**REQUEST FOR PROPOSALS (RFP)**

**CUSTOMER SERVICE CENTER (CSC) SERVICES**

**OS/CSC/15-001-S**

**AMENDMENT #3**

**August 27, 2014**

Prospective Offerors:

This amendment is being issued to amend certain information in the above named RFP. All information contained herein is binding on all Offerors who respond to this RFP. Specific parts of the RFP have been amended. The changes are listed below. New language has been double underlined and marked in **bold (i.e. word)**, and language that has been deleted has been marked with a strikethrough (i.e. ~~word~~).

1. Section 3.2.1 (M), Interactive Voice Response System (IVRS) is deleted as follows:
2. ~~Create automated Customer satisfaction surveys to rate CSC and DHR performance. The survey shall be sent via phone, text, or email and shall be accessible via web or phone.~~
3. Section 3.2.4.3 - Postal Mail/Document Fulfillment Requirement is revised to include letter (C) as follows:
4. **Generate and mail from within the CSC any Correspondence or fulfillment containing PII. Other non-PII related documents, i.e., applications and forms, may be processed at an offsite fulfillment center.**
5. Section 3.2.4.4, Email Requirementis revised as follows:
6. ~~CSRs shall refer any questions that the CSR is unable to answer to the local Child Support office or the CSO via email no later than one (1) Business Day after its receipt. When it is necessary to refer a question or request to the local Child Support office or the CSO, the CSR must notify the Customer of the referral and that the inquiry will be answered by the Administration/office receiving the request~~.
7. **Due to confidentiality, CSRs are prohibited from answering Case specific questions received via email.**   An auto generated Administration specific statement is provided to these types of inquiries and Customers are asked to contact the CSC during Normal Business Hours to speak to a CSR. Answers to general questions are to be provided no later than one (1) Business Day. **Any questions the CSRs are unable to answer must be referred to the respective LDSS, local child Support office or DHR CSO no later than one (1) Business Day after receipt.**

-2-

1. Section 3.3.1, General Requirements, is revised to include letter M (12) as follows:

**12. Alert users via email of the arrival of a new WO assignment.**

1. Section 3.4.3 (A), Customer Satisfaction is revised as follows:
2. Conduct monthly automated Customer Service Surveys regarding Customer satisfaction with both the IVR and CSR services. The surveys shall allow the Customers to rate the quality, timeliness, and other service delivery elements carried out by the Contractor under the Contract. **Surveys shall be conducted on a secure website. Notification to customers selected for surveys may be sent via email or text.**
3. **ATTACHMENT S, TECHNICAL SPECIFICATIONS, Exhibit 1, OPERATIONAL INTEGRATION ROLES AND RESPONSIBILITIES** is deleted and replaced. See the revised ATTACHMENT S below.
4. **ATTACHMENT X, DHR IVR CALL FLOW STRUCTURE** is being added and is included as a separate attachment to this Amendment.
5. **ATTACHMENT Y, EXIT POINT REPORT** is being added and is included as a separate attachment to this Amendment.

**IMPORTANT NOTICE:** Effective September 26, 2014 the Living Wage rates will increase to $13.39 for Tier 1 and $10.06 for Tier 2. The link to DLLR's Living Wage page is:  [**http://www.dllr.maryland.gov/labor/prev/livingwage.shtml**](http://www.dllr.maryland.gov/labor/prev/livingwage.shtml)**.** Per RFP Section 1.34, whereas the Living Wage may change annually, the Contract price may not be changed because of a Living Wage change.

Should you require clarification of the information provided in this Amendment, please contact me via email at [**yvonne.barr@maryland.gov**](mailto:yvonne.barr@maryland.gov) or by telephone at (410) 767-7256.

By:

*Yvonne Barr*

Procurement Officer

|  |
| --- |
| **ATTACHMENT S – TECHNICAL SPECIFICATIONS** |

Solicitation Number: OS/CSC-15-001-S

**Exhibit 1**

# SYSTEMS TESTING AND INTEGRATION

The contractor shall perform services and activities associated with building and maintaining the technical infrastructure, and the testing, integration and migration activities to ensure that all components of the distributed computing environment work together effectively.

The following table identifies the underlying roles and responsibilities associated with systems engineering, testing and integrated services

# Systems Testing and Integration Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Systems Testing and Integration Roles and Responsibilities** | Contractor | State |
| 1. Develop and document engineering, testing and integration requirements and policies. | X | X |
| 2. Develop engineering, testing and integration procedures that meet requirements and adhere to defined policies | X |  |
| 3. Approve engineering, testing and integration procedures |  | **X** |
| 4. Prepare system engineering plans and schedules to support new and enhanced applications, architectures and standards | X |  |
| 5. Review and approve engineering plans and schedules |  | **X** |
| 6. Define and document unit and systems acceptance criteria | X | **X** |
| 7. Conduct testing for all new and upgraded equipment, software or services to include unit, system, integration, and regression testing. | X |  |
| 8. Define and document user acceptance criteria. |  | **X** |
| 9. Perform and approve user acceptance testing for new and upgraded equipment and software. |  | **X** |
| 10. Assess and communicate the overall impact and potential risk to existing operations prior to implementing changes. | X |  |
| 11. Coordinate implementation and migration support activities with the help desk and the Department. | X |  |
| 12. Coordinate the scheduling of all changes to the distributed computing environment through defined change control processes. | X | **X** |
| 13. Conduct pre-installed site surveys, as applicable. | X | **X** |
| 14. Test and stage new and upgraded equipment and software to smoothly transition into production environment prior to going live on the network. | X | **X** |
| 15. Perform project management (including the creation of project plans and management documentation) | X |  |
| 16. Perform data migration from existing systems to new systems. (If applicable) | X |  |
| 17. Provide technical assistance to Department during transitions as needed. | X |  |
| 18. Update configuration management documentation and asset inventory to reflect hardware and software changes. | X |  |
| 19. Provide training to Department personnel as appropriate on new/upgraded hardware/software (e.g. Features of new hardware etc.) as needed. |  |  |

Configuration Management Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Configuration Management Roles and Responsibilities** | Contractor | State |
| 1. Develop and document configuration management tool | X |  |
| 2. Approve configuration management tool. |  | X |
| 3. Document and maintain distributed computing hardware and software specifications and configurations. | X |  |
| 4. Provide information about the configuration, functionality and other aspects of the distributed computing environment upon request. | X |  |
| 5. Track all software versions in use in the distributed computing environment. Document issues and considerations associated with each version and environment. | X |  |
| 6. Ensure that disaster recovery documentation correctly reflects the distributed computing environment. | X | X |

# Operational Integration Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Operational Integration Roles and Responsibilities** | Contractor | State |
| 1. Train Contractor’s employees on systems and operational procedures related. | X | X |
| 2. Train Department’s staff and third-party vendors on contractor’s system(s). | X |  |
| 3. Contractor employees capable of performing mail opening, scanning, and imaging. | X |  |
| 4. Department’s State, local and privatization contractor employees capable of accessing contractor’s data. | X | X |

**Exhibit 2**

**DHR AUTOMATED SYSTEM**

**SECURITY REQUIREMENTS**

# Security Personnel Designation

# In order for an adequate level of security to exist in the DHR application systems an agency data security structure has been developed. The access procedure begins with the DHR supervisors and ends with the DHR supervisors and ends with the DHR security officers of the OIM/DSD. This structure is intended to provide a systematic means for staff to protect data and to gain the proper level of access to DHR’s automated systems.

# The following outlines the responsibilities of each of the key security-related positions in DHR.

# DHR Supervisors responsibilities:

# To determine the appropriate security level(s) for each of his/her employees.

# To complete and forward the appropriate security transaction form(s) to the security monitor when an employee needs to be added to or deleted from a system; have his/her system access level modified; or have a name changed. All forms need to be sent to the security monitor within five (5) working days of the personnel action.

# To ensure the accuracy and completeness of forms.

1. To review at least annually (usually at the employee’s annual performance review or when an employee’s job responsibilities changes) the employees’ current job duties and compare them to the employee’s current security access level to determine if any modification(s) is needed.
2. To communicate when necessary or at least annually to his/her employee’s and others of the need for keeping DHR’s data confidential and their password(s) a secret.
3. To adhere to the security matrix to ensure for a proper separation of duties. If staffing levels prohibit strict adherence to the matrix then to implement a strong supervisory review of employee’s activity to prevent fraud from occurring.
4. To make sure that their employees receive all needed information in regards to protecting the confidentiality of DHR’s data and secrecy of their password(s).

**DHR AUTOMATED SYSTEM**

**SECURITY REQUIREMENTS**

**DHR Employee and Contractor Responsibilities:**

1. To keep his/her password a secret and DHR’s data confidential.
2. To report any system access problem(s) to his/her Security Monitor or supervisor immediately.
3. To read, sign, and abide by the Security Acknowledgment/Advisory Form.

**Security Monitor’s Responsibilities:**

1. To expeditiously review forms (for accuracy and completeness), to sign and forward appropriate security transaction form(s) to the DSD whenever an employee needs to be added to or deleted from a system; have his/her system access level modified; or have his/her name changed. Security monitors are the only staff members authorized to forward Security Transaction Form(s) to the DSD or to inquire about their status.
2. To notify the supervisor and/or the end user of the status of his/her security access request.
3. To report all access problems to the DHR System Support Center or to a DHR Security Officer. Security monitors are the only staff members authorized to call in the DHR System Support Center or a DHR Security Officer concerning system access problems.
4. To remind supervisors to forward all security access transaction forms to the security monitors within three (3) day of an employee entering or leaving a unit or local department.
5. To remind supervisors to monitor an employee’s security access levels for appropriateness to their job responsibilities.
6. To communicate as needed or at least annually to supervisors, staff, and others the requirement that DHR’s data is to be kept confidential and that the passwords are to be kept a secret.
7. To serve as a liaison between the Local Department and the DSD.
8. To review and disseminate all Data Security Policies and Procedures. Primary security monitors must distribute all Security Alerts and other security related information to secondary security monitors.
9. To ensure that the current versions of security transaction forms are being utilized.
10. To attend any scheduled security monitor briefings and training sessions.
11. To ensure adherence to all policies and procedures concerning security access requests.

**DHR AUTOMATED SYSTEM**

**SECURITY REQUIREMENTS**

**LDSS, Modals and Contractor Responsibilities:**

1. To appoint a responsible and conscientious person as the security monitors.
2. To expeditiously (within ten (10) working days) complete, sign, and forward the appropriate security transaction forms to the DSD whenever an employee needs to be appointed or deleted as a security monitor.
3. To expeditiously (within ten (10) working days) notify the DSD of any change in physical location, address, fax number, or voice number of a security monitor.
4. To remind staff as needed or at least annually of the requirement that staff keep DHR’s data confidential and their passwords a secret.
5. To remind supervisors as needed or at least annually (usually at the employee’s annual performance review) to review employee’s current job duties and compare them to the employee’s current security access level to determine if any modification is needed.
6. To remind supervisors, security monitors, and staff to follow all rules, guidelines, and deadlines as specified by policies or management.

**OIM/DSD Responsibilities:**

1. To review and process all security transaction requests within seven (7) working days of receipt.
2. To notify security monitors within fourteen (14) working days in writing or by electronic mail when his or her security requests are completed.
3. To respond to valid verbal security related inquiries within two (2) working days and/or valid written security related inquiries within five (5) working days.
4. To conduct periodic security meetings and training sessions for security monitors, DHR supervisors, and other staff members as necessary.
5. To review, revise, and enforce current security policies and to implement or develop new ones.
6. To maintain the Information Systems Security Handbook and the Standards and Procedures Manual.
7. To remind security monitors and other staff members of the requirement to delete unnecessary logon-ids and to supply security monitors with periodic logon-id listings for review and maintenance.

**DHR AUTOMATED SYSTEM**

**SECURITY REQUIREMENTS**

1. To review and investigate security violation reports from the ADC and IBM/GS.
2. To communicate to staff members and others when necessary or at least annually the requirement that they keep DHR’s data confidential and their passwords a secret.
3. To remove unnecessary logon ids from DHR’s automated systems and to periodically review the necessity of high level logon ids’ access.

**“THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK”**

**Exhibit 3**

**DHR IT Hardware (Desktop Computer) Standards**

*(\*Revised December 2013)*

**Dell** hardware is the standard platform for DHR desktop and notebook/laptop.

Listed below are the current **minimum** hardware, software and warranty requirements. Solicitations to vendors may be greater.

**Desktop Standard**

**Hardware**

* **Business Class Workstation**: Dell **OptiPlex** line
* Processor: Quad Core (3.4 GHz, 8 M cache)
* Memory: 6.0 GB
* Monitor: 24" Wide Screen Flat Panel Monitor
* Graphics: AGP w/8MB video memory
* Hard Drive: 320 GB
* Network Card: 100/1000 Ethernet
* 16X DVD+/-RW
* Mouse: USB
* Keyboard: USB

**Software and Warranty**

* Operating System: Windows 7 Professional 64-bit
* Office Productivity Suite: Microsoft Office 2007 Professional
* **Attachmate Extra! Terminal Emulator v9.x**
* Keep your Hard Drive **– 3 Year**
* Hardware Resource CD
* Warranty: 3 Year Next Business Day Onsite

\*The above DHR standards may change. Coordinate with the DHR-OTHS prior to making any purchases.

**DHR IT Hardware (Notebook/Laptop) Standards**

*(\*Revised December 2013)*

**Dell** hardware is the standard platform for DHR desktop and notebook/laptop.

Listed below are the current **minimum** hardware, software and warranty requirements. Solicitations to vendors may be greater.

**Notebook/Laptop Standard**

**NOTE:** *In an effort to reduce equipment costs and simplify user support requirements, it is the policy of OTHS, that those DHR users who have a need for mobile computing utilize the notebook computer as their sole IT device. This eliminates the need for two separate computers and the associated costs and complexity of supporting multiple devices.*

**Hardware**

* **Business Class laptop**: Dell **Latitude** line
* Processor: Quad Core Mobile – QM (2.7 GHz, 6 M cache)
* Memory: 6.0 GB
* Screen: 14.0” HD+ (1600x900) Anti-Glare LED
* Hard Drive: 250 GB 7200 rpm
* Graphics: nVidia® NVS™ 4200M 512MB DDR3 Discrete Graphics for Quad Core
* Network Card: 100/1000 Ethernet
* Wireless LAN: 802.11 a/g/n
* 8X DVD+/-RW

**Port Replicator/Docking Station & Accessories:**

* Compatible port replicator/docking station for notebook
* Monitor: 24" Wide Screen Flat Panel Color Monitor, Lock Down Cable
* Mouse: Optical USB
* Keyboard: USB

**Software and Warranty Requirements**

* Operating System: Windows 7 Professional 64-bit
* Office Productivity Suite: Microsoft Office 2007 Professional
* **Attachmate Extra! Terminal Emulator v9.x**
* **Computrace Tracking Agent**
* Keep your Hard Drive Option **– 3 Year**
* Hardware Resource CD
* Warranty: 3 Year Next Business Day Onsite
* **Hard-drive encryption solution that is FIPS 140-2 compliant**

\*The above DHR standards may change. Coordinate with the DHR-OTHS prior to making any purchases.