations.

4.4.3.6.5 Data Encryption

The contractor must describe the solution's ability to encrypt non-public State data at rest. Include encryption algorithm(s) and the approach to key management

4.4.3.6.6 Securing State Data

The contractor must describe how the State's data will be protected and secured.

4.4.4 Cloud/Remote Hosting Requirements

This section is mandatory for bidders proposing to host systems and/or non-public data outside of the State network. Bidders must respond as required for each subsection below. Failure to respond as instructed may be cause for rejection of the entire proposal. If your firm has questions about this section, please submit in writing as instructed in this RFP.

If the proposed system and/or data will be hosted outside of the State network, bidder is instructed to include in their response to this section the following statement, "**Proposing a Cloud/Remote Hosting solution. Therefore the State Hosting Requirements from section 4.4.3 do not apply and are not addressed in this proposal".**

4.4.4.1 Terms and Conditions Template Requirement

DTI publishes two templates for hosting data. One is for hosting Public data and the other for hosting Non-Public data. Include the appropriate link below depending on the type of data the vendor will be hosting. Public data is generally publishable/available information like State clinic locations. Non-Public data is generally any confidential information which is not publishable or would require specific authorization before release to a third party.

Bidder is instructed to review the following hosting template and sign and scan and include with your response.

Include only one of the following templates in the response to the RFP.

State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

Public
http://dti.delaware.gov/pdfs/pp/CloudandOffsiteHostingTemplatePublic.pdf

-OR-

Non-Public
http://dti.delaware.gov/pdfs/pp/CloudandOffsiteHostingTemplateNonPublic.pdf

All template clauses are mandatory. Complete and sign the template and include with the response to this RFP.

If the bidder can only accept a clause with conditions (Accept Conditionally) or does not agree with (Reject) a clause as written, then please fill out the following Template Exceptions table as part of your response to this section. Clauses that are rejected must include in the Comment the reason why the bidder cannot comply with the requirement as written and what controls are or can be put into place to provide for the same or similar level of compliance.

Cloud and Offsite Hosting Template Exceptions (Example)

Clause #	Response	Comment
3	Accept Conditionally	Our attorney will contact the State within 48 hours in this situation.
8	Reject	The State will not be permitted to perform this type of audit either directly or indirectly through a State-chosen third party with 30 days advance notice. We have a qualified independent IT audit firm under contract that can provide the required information upon 45 days advance written notice.
9	Accept Conditionally	We will disclose all subcontractor firms within 30 days of contract signature. Some of these relationships are in the process of being negotiated.

Any template exceptions listed above will be vetted by DTI prior to contract signature. Individual clauses may be negotiated and updated by the State in the template. In this case, DTI's written approval of the final template version will be attached to the final contract.

If the bidder accepts all clauses as originally specified, bidder will respond to this subsection with "We accept all clauses in the Cloud and Offsite Hosting Template". Do not include the Template Exceptions table in this situation.

Warning: Failure to complete and sign the Terms and Conditions Template or rejection of any clause may result in the rejection of the entire proposal at the sole discretion of the State.

4.4.4.2 Terms and Conditions for Subcontractors

Subcontractors involved in offsite/cloud data hosting are not required to sign the DTI template; however the primary contractor is expected to hold them responsible to the same clauses so that State data is adequately secured. The State's expectation is that the clauses from the appropriate template be included in the subcontractual agreement. In this manner, the subcontractor explicitly agrees to be bound by the same terms and conditions in the DTI templates as the primary contractor. These subcontractor agreements must be approved by the State prior to signature of the contract with the primary contractor.

4.4.4.3 Standard Practices

The contractor(s) shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished to the State. The contractor(s) shall follow practices consistent with generally accepted professional and technical policies and standards.

4.4.4.4 Mandatory Inclusions for Cloud/Remote Hosting

4.4.4.4.1 Network Diagram

The Service Provider must include a network diagram of the user's interaction with the solution and any interfaces between the solution and the State needs to be clearly documented (ports, protocols, direction of communication). The network diagram does not need to contain the inner workings of the solution or proprietary information.

4.4.4.4.2 List of Software

The Service Provider must include a list of software that the State needs to utilize the solution. For example, a certain web browser (IE) or web service technology for an interface. The Service Provider will include a list of browsers and versions that are officially supported. The software list will be formatted as follows:

Product Name	Version	Vendor Name

4.4.5 DHSS-Specific Security Requirements

Sections 4.4.3 and 4.4.4 above are DTI-specific requirements. Following are DHSS-specific requirements that are <u>more strict</u> than the DTI requirements. The requirements in this section are mandatory.

4.4.5.1 Encryption of Data at Rest

Bidder will describe the method(s) for encrypting data at rest in their proposed solution.

4.4.5.2 Encryption of Data in Transit

All data in transit must be encrypted whether transmitted over a public or private network. Bidder will describe the encryption method(s) proposed.

4.4.5.3 Ownership of State Data

All State-owned data (Public or Non-Public) related to services provided under this contract will remain the sole property of the State. De-identified data is not exempted from this requirement. This provision shall survive the life of the contract. Except as otherwise required by law or authorized by the State in writing, no State-owned data shall be retained by the vendor for more than 90 days following the date of contract termination. After the 90 day timeframe the following provisions will remain in effect: contractor will immediately delete or destroy this data in accordance with NIST standards and provide confirming evidence to the State; contractor is expressly prohibited from retaining, repurposing or reselling State–owned data except as otherwise authorized by the State in writing; contractor retains no ongoing rights to this data except as expressly authorized in the contract.

4.4.6 UAT Environment

The UAT environment must be secured at a level equivalent to the security in place for the production environment. It must be sized and architected such that an entire copy of the production files can be copied over into UAT. The architecture must be equivalently configured so that performance and load testing will essentially produce the same results and expectations as testing in the production environment. There is no expectation to mask field values in UAT. Lower environments that are secured in the same manner may be exempt from masking requirements as well however this may be subject to State or Federal requirements that may override this potential exemption.

4.4.7 Masking of Production Data in Non-Production Environments

While securing of production data is of critical importance, migration of that data to non-production environments presents its own set of challenges as lower environments typically are non as secure as production environment. Masking of production data in lower environments usually involves deletion or obfuscation of actual PII-related field values such that they have no meaning as plain text or identifiable method of translation back to the original values. If there are plans to copy production data to a less secure environment, bidder will describe in detail their proposed masking strategy. If there is no expectation that production data will be copied into less secure environments, Bidder will describe their proposed test data generation plans and state clearly in this section that masking of production data is not required under this proposal.

4.4.8 Other Technical Considerations

The State prefers to have a system with a web front-end for a common user interface. Web browser based applications are now considered the only acceptable platform for custom applications development. For proposed COTS (Commercial off the Shelf) solutions, the State prefers those that are web browser based and that:

- Use Microsoft Windows Server as their operating system
- Use Microsoft Internet Information Server (IIS) as their web and application server software
- Use either Microsoft SQL Server or the mainframe DB2 database for their data store (the Microsoft database platform is the preferred platform due to its higher availability and capacity)
- Have been developed using Microsoft C#.NET