District of Columbia Retirement Board

(DCRB)

Request for Proposal for the Implementation of a Data Management Solution

Solicitation Number: DCRB-14-028

Release Date: July 18, 2014

Eric Stanchfield, Executive Director

900 7th Street, N.W. Second Floor, Washington, DC 20001

SOLICITATION, OFFER, AND AWARD

1. Caption	Page of Pages	
Implementation of Data Management Solution	1	114

2. Contract Number	3. Solicitation Number	4. Type of Solicitation	5. Date Issued	6. Type of Market
RB-14-028	DCRB-14-028	[ ] Sealed Bid (IFB) [X] Sealed Proposals (RFP) [ ] Sole Source [ ] Emergency	7/18/2014	[X] Open [ ] Set Aside [ ] Open with Sub-Contracting Set Aside

7. Issued By:	8. Address Offer to:
District of Columbia Retirement Board Procurement 900 7th Street, NW, 2nd Floor Washington, DC 20001	District of Columbia Retirement Board ATTN: Procurement Office 900 7th Street, NW, 2nd Floor Washington, DC 20001

NOTE: In sealed bid solicitations "offer" and offeror" means "bid" and "bidder"

SOLICITATION

9. Offers submitted via email with 1 copies furnished to the Source Selection Evaluation Board in accordance with the RFP.

proposals were due to be submitted to the identified contact in the solicitation on or by 5:00pm local time 8/29/2014

CAUTION: Late Submissions, Modifications and Withdrawals: See Solicitation. All offers are subject to all terms & conditions contained in this solicitation.

10. For Information Contact ☞	A. Name	B. Telephone (Area Code)	(Number)	(Ext)	C. E-mail Address
	Yolanda Smith	202	343-3200		yolanda.smith@dc.gov

11. Table of Contents

OFFER

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 180 calendar days from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified herein.

13. Discount for Prompt Payment ☞	10 Calendar days %	20 Calendar days %	30 Calendar days %	____ Calendar days %

14. Acknowledgement of Amendments (The offeror acknowledges receipt of amendments to the SOLICITATION):	Amendment Number	Date	Amendment Number	Date

15A. Name and Address of Offeror	16. Name and Title of Person Authorized to Sign Offer/Contract

15B. Telephone (Area Code)	(Number)	(Ext)	15 C. Check if remittance address is different from above - Refer to Section G	17. Signature	18. Offer Date
			[ ]		

AWARD (TO BE COMPLETED BY GOVERNMENT)

19. Accepted as to Items Numbered	20. Amount	21. Accounting and Appropriation

22. Name of Contracting Officer (Type or Print)	23. Signature of Contracting Officer (District of Columbia)	24. Award Date
Eric O. Stanchfield, Executive Director		

District of Columbia Retirement Board

Article I. DCRB Objectives and Requirements

Overview and Background Material

The District of Columbia Retirement Board (DCRB) is responsible for administering the District of Columbia Police Officers and Firefighters' Retirement Plan and the District of Columbia Teachers Retirement Plan (the "Plans"). In order for DCRB to effectively fulfill its mission of providing quality and efficient retirement services to members of the Plans, service and contribution data must be accessible and accurate.

While DCRB is an independent District Agency, it is under U.S. Treasury oversight and therefore must follow both the District as well as the Federal guidelines for data management, security, and Personally Identifiable Information (PII). All integrators and contractors are required to adhere to these standards and provide support in DCRB's efforts to remain fully compliant of process, standards, and governance models.

Section A. – Objectives

DCRB is seeking to modernize the defined benefit retirement service process and provide enhanced member services through the Retirement Modernization Program (the "Program"). The Program's mission is to support DCRB benefit services for all members, and to expand and improve benefit administration capabilities, resulting in the timely and accurate payment of benefits to retirees, survivors, and beneficiaries. The key benefit of the Program is to help facilitate the modernization of DCRB's administrative capability, to provide the timely and accurate payment of benefits, and to enhance services to members by using the data in the District's PeopleSoft system.

The Data Management Project (the "Project") is an initiative within the Program with a focus on providing the necessary tool set for transmitting/receiving, transforming, validating, verifying, reclaiming, cleansing, and storing of data of active plan members facilitating enhancements to their benefits-related services. These tools include an Enterprise Service Bus (ESB), Enterprise Data Quality (EDQ) system, and Master Data Management (MDM) system as well as the services necessary for installation, configuration, and customization; hardware costs; and training of DCRB staff. Each of these three tools is part of the communication chain from the District of Columbia's PeopleSoft Human Resource (HR) system to the DCRB databases.

The Data Management Project was initiated to facilitate the procurement of a toolset for the communications, transformation, validation, verification, and merging of data from the District's PeopleSoft system into the DCRB enterprise. These tools will provide the communication layer, data quality functionality, and a repository of authoritative data on member demographics, service history, and fiscal history. The key benefit of the Project is to help facilitate the modernization of DCRB's administrative capability in providing the timely and accurate payment of benefits and to enhance services to members by leveraging the data contained in the District's PeopleSoft system.

High-level goals for the Data Management Project are:

Enabling the automated transfer of data from the District and U.S. Treasury's PeopleSoft systems to DCRB through secure data transfer

Transforming, validating, verifying, and merging incoming data with authoritative data sets

Monitoring and logging the transmission of data, and generating alerts for system administrators in the event of an invalid or incomplete data record

Providing a storage solution for a master data record for each member consisting of demographics, fiscal (payroll, retirement contributions), and service history (personnel actions, promotions, COLA, etc.)

Ensure that access to the Master Data Record is monitored according to PII standards and record all access of the record into secure logs;

The objective of this request for proposal is for DCRB to select a single software (*integrator)* offeror and solution(s) for its ESB, EDQ, and MDM solution and the services necessary to implement, configure, transition, maintain and customize the solution to DCRB's IT organization. We anticipate awarding a one (1) year firm term contract with 3 one (1) year option periods.

Project Implementation Timeline

DCRB desires to install the three systems by the end of the first quarter in Fiscal Year 2015 (December 31, 2014) and to have the systems fully operational by the end of the second quarter (March 31, 2015). DCRB requires the offeror who is awarded the contract for the services described above submit a timeline in the form of a performance work statement (PWS) in accordance with the standards prescribed in Section D. Deliverables.

Section B. – General Requirements

DCRB Environment

The District of Columbia government currently uses PeopleSoft for the collection of HR related information on all employees. Members in the DCRB Plans are identified "contribute", and their contributions are documented through this system. The data contained within PeopleSoft, along with supporting information in the personnel records, comprise the information necessary to process and provide retirement benefits to members of the plan when they retire. At this point, the data contained within PeopleSoft is accessible by DCRB in a read-only fashion and does not provide the agency with the ability to correct or maintain this information.

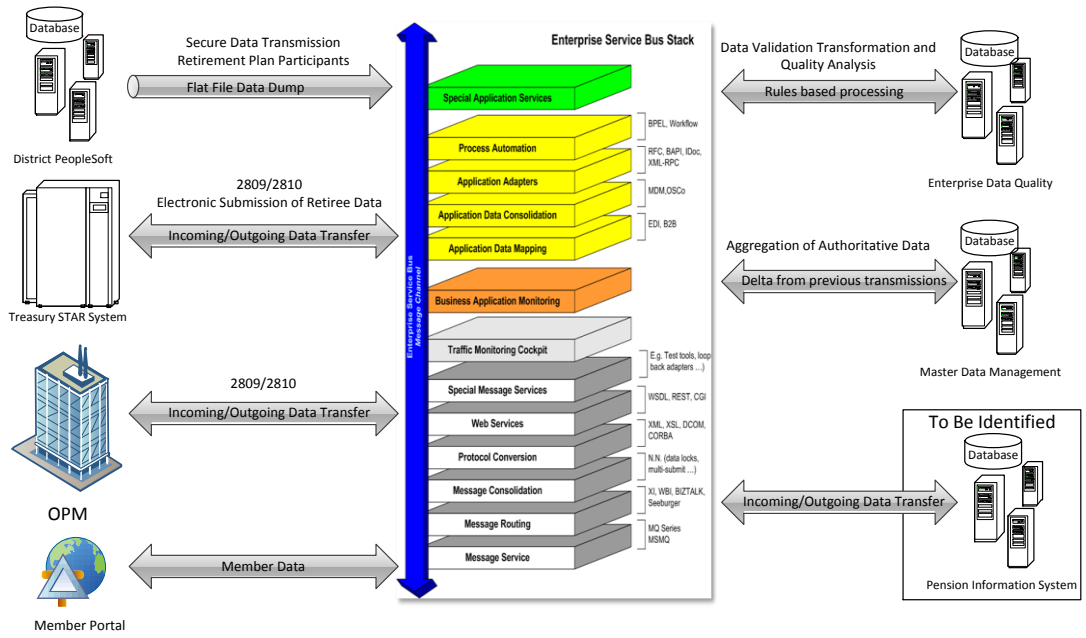
DCRB has defined a need for a Pension Information Management System (PIMS) that will receive a feed of the HR data on members and enable the Benefits Department to manage retirement related information for members including the ability to calculate retirement benefits, provide an annual statement for each member and reconcile fund contributions with the data provided to DCRB from the Office of Chief Financial Officer (OCFO). The final state of the environment will have a Pension Information Management System (PIMS) that DCRB's Benefits Department can leverage to efficiently and effectively process requirements. To reach the state that a PIMS system can be implemented, a set of products and processes must be implemented.

To facilitate the implementation of a PIMS, data will have to be transferred and updated on a regular basis to reflect the current state of all employees. The transmission of these data elements requires three basic components:

- Communications Layer
- Quality Assurance
- Master Data Repository

Together, these components will enable data to be transmitted, transformed, validated, and aggregated into a single, authoritative repository of member data. Each tool will provide a mechanism to support the data flow and together will provide a single stream of processes that will ensure data input from the District and Treasury are output to a master data record to be governed according to the DCRB data management policies. This master record will be used as part of a data feed to the DCRB PIMS system once that system has been selected and installed.

The proposed solution will support the following high level data flow:



Current Environment

DCRB operates a multi-site data center leveraging a high-availability infrastructure with an extensive use of virtualization technology, where possible. DCRB follows Information Technology Infrastructure Library (ITIL) standards for management of IT operations including Incident Management, Change Management, and root cause analysis. As such, the implementation and configuration of new systems will be architected and approved step-by-step through the Change Advisory Board (CAB) to ensure that the enterprise architecture is managed in an effective and efficient manner.

Primary Applications

DCRB has defined the following applications in the table below as sources and/or consumers of master data. A description of, and purpose for, each application is included.

Table 1. Applications That Integrate with MDM as Sources or Consumers of Data

Application Name	Data Source/Consumer/Both	Description
PeopleSoft	Source	District of Columbia's human resource (HR) System
STAR	Both	US Department of Treasury's retirement system (PeopleSoft)
SFTP	Source	DCRB's Secure File Transfer Protocol (Global Scape) repository

Application Name	Data Source/Consumer/Both	Description
FileNet	Both	DCRB and the District of Columbia leverage FileNet for the storage of scanned images.
SharePoint (2010/2013)	Both	DCRB uses SharePoint for workflow management, document storage, and data management
Project Server (2010/2013)	Both	Programs and projects are managed through Project Server at DCRB. Projects contain schedules, task information, performance measures and document repositories.
Microsoft Dynamics GP – Future	Both	Financial system
Tamale – Future	Both	Investment management system

Current Infrastructure and Standards

DCRB's network is expanding rapidly as new products and services are offered to the organization. As such, both scalability and security are crucial to the success of the organization. DCRB's IT organization provides full internal support to the agency as a whole and will support the data management solution once it is fully operational. All products, operating systems, and drivers must be compliant with Federal standards for security (NIST 800.53 and FIPS 199/140.2) and with Personally Identifiable Information (PII) policies in Appendix D of this solicitation (DCRB follows federal standards for PII data as posted in the FAR). In addition, offerors must provide training and best practice standards to DCRB for internal support of products and services.

DCRB has developed both an as-is as well as a to-be enterprise architecture. Details of this architecture will be provided to the selected offeror for their reference when architecting the final solution. All proposals are requested to provide high-level architectural diagrams based on industry standard networks. Virtualization should be leveraged where feasible and should be in line with best practices.

The final solution will encapsulate all three products (ESB, EDQ, and MDM) as well as the services necessary for installation, integration, configuration, training, and transition to operations. The implemented solution will be required to comply with DCRB's enterprise architecture and must integrate into DCRB's as-is and to-be enterprise architecture and meet the following infrastructure requirements:

1. Server Requirements
    a. Solution may leverage either a physical or virtual environment
    b. Offerors must recommend a best practice architectural design with their proposed solution (a diagram must be included as part of the proposal).
    c. Offeror will be required to provide hardware specifications with alternatives.
    d. If a virtual server architecture is proposed and it leverages an Intel based chipset, DCRB would prefer a system that runs in a VMware-clustered environment.
2. Network Requirements
    a. The solution must offer high availability (99.95%) of up-time as measured through performance measurements defined in the Service Level Agreements (SLA)
    b. The system must support redundant network connections
    c. The EDQ and MDM system must be IP based
    d. The system must support 1/10 Gig connection
    e. The system must allow for throttling network bandwidth
    f. The system must enable batch management based on scheduled or real-time
    g. The system must support implementation of applications (ESB, EDQ, MDM) on separate subnets through the DCRB enterprise environment
    h. The offeror must provide network utilization expected benchmarks for the system in advance.
3. Software (OS) Requirements
    a. The solution shall be capable of running on a Unix/Linux Based Operating System (OS)
    b. The offeror must provide hardware specifications and pricing as part of the proposal.
        i. Alternative specifications must also be provided in the event DCRB chooses to purchase hardware separately.
4. Databases
    a. The ESB, EDQ and MDM solutions must be optimized to run on an Oracle database
    b. DCRB currently has Enterprise licenses for Oracle that will be used as required for this RFP. Oracle Database Licenses are not to be included in the price proposal.
5. High Availability
    a. The system must be clustered for high availability operations
    b. The database architecture must support active/active (utilizing Oracle Dataguard) synchronization
    c. The ESB System must be load balanced to maximize high availability across primary and secondary sites to ensure high availability

   d. The ESB solution and proposed architecture must account for the future use of hardware based load balancers (should DCRB choose to implement a load balancing solution)
   e. The system must support 99.95% availability
   f. The architecture must be built on an Event Driven Service Oriented Architecture (SOA).
6. Disaster Recovery
   a. The solution should conform to and operate within a DR Solution leveraging NetBackup and Vmware's Site Recovery Manager solution if the hardware is virtualized
   b. The final solution must be configurable to meet industry standards for Disaster Recovery and will be included in DCRB's Disaster Recovery plan.

Description of ESB Objectives

The Communications layer is facilitated by an Enterprise Service Bus (ESB) that operates as a highway of information. An ESB receives and transmits data from industry standard and custom communication interfaces in various file and data stream formats. The ESB automates the input and output of data through systems and ensures that data received is transformed into formats necessary for output to systems and databases.

DCRB will leverage an ESB to both communicate with systems outside of our network as well as to provide a layer of communication between internal systems. Internal databases and applications will all send and receive data through the ESB in eXtensible Markup Language (XML) format, while external systems will transmit and receive data packets in various industry standard forms as well as communication protocols.

Multiple external sources of data have been identified at DCRB including PeopleSoft data feeds from the District of Columbia and the United States Department of Treasury. Data feeds will be both push and pull communications and will be received in industry standard data formats (XML, CSV, JSON, etc.)

The ESB will also operate as the primary internal communication channel and will transfer data from external sources to the EDQ. The ESB will then operate as an internal channel from the EDQ to the MDM or to other data repositories. At a later date, a PIMS will be installed, and data will be transmitted from the MDM to the PIMS via the ESB.

Description of EDQ Objectives

DCRB receives a number of data feeds from various sources. Two initial feeds that will be implemented will be a feed from the District of Columbia's PeopleSoft Human Resource system for active members as well as a feed from the U.S. Treasury's PeopleSoft system on retired members. The combination of these two data sources into a single master data record is the primary objective of this effort.

In the flow from the District of Columbia, a data extract will be transmitted from the District's PeopleSoft Human Resource system. This feed is a complete snapshot of the database after each payroll period has been completed. Once the feed is received it will go through a quality assurance process supported by the EDQ tool. The EDQ will take multiple streams of data, and through the use of libraries, rules, and protocols, the EDQ will transform, verify, and validate each data element to ensure that it meets standards such as proper value, formatting, data structure, and the enforcement of unique valuations. The EDQ receives raw data as an input, aggregates multiple feeds, and outputs to a single master record stored in the MDM.

For each data feed, the EDQ will regularly check the feed for changes (deltas) and will only update the MDM with changed data sets. In addition, data correction processes have been developed. These corrections are stored in an Excel data file and will be merged into the data feed to correct known issues. The data correction files will be updated on a regular basis and will be part of the quality assurance process.

To facilitate efficient processing, the EDQ will enable for workflow and error routing to the quality assurance team for notification and correction of data flagged by a business rule. Workflow approvals will need to be open ended so that they can be modified on an ongoing basis and the appropriate resources can be included. The MDM solution will have an interface that facilitates the correction of data points where necessary and will log each correction. Corrections should also be updated in the business rules engine so that the system automatically corrects the data point in subsequent data feeds.

In addition, DCRB will define business rules to be executed by the EDQ, and the system will use a rules-based engine to perform data quality checks and verification. The EDQ will be used with various data packets received from multiple external and internal entities. The EDQ will be connected to an ESB that will transmit and receive all data. In addition, the system will perform multiple data checks, validation, and verification processes including analyzing data for changes in data (deltas), cross-checking information across multiple look-up sources, and identifying errors in the data to be further analyzed by quality engineers.

Description of MDM Objectives

The MDM will receive data processed by the EDQ and transmitted through the ESB. The system will provide governance over the data set to ensure that any changes to data are logged, performed with appropriate authority, and meet the necessary standards for the system. For the purposes of the Retirement Modernization Program, the MDM will be a multi-domain system that allows for customized, multiple master data models such as a member, financial, or retirement plan. These models operate under a strict set of guidelines and constrain changes to ensure that the data stored is governed in such a way as to ensure consistency and data accuracy.

The MDM will provide governance over member records to ensure that modifications, additions, or deletions are documented and accomplished only through approved processes. It will receive data from the EDQ via an ESB transport layer and will only merge approved data. The MDM will be the

authoritative source of data for DCRB members and, as such, must control and document all changes to records. The DCRB member data includes Personally Identifiable Information (PII) and therefore will need to have appropriate protections enabled.

The MDM will eventually be used to also store investment information including financial transactions, company profile data, annual financial reports, stock prices, and daily positions. This additional data model must be supported through a multi-domain MDM solution.

MDM offerors should provide some functionality in the following areas:

- Comprehensiveness and flexibility in data modeling (including metadata management support)
- Support for hierarchy management
- Data modeling and metadata
- Hierarchy management
- Data quality
- User interface (data maintenance)
- User interface (data stewardship)
- Data loading, integration, and synchronization
- Business services and workflow
- MDM architecture
- System architecture, security, and administration

Service Level Agreement Management

Performance Measurement

All supported applications must be available and operational based on the performance measurements listed below. Upon contract award, DCRB will evaluate Offeror's performance using this metric as a baseline to determine the effectiveness of the Offeror's performance.

Measurement	Minimum Performance Standard	Expected Performance Standard
Availability of Critical Applications/Systems	98.78%	99.95%
Availability of Servers	98.78%	99.95%
Backup Restoration	Less than 2 hours for 95% of all events; less than 8 hours for 100 % of all events	Less than 1 hour for 95% of all events; less than 4 hours for 100 % of all events
Downtime Frequency (All servers)	No more than 7 events per month	No more than 3 events per month

Time to Respond	Immediate response for all Critical incident events whether onsite or on call	Unless mutually agreed otherwise for specific systems or applications: Critical incident: No more than 15 minutes for 100% of all events whether onsite or on call

Support Response Times

Critical and high priority incidents require that DCRB IT management is notified within an hour and three hours respectively. The procedures associated with critical and high priority issues include email notifications to designated management team members and setting up a conference bridge to resolve the issues identified.

Priority Level	Ticket Acknowledgement	Target Resolution time	Escalation Threshold	Customer Reporting Frequency	Root Cause Analysis (RCA) require
Critical	Immediate	4 hours	1 hour	Every 1 hour	Yes
High	Within 1 hour	8 hours	4 hour	3 hours	No
Medium	Within 8 hours	3 days	1 week	1 day	No
Low	Within 8 hours	1 week	1 week	3 days	No

The offeror's Service Desk personnel will assign the correct priority level to the reported incident i.e., critical, high, medium, or low:

- **Critical**: Complete failure of production servers, service, software, equipment, network component or business critical system(s) preventing the operation of key business applications or seriously impacting normal business operations. The incident affects a group, groups of people or a single individual performing a critical business function. No work around is available and the outage has a very high business impact.

- **High**: Partial or substantial IT service, system, or component failure causing impacts to the agency's ability to operate significant business processes or applications. Business operations are severely disrupted or limited. No work around is available. This constitutes a high business impact.

- **Medium**: Component or single user failure not affecting the agency's or user's ability to operate significant business operations. Reasonable work around or manual processes are available.
- **Low**: Incidents that minimally affect the operation of any IT systems throughout the enterprise. Reasonable work around or manual processes are available.

Support Hours

The Offeror support staff will be available for maintenance support services during the following hours:

Classification	Hours of Service
Normal Support	8:30 AM to 5:00 PM EST, Monday – Friday
After Hours	This time period will be used for critical operational support, maintenance and support that requires application and system downtime.

Section C. – Mandatory Requirements

Items listed in the Functional Requirements (See Appendix A) marked Mandatory ("M") and the Security Requirements under Section VI. Technical Proposal is deemed mandatory requirements. Offerors are required to meet the mandatory requirements in order to be considered. Offeror(s) who fail to satisfactorily meet the mandatory requirements will not be further considered for contract award. The Functional and Security Requirements must be submitted with the Offeror's Technical Proposal as a separate item allowing DCRB to evaluate these requirements.

Section D. – Deliverables

The following details the deliverables/services to be provided to the District of Columbia Retirement Board in performance of a subsequent contract. The Offeror shall provide detailed descriptions on how it plans to meet each of the deliverables in its technical response. All deliverables shall be provided to the Director of Information Technology who shall serve as the Contracting Officer's Technical Representative (COTR) for this Contract or his designee.

Deliverable	Description	Submittal Requirements	Format	Schedule
Network Analysis	Offeror is required to perform an analysis of DCRB's existing Information Technology infrastructure, including but not limited to, its architecture, databases, and disaster recovery platform. Upon completion of analysis, the Offeror shall provide DCRB with a written report detailing the readiness of its infrastructure to support the addition of its proposed solution and identify any gaps that require additional work to be performed.	Report	MS Word	90 days upon contract award
Revised Performance Work Statement (PWS)	Offeror shall provide a revised timeline post award pursuant to discussions with DCRB to meet the standards and objectives of the contract effort identified in Section A. Project Implementation Timeline.	Report	MS Project Server or equivalent	30 days after Network Analysis
Weekly Status and Quarterly Review Reports	Offeror is required to prepare and submit weekly status and quarterly review reports, and participate in weekly and quarterly meetings with the COTR and DCRB IT staff. The COTR will schedule and facilitate weekly and quarterly meetings either onsite and via remote conferencing. A weekly meeting schedule will be identified during the project kickoff meeting. During the one hour weekly meeting the Offeror's Primary Consultant will be responsible for reporting on the status of the project.	Email	MS Word	Weekly/ Quarterly

Project Management Plan	As part of the governance and operating procedures, a comprehensive and detailed project management plan shall be developed, specifically for enhancement services, outlining the implementation schedule (test and development environments), testing in the test and development environments, and deployment. Each project plan shall identify appropriate end user training (i.e., administrative, etc.)	Email	MS Word	
Requirements Document	As part of the governance and operating procedures, a comprehensive requirements document that includes operational processes, governance, architecture, and technical solutions should be completed. Stakeholders will be made available to ensure timely completion of the requirements gathering tasks	Email	MS Word	
Training plan and related materials	Offeror shall provide end user training to DCRB staff designated by the COTR. Training shall include but not be limited to technical and support training. Training will be provided as needed.	Training: Person/Consultant Materials: Email	Training: In a format agreed upon between DCRB and Offeror Materials: Agreed upon between DCRB and Offeror	As needed
Installation (Systems)	Offeror shall install hardware and software for solution (ESB, EDQ, MDM).	As required by the manufacturer and in consultation with the COTR	As required by the manufacturer and in consultation with the COTR	

Maintenance (Software)	Offeror shall install manufacturer required patches, system updates, upgrades, and hotfixes to ensure software application is operating using current technological capabilities and at its maximum capacity. For application maintenance that is not mandated by the software manufacturer, Offeror shall collaborate with DCRB to implement required maintenance tasks.	As required by manufacturer and in consultation with the COTR	As required by manufacturer and in consultation with the COTR	As required
Adoption Strategy	As part of the governance and operating procedures, a comprehensive adoption strategy which shall include but not be limited to how the newly implemented capabilities become part of the day-to-day tools of end users, which features changes as a result of the implemented software and how to translate this change into the agency's business processes.	Email	MS Word	
Roadmap Document	As part of the governance and operating procedures, a comprehensive roadmap document that include a strategic approach for future implementation, configuration, training and reporting recommendations for items NOT addressed during this initial engagement.	Email	MS Word	
Enhancement Services	Offeror shall collaborate with DCRB to identify system capabilities that would provide opportunities for the agency to leverage its existing enterprise environment. COTR shall provide a separate scope of work and negotiate separate tasks with Offeror as requested.	As agreed upon between DCRB and Offeror	In a format agreed upon between DCRB and Offeror	As requested by DCRB

Section E. – Proposals

Schedule of Events

The following is the schedule of events this RFP process. Dates listed below may be amended as appropriate by DCRB and changes will be made provided in writing.

Activity	Scheduled Date
Release of RFP	July 18, 2014
Deadline for Written Questions	July 31, 2014
Response to Written Questions	August 6, 2014
Pre-Proposal Conference	August 12, 2014
Response to Pre-Proposal Conference Questions	August 15, 2014
Proposal Due	August 29, 2014

Section F. – Pre Proposal Conference

On August 12, 2014, at 10:00 a.m., DCRB will hold a Pre-Proposal Conference with prospective bidders at 900 7th Street, NW, 2nd Floor, Washington, DC 20001. The purpose of this conference will be for DCRB's representatives to explain its needs and to receive suggestions and recommendations from those attending. Prospective offerors may submit written questions in advance to Yolanda Smith, via email at Yolanda.Smith@dc.gov, no less than 3 business days prior to the conference. Prospective offerors wishing to attend the conference must contact Ms. Smith no less than 48 hours in advance of the conference to gain access to the event.

A complete record of the conference will be made and posted on the DCRB web site (www.DCRB.dc.gov). Please note that any remarks or explanations at the conference shall not qualify the terms of the solicitation and the terms of the solicitation will remain unchanged unless the solicitation is amended in writing.

Section G. – Questions and Amendments

All Offeror questions must be submitted in writing via e-mail to Yolanda Smith.

Questions will not be accepted via telephone. No oral communication provided by any DCRB staff will be considered binding on DCRB. This RFP is issued by DCRB and is subject to the Board's lock-out rule (Appendix B), procurement and conflict of interest rules (Appendix C). Further, from the issue date of this RFP until a successful Offeror is selected, there shall be no communication by Offerors with any DCRB Board or staff members other than the DCRB designee. Failure to comply with this provision of the procurement will result in Proposal rejection and disqualification.

Any interpretation, correction or change to this RFP will be made by an amendment issued by DCRB. Interpretations, corrections or changes to the RFP made in any other manner will not be binding.

No amendments will be issued by DCRB within 48 hours of the final submission date and time without a corresponding extension of the submission deadline.

For all matters and questions relating to this RFP the point of contact is:

Name:	Yolanda Smith
Address:	District of Columbia Retirement Board 900 7th Street NW; Suite 200 Washington, D.C. 20001
Telephone:	(202) 343-3200; Fax: (202) 566-5000
E-Mail:	Yolanda.Smith@dc.gov

Section H. – Proposal Preparation, Submission, and Evaluation

I. General

To expedite the evaluation of offeror responses ("Proposals"), it is essential that Offerors follow the format and instructions contained herein. Failure to respond in this manner may render the proposal, at the sole discretion of DCRB, as non-responsive or otherwise unacceptable and may result in disqualification and the elimination of the Offeror from consideration.

DCRB will not be liable for any costs incurred by the respondents in preparing responses to this RFP or for negotiations associated with award of a contract.

It is the sole responsibility of the respondents to ensure that their responses arrive in a timely manner. DCRB reserves the right to reject any late arrivals.

All Proposals submitted become the property of DCRB and may be subject to public disclosure under the Freedom of Information Act ("Act").

II. Submission of Proposals

Offerors must prepare and submit both a separate technical proposal and a price proposal. Offerors are responsible for submitting the proposal, and any modification, or revisions, so as to reach the DCRB office designated in the solicitation by the time specified in the solicitation.

All proposals shall be submitted via email to the Point of Contact identified in this solicitation in their entirety.

An initial validation of all proposals received will be conducted, before they are distributed for evaluation, to ensure that all the requirements for format, content, and page limits established in the solicitation have been met. Offerors may not use subcontractors.

The DCRB reserves the right to reject any proposal that does not substantially comply with these proposal preparation/submission instructions.

III. Withdrawal/Modification(s) of Proposals

The offeror or an authorized representative may withdraw proposals by written notice received at any time before award. The withdrawal is effective upon receipt of notice by the contracting officer. Proposal modification is a change made to a proposal before the solicitation's closing date-and time, or a change made in response to an amendment, or made to correct a mistake at any time before award.

Proposal revision is a change to a proposal made after the solicitation closing date, at the request of or as allowed by a contracting officer as the result of negotiations.

The offeror must propose to provide all items in order to be deemed responsive to this solicitation.

1. The offeror shall submit the proposal in response to this solicitation in English.

2. The offeror may submit modifications to the proposal at any time before the solicitation closing date and time, and may submit modifications in response to an amendment, or to correct a mistake at any time before award.

3. The offeror may withdraw its submission proposal at any time before award.

4. Proposals received in response to this solicitation will be valid for up to 120 days from the receipt of the proposal.

IV. Method of Proposal Submission

The offeror's proposal must be submitted electronically via email no later than 5:00 PM Eastern Daylight Time on **August 29, 2014**. Offerors must comply with the detailed instructions for the format and content of the proposal(s); if the proposal(s) does not comply with the detailed instructions for the format and content, the proposal(s) may be considered non-responsive and may render the offeror ineligible for award.

Name:	Yolanda Smith
Title	Contract Specialist
Address:	District of Columbia Retirement Board 900 7th Street NW; Suite 200 Washington, D.C. 20001
Telephone:	(202) 343-3200; Fax: (202) 566-5000
E-Mail:	Yolanda.Smith@dc.gov

V. Proposal Format

To maximize efficiency and minimize the time for proposal evaluation, it is required that the offeror submit the proposal in accordance with the format and content specified herein. The electronic proposal shall be prepared so that if an evaluator prints the proposal it meets the following format requirements:

1. 8.5 x 11 inch paper · Single-spaced typed lines · No graphics or pictures other than those required · Tables are allowed for the list of key personnel · 1 inch margins · Times New Roman 12-point font in text · No hyperlinks · Microsoft Word 2003 software or later version· The offeror shall insert their company's name in the filename; all files named with the file extension .doc

2. Information provided on any other sized paper besides 8.5 x 11 inch paper, will not be evaluated. Instructions regarding use of certain electronic products listed herein should not be construed as DCRB's endorsement of specified products.

3. Page Numbering: The offeror shall use a standard page numbering system to facilitate proposal references. Charts, graphs and other insert materials shall be page-numbered as part of the page numbering system.

4. Page Limitations: Each technical proposal, not including title pages, cover pages, and introductions cannot exceed 40 pages. When a page is designed to print on both sides of a sheet, it shall be counted as two pages. Included in the page count are separate pages providing graphics, charts, illustrations and pictures.

5. Cover Page, and Table of Contents: Each proposal will include a cover page and a table of contents. The cover page shall identify the solicitation number and title, and the offeror's name. The table of contents shall identify, by content, the page number of each section of the proposal. *These pages will not be counted toward the page limitation requirement.*

Proposals should be as succinct as possible while providing an accurate picture of the offeror's ability to meet the needs of DCRB in a thorough, accurate, responsive and cost-effective manner.

All offerors must submit both a separate technical proposal and a cost proposal.

Integrators must address all information specified by this RFP. All questions must be answered completely. DCRB reserves the right to verify any information contained in the offeror's RFP response, and to request additional information after the RFP response has been received.

Marketing brochures included as part of the main body of the bid response shall not be considered. Such material must be submitted only as attachments and must not be used as a substitute for written responses. In case of any conflict between the content in the attachments and an offeror's answers in the body of the proposal, the latter will prevail.

The proposal will consist of:

- Title Page – 1 page
- Covering Letter – 1 page
- Offeror Profile and Demographics – 1 page
- Technical Proposal: General Requirements – 40 Page Maximum
    - Table of Contents
    - Description of Solution
    - Product Capabilities and Functions
    - Product and Service History
    - Product Support and Service Warranty
    - Product Upgrades and New Version Releases
    - Solutions from Cloud Providers
    - Training
    - Skill Set Requirements of Personnel
    - Key Personnel
    - Organizational and Consultant Conflict of Interest (OCCI) Mitigation Plan
    - Performance Work Statement (PWS)

  - Proposed Architecture
  - Past Performance
  - Security Requirements
- Requirements Matrix (Excel) – 60 Page Maximum
- Price Proposal (Separate from Technical Proposal)
  - Narrative – 5 page maximum
  - Price Worksheet

VI. Technical Proposal

The technical proposal is made of up two sections — Section 1: General Requirements, and Section 2: Functional Requirements, generic enterprise architectural diagram based on a best-practices based Windows network with two physical sites operating behind the DC Net network. The architecture should demonstrate how the solution would integrate into an enterprise network, the location of physical servers in relation to firewalls, DMZ, and Storage Area Networks (SAN) as well as a virtualization strategy where appropriate. Answers within the General Requirements section should be limited to a maximum of three paragraphs and should address every point as directly and factually as possible. Lengthy narratives should not be inserted into the body of a direct response.

The offeror will provide services to install, integrate, and transition the solution to the DCRB IT Operations organization. Once the solution has been transitioned, DCRB IT will support the system on a day-to-day basis. Additional support from the offeror or software provider may be necessary for the daily support of the system. The proposal shall be limited to the following:

Section I. General Requirements

Cover letter

The proposal must include a cover letter signed by an individual legally authorized to bind the respondent to both its technical and price proposals. The cover letter should contain the solicitation number, name, title, address, email address, and phone number of the person(s) who are authorized to represent the Offeror and to whom DCRB should direct follow-up correspondence.

Description of Solution

Based on the requirements for information contained in this document, please provide a general description of your proposed solution for DCRB's Data Managed platform. Please itemize and describe *all* hardware, software and service components required.

Product Capabilities and Functions

In addition to the requirements stated above, please detail any other product capabilities and functions that may be of interest to DCRB. Offeror shall include in its description how the system(s) are leveraged collectively and individually to maintain high availability in accordance with the Service Level Agreement Management section of this RFP.

Product and Service History

Offerors should describe the history of current solutions, including initial release date, current version number and development history (that is, if they were developed as a marketable package or as a solution for a particular organization).

Offerors shall indicate whether *any or all* source code for the application will be made available to DCRB or, if it will not be available, they must name the software escrow service used, give contact information and describe company policy regarding software escrow updates.

Offerors shall provide detailed information on the direction of product development, including a road map and timeline of planned future functionality.

Offerors shall indicate which third-party software packages are required for their services to function correctly (for example, libraries, data quality, data integration, agents or clients for backup, software distribution and security), and should indicate if DCRB, itself or a third party service provider will be responsible for purchasing and maintaining licenses for this software.

Offerors should provide a list of any user associations or public discussion areas relating to the product or service offerings.

Product Support and Service Warranty

Offerors should describe the support offerings available for the total solution and any associated products. In addition, they should provide a copy and description of all warranties associated with the products to be implemented.

Product Upgrades and New Version Releases

Offerors should describe:

- The process and cadence of new version releases and the application of service packs to the production system;
- The quality assurance/testing processes that are followed to determine whether an upgrade or custom modification is suitable for release;
- The process by which tests for confirmed problems/bugs are incorporated into the quality assurance/testing processes for future releases;
- The process by which opportunities for system enhancements are identified, screened, programmed, field-tested and released to users; and
- Whether the upgrade methodology includes a tracking system to report on the status of the upgrade and record problems/bugs.

Proposed Architecture

Offerors should provide an architectural diagram demonstrating how the products should be installed in a generalized enterprise environment with primary and failover site. The diagram should including depiction of where products reside in relation to firewalls, DMZ, and redundant servers/virtualization at the failover site. The diagram should show, at a high level, the recommended (best practice) installation and integration of all products into an enterprise environment. Virtualization should be leveraged where feasible and should be in line with best industry practices.

Solutions from Cloud Providers

Offerors should describe their experience with implementing their software in a cloud environment and/or provide details of any cloud services their organization provides. All cloud driven solutions should include an architectural diagram showing security, scalability, and virtualization strategies as well as depicting the internal location for any components or interfaces installed at the client site.

Training

Offerors should describe what training and other formal support of DCRB staff is required or recommended to support the implementation of their products and services. Information on training should include proposed content, duration, expected knowledge of participants, and objectives of courses.

Skill Set Requirements of Personnel

Offerors should describe the skills needed to implement and support their product, as outlined in this proposal.

Key Personnel

The Offeror must include the following information about each of the key personnel who shall serve as the Primary and/or Co-Primary Contractor(s) and will be *substantially devoted to one or more of the tasks throughout the period of performance* the DCRB activity for which it is submitting a proposal. The Offeror shall identify the Primary and/or Co-Primary Contractor(s) in accordance with Article II. General Terms and Conditions, Section H. of this solicitation:

- Individual's Name;
- Position Title with brief description;
- Years of Professional Experience;
- Highest Degree Attained/Degree Area;
- Relevant Professional Certifications; and
- Anticipated Role and Responsibilities on the DCRB contract.

Organizational and Consultant Conflict of Interest (OCCI) Mitigation Plan

Offerors shall identify any and all potential or actual conflicts of interest. This includes actual or potential conflicts of interest of proposed subcontractors. If it is believed that conflicts of interests are either real or perceived, a mitigation plan shall be developed and submitted to the Contracting Officer as part of your proposal submission. The Offeror's plan shall describe how the Offeror addresses potential or actual conflicts of interest and identify how the Offeror will avoid, neutralize, or mitigate present or future conflicts of interest.

Offerors must consider whether their involvement and participation raises any OCCI issues, especially in the following areas when:

1. Providing systems engineering and technical direction;
2. Preparing specifications or work statements and/or objectives;
3. Providing evaluation services; and
4. Obtaining access to proprietary information.

If a prime Contractor or subcontractor breaches any of the OCCI restrictions, or does not disclose or misrepresents any relevant facts concerning its conflict of interest, the DCRB may take appropriate action, including terminating the contract, in additional to any remedies that may be otherwise permitted by the contract or operation of law.

Performance Work Statement (PWS)

Offerors must prepare and submit a PWS for the specific activity for which it is submitting a proposal and wishes to be considered for award. Please note the DCRB has adopted the Project Management Institute Project Management Body of Knowledge as its standard and offerors should use this framework when preparing their response to this section.

Each PWS, at a minimum, must include:

1. A clear description of how the offeror's PWS meets the DCRB's a) business, b) technical, and c) management objectives, as described in Section B. General Requirements and Appendix A. Functional Requirements, including but not limited to:

    a. Initial assessment of the current state

    b. Development, design and customization plan

    c. Installation and implementation plan

    d. Monitoring and controlling the approved installation and implementation

    e. Training and deployment plan

    f. Maintenance and support plan

2. Identification of all assumptions and constraints
3. Identification of all risks associated with this effort including a 1) qualitative assessment of risk based on probability and impact and 2) an approach for mitigating each identified risk
4. Major project milestones
5. Work Breakdown Structure
6. Identification of all major tasks and subtasks identified by
   - Task/Subtask number
   - Task/Subtask description
   - Task/Subtask milestone
   - Task/Subtask objective performance measure
7. Description of how the offeror will establish and maintain a quality assurance system

Past Performance

The Offeror shall identify three (3) contract efforts conducted within the last three years or work that is ongoing. The contracts identified should demonstrate in-depth knowledge and successful implementation of the efforts of similar size and scope and relevance to this solicitation. The identified contracts can be with Federal, District of Columbia, commercial or other customers.

For each contract, the Offeror shall identify the following the 1) Program Manager (PM) and 2) Contracting Officer (CO). The Offeror shall provide the current address, phone number, Fax number, and email address for each customer POC.

For each of the contract efforts identified, the Offeror shall provide the following narrative information:

1. Description of how the scope for this contract/task order relates to this effort in size and scope and relevance.
2. Description of the significant achievements, challenges or obstacles that were encountered during contract performance and the measures taken to overcome them.
3. Description of achievements against the most recent period for which performance measures have been applied to each contract. The performance measures should be specific and show the target performance levels that are set forth under the applicable contracts as well as the level of performance achieved.
4. The names and roles and responsibilities of the individuals performing the work described.

Security Requirements

Offeror shall submit with its technical proposal a risk mitigation plan that will identify the manner through which any risks are to be responded to. Offeror shall describe as part of its risk mitigation plan:

1. Security processes that are sufficient to access, control, and safeguard sensitive and/or classified material;
2. How it plans to support a secure development environment, including facility and personnel clearance management processes;
3. How these processes and procedures will be applied to the requirements of this proposal; and
4. The assumptions on which it based its security proposal.

Section II. Functional Requirements

Offeror shall submit a comprehensive response to the questionnaire in *Appendix A. Functional Requirements* of this solicitation by completing responses to all functional requirements (marked "M" mandatory **and** "D" desired).

VII. Price Proposal

DCRB anticipates awarding a "hybrid" contract – a Firm fixed Price and a Cost Plus Fixed Fee contract for task order services to one offeror. The price used for evaluation purposes will be the combination of the 1) one year base period and 2) each of the three (3) one year option periods.

The offeror shall include option year pricing for each line item/section in its submission. Failure to submit a price proposal with pricing for ***each*** of the three (3) one year option periods in addition to the base period pricing will be deem your proposal submission "nonresponsive".

The following services shall be submitted in the respective pricing structures:

- Firm-fixed price for the following tasks/deliverables:
    - Software
    - Hardware
    - Annual Support
    - Maintenance

- Level of effort (labor hour) for the following activities:
    - Installation, Configuration
    - Training
    - Customization

Offerors are to submit a single "fixed price" for completing each of the above services/deliverables for the base period of performance and each option period. Offerors are to submit labor hour rates and estimated number of hours / resources for performing each of the above level of effort activities for the initial period and each option period. DCRB anticipates issuing a series of Task Orders describing specific tasks/deliverables to be performed and negotiated between the DCRB and the awardee.

NOTE: Offerors are to complete and submit price proposals using the following matrix available at http://dcrb.dc.gov/page/dcrb-procurement-opportunities for the base period ***and*** for each of the three (3) one year option periods.

Task Orders (TO) will be used for project based work. Task Orders will be based on the costs established for labor categories in the pricing matrix. Each Task Order will have specific deliverables and objectives, performance metrics, estimated Level of Effort (LOE), resource allocation, risks, assumptions and constraints. Each TO will be negotiated between DCRB COTR and the offeror to ensure that requests are comprehensive of the services and effort needed to achieve objectives. The initial task order will consist of services required for installation, configuration, customization, training and transition services. Offerors are to complete and submit price proposals using the pricing matrix Excel spreadsheet. Offerors, based on the work described in this solicitation, should determine the appropriate labor hour categories consistent with their proposed methodology and technical approach and DCRB's needs.

Price reasonableness determination will be based on the total combined price for the: 1) Software; 2) Hardware; 3) Installation and customization; 4) Annual Support and Maintenance; 5) Labor Costs; 6) Estimated Hours and Fee structure for Cost Plus Fixed Fee services.

An Offeror's proposal is presumed to represent its best efforts to respond to the solicitation. Any inconsistency between promised performances, the technical/management proposal, identified personnel resources, and price must be explained in the proposal. For example, if the intended use of new and innovative techniques is the basis for an unusually low estimate, the nature of these techniques and their impact on cost or price shall be explained; or, if a corporate policy decision has been made to absorb a portion of the estimated price, that must be stated in the proposal. Any inconsistency, if unexplained, may raise a fundamental question of the Offeror's understanding of the nature and scope of the work required and may adversely impact the Offeror's standing upon evaluation. The burden of proof as to cost/price credibility rests with the Offeror. Unrealistically low prices may indicate an inability to understand requirements and a high-risk approach to contract performance. Accordingly, the DCRB may consider the findings of such an analysis in evaluating an Offeror's ability to perform and the risk of its approach.

DCRB will base its award on its analysis of both the offeror's technical and price proposals with the technical proposal being given more weight.

DCRB reserves the right to not make an award.

Price proposal narratives shall be no more than five (5) pages excluding a cover page. Pages exceeding this limit shall ***not*** be considered or evaluated.

Each price proposal shall address the following in support of their proposal in narrative, related to the fixed price level of effort service areas:

(a) Fee structures for other public agency clients and any reduced fees offered to other municipalities, governmental entities or nonprofit firms.

(b) Information on how you propose to keep track of, and charge for, any expenses. (Incidental office expenses will not be reimbursed for this work. No fees or expenses will be paid for travel time or mileage). Include in your proposal any assumptions on which your hourly fee is based.

(c) A certification that the proposed hourly rates do not exceed the lowest hourly rates charged to any entity of the District of Columbia or any Federal, State, or local government entity for performing similar types of work of similar size scope.

(d) A certification that if, subsequent to award of a contract, hourly rates charged to any District of Columbia, Federal, State, or local government entity for performing similar types of work become lower than the hourly rates specified in the contract, the offeror shall promptly notify DCRB and substitute the lower hourly rates for all future work.

DCRB is subject to the annual appropriations process of the District of Columbia government that culminates in an appropriation act passed by the U.S. Congress and signed the President of the United States. Therefore, funds for the contract term are subject to the availability of funds.

VIII. Evaluation of Proposals

Basis for Award

This procurement will be awarded on a Best Value basis. DCRB will not a make an award to an Offeror if the DCRB makes a determination that an Offeror does not have the technical capability of successfully performing the work contained in this RFP.

Best Value determination will be reached by comparing the differences in the value of the technical factors with the differences in the prices proposed. In making this comparison, the DCRB is more concerned with obtaining superior services than lowest overall price. However, the DCRB shall not make an award at a significantly higher overall price to achieve only slightly superior service.

The proposals will be evaluated by the DCRB Source Selection Evaluation Board (SSEB) who will provide their consensus recommendations to the DCRB Contracting Officer who will then make the final best value determination.

Evaluation Process

The evaluation process will be conducted in three phases:

- Phase 1: An initial technical review of all proposals to determine if the offeror fully complies with all "mandatory requirements" (Section C.) and Security Requirements identified under the Technical Proposal Requirements in this solicitation . All offerors whose proposals do not meet the mandatory and security requirements will be eliminated from further consideration.

- Phase 2: Those proposals who meet the mandatory and security requirements will then be subject to a more detailed technical review based on the Technical Evaluation Criteria contained in this RFP. In addition, the DCRB will also review each offeror's price proposal. Based on a review of both the technical proposal and the price proposal, the DCRB will select a group of proposals who they believe represent the best potential value to the DCRB considering both technical and price. It is this subset of offerors who will be eligible to participate in Phase 3.

    - Technical Proposal – Evaluation Criteria (all of equal weighting)
        1. Product Capabilities and Functions
        2. Proposed Architecture
        3. Requirements Matrix (Excel)
        4. Performance Work Statement (PWS)
        5. Training
        6. Key Personnel
        7. Past Performance

- Phase 3; Select offerors, whose proposals represent best value, will be required to participate in a "scripted demonstration" as defined below.

Scripted Demonstration

Those proposals that have been determined to represent "best value" will be required to demonstrate their end-to-end solution using specific data and use cases from DCRB for executives, project team members, technical staff and selected end users. Each offeror selected will receive a "Demonstration Package" containing evaluation criteria, sample data, business cases, and features to be demonstrated to DCRB.

Selected offerors will hold a brief discussion with selected members of DCRB's staff. Offerors will then meet with a larger group of executives, project team members and selected end users to provide a scripted demonstration. Offerors will use their proposed software products in conjunction with specific data and use cases from DCRB. This portion of the demonstration should take no more than 8 hours (1 day).

The successful offeror will be required to demonstrate the functionality of equipment/systems proposed. The demonstration must be conducted with the products included in the offeror's proposal and must be able to achieve the functionality, speed, and capacity as stated in the offeror's proposal. Failure to use the products proposed in the offeror's response to DCRB's requirements or achieve the

performance proposed represented by the offeror in its proposal response might disqualify the offeror and the demonstration will be concluded.

Logistics

All offerors selected for the scripted demonstration phase will be provided with evaluation criteria, a sample set of data from various DCRB source systems as well as business cases and scenarios within two weeks of the scheduled demonstration date. Offerors should plan to bring their own computer hardware and software to the demonstration. Network connectivity will be provided by DCRB, if required.

Instructions for the scripted demonstration will be provided in writing under separate cover. Specific points of evaluation will be stressed in this document, such as data quality achievement or use case fulfillment as applicable.

Notification of Award

A contract will be awarded to an offeror based on the evaluation of the RFP response, the scripted demonstration and the satisfactory outcome of financial negotiations. After the contract has been awarded, DCRB will notify the unsuccessful offerors.

The DCRB reserves the right to award this effort based on the initial offers received, without discussion of such offers. Accordingly, each initial offer should be submitted on the most favorable terms from a price and services standpoint which the Offeror can submit to the DCRB. However, the DCRB also reserves the right to award no contract at all, depending on the quality of the proposal(s) submitted, the availability of funds, and other factors.

IX. Technical Evaluation Rating

Technical proposals will be evaluated by use of an adjectival rating system methodology.

The evaluation methodologies will allow the SSEB to identify and clearly describe strengths, weaknesses, deficiencies, and risks associated with each proposal. The definitions for each rating are as follows:

Adjective	Description
Unacceptable	Fails to meet minimum requirements; e.g., no demonstrated capacity, major deficiencies which are not correctable; offeror did not address the evaluation criteria.
Marginal	Fails to meet evaluation standard; however any significant deficiencies are correctable. Lacks essential information to support a proposal.
Acceptable	Meets requirements; weaknesses are correctable.
Exceeds	Exceeds most, if not all requirements; no deficiencies.

In conformance with the requirements of this RFP, DCRB will evaluate option years as well as the base year. Evaluation of options shall not obligate the DCRB to exercise them.

X. Security Rating System

The Security Requirements will be evaluated using the pass/fail adjectival rating system methodology. An offeror's proposal that receives a "fail" rating will not be considered for contract award.

Security Rating System	
Pass	The security aspects of the Offeror's approach include no deficiencies or weaknesses. The processes described appear sufficient to safeguard DCRB sensitive materials and information and support a secure development environment, including facility and personnel clearance management processes.
Fail	The security aspects of the Offeror's approach may include either deficiencies and/or weaknesses. The processes described do not appear sufficient to safeguard DCRB sensitive materials and information, nor to support a secure development environment, including facility and personnel clearance management processes.

ARTICLE II. GENERAL TERMS AND CONDITIONS

A. Reservations

DCRB reserves the right to reject any and all offers.

DCRB is not liable for any expense incurred in the preparation, delivery or presentation of Proposals in response to this RFP.

If, prior to execution of any contract, subsequent information or circumstances indicate that such contract is not in the best interest of DCRB, the right is reserved to rescind the offer and either award the contract to another Offeror or reject all responses.

B. Confidentiality

Confidential Information is any and all information which is proprietary, confidential, secret or otherwise, not generally known to the public, including personal and identifying information concerning participants in the Retirement Funds. Confidential Information shall not include information which, as established by credible evidence: (a) is or becomes public knowledge without any action by, or involvement of, the party receiving the Confidential Information hereunder: (b) is independently developed by the receiving party without the use of the other party's Confidential Information: (c) is already known to the receiving party at the time of disclosure under this Agreement without restriction of confidentiality: (d) is disclosed to the receiving party by a third party who is entitled to disclose it without restriction of confidentiality: or (e) the disclosing party subsequently approves for disclosure without restrictions.

Each party, on behalf of itself and its employees and agents, agrees that it and its employees and agents: (a) shall not use any Confidential Information of the other party for any purpose other than to perform its obligations under this Agreement; and (b) shall keep and maintain all Confidential Information as strictly confidential and shall not directly or indirectly transfer or otherwise disclose any such Confidential Information to any third party other than those of its employees with a need to have access thereto. Each party shall cause those of its employees and agents receiving Confidential Information of the other party to observe the terms of this Paragraph. Each party shall be responsible for any breach of this Paragraph by any of its employees or agents.

A party shall not be liable for the disclosure of any Confidential Information if the disclosure is: (a) required by law, regulation or legal process and uses reasonable efforts to obtain assurances that, if possible, confidential treatment will be accorded such Confidential Information or (b) inadvertent despite the exercise of the same degree of care as that party takes to preserve and safeguard its own Confidential Information, provided that upon discovery thereof that party takes all reasonable steps to retrieve the inadvertently disclosed Confidential Information and that such inadvertent disclosure will not relieve that party from its continued adherence to the terms and conditions of this Paragraph.

The successful Offeror will be required to execute and submit Confidentiality Agreements before service contract award. All person(s) assigned to the project in any capacity will be required to sign

statements of confidentiality in order to participate in the project. The Offeror must certify that criminal background checks have been conducted on all person(s) participating in the project.

C. Indemnification

Offeror hereby agrees to hold harmless the Board, its members, officers, employees, agents and representatives and the District of Columbia Government, and to indemnify and exonerate same against and in respect of any and all claims, demands, damages, actions, costs, charges, losses, liabilities, and deficiencies, including legal fees and expenses, resulting from, arising out of, or in any way related to (a) any untrue warranty or representation or material omission of Offeror in this Contract; and/or (b) any liens, claims, encumbrances, or infringement of any patent, trademark, copyrights, or other proprietary or intellectual property right; and/or (c) Offeror's willful misfeasance, bad faith, negligence or reckless disregard of its obligations in providing services under the terms of the Contract.

D. Sole Property

All deliverables, reports, and documents produced in the performance of this Agreement shall be the sole property of DCRB. The Offeror shall make no distribution of work specifically produced for DCRB under this Agreement to others without the express written consent of the agency. The

Offeror agrees not to assert any rights at common law or in equity or establish any claim to statutory copyright in such reports.

E. Contractual Requirements

Offerors are each responsible for complying with all statutory provisions applicable to doing business in the District of Columbia and with DCRB; however, such compliance does not limit DCRB to any rights or remedies available to DCRB under other general, state or local laws.

The terms, conditions, and specifications of the RFP, the successful Offeror's response, the completed and executed contract, and all RFP amendments (if any) will comprise the entire agreement between DCRB and the successful Offeror.

F. Complete Contract

This Contract including all amendments, the Offeror's technical and price proposals (including proposal revisions), represents the entire and integrated Contract between DCRB and the Offeror and supersedes all prior negotiations, proposals, communications, understandings, representations, or Contracts, either written or oral, express or implied. All amendments or modifications of this Contract shall be in writing and executed by DCRB and the Offeror.

G. Prohibition Against Contingent Fees

Offeror warrants that it has not employed or retained any company or person, other than a bona fide employee working solely for it, to solicit or secure this Contract, and that it has not paid or agreed to pay any company or person, other than a bona fide employee working solely for it, any fee, commission, percentage, gift, or any other compensation contingent upon or resulting from the

award or making of this Contract; except where: (a) Offeror has disclosed, in writing to the Board, that it has engaged such a company or person other than a bona fide employee to secure this engagement, and (b) the cost of such engagement is not charged to DCRB under the terms of compensation under this or any other current or subsequent Contract. For breach or violation of this warranty, DCRB shall, at its discretion, void this contract without liability, entitling DCRB to recover all monies paid hereunder and Offeror shall not make a claim for, or be entitled to recover, any sum or sums due under this Contract. This remedy, if affected, shall not constitute the sole remedy of the Board for the falsity or breach, nor shall it constitute a waiver of the Board's right(s) to claim damages or refuse payment or take any other action provided for by law pursuant to this Contract.

H. Primary Consultant/Contractor

In performing the services under this Contract, Offeror's representative assigned to DCRB as the Primary and/or Co-Primary Consultant/Contractor, shall report to on an ongoing basis, and meet with DCRB for the purposes of providing the services under this Contract. Designation of a new Primary or Co-Primary Consultant/Contractor shall be subject to DCRB's approval, which approval shall not be unreasonably withheld.

I. Assignment

Neither party will, directly or indirectly, assign or transfer any claim arising out of this Contract. Offeror recognizes that this Contract is for specific performance of personal consulting services to be performed solely by Offeror.

J. Restriction on disclosure and use of data

All proposals become the property of DCRB and may be subject to disclosure under the Freedom of Information Act. Pages of a proposal containing confidential or proprietary information shall contain a header and footer with an appropriate restrictive legend.

If the Offeror includes in the proposal data that it does not want disclosed to the public for any purpose, or used by the DCRB except for evaluation purposes, the Offeror shall:

A. Mark the title page with the following legend:

"This proposal includes data that shall not be disclosed outside the DCRB and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this Offeror as a result of, or in connection with, the submission of this data, the DCRB shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the DCRB right to use information contained in this data if it is obtained from another source without restriction."

B. Mark each sheet of data it wishes to restrict with the following legend: "Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal"

K. Notices

Any notice or consent required to be given in accordance with this Contract shall be in writing and shall be either (i) delivered by hand to the other party; (ii) mailed, with first class postage prepaid, to the address of the other party, by certified mail, return receipt requested, or (iii) sent electronically with a receipt detailing the transmitted message. Notices and requests for consent shall be addressed to the Chief Contracting Officer. The Executive Director of the Board is the Chief Contracting Officer for this Contract.

L. Contract Term

The term of the contract shall be for a base period of one year from date of award and three (3) on year option periods. DCRB's total requirements may change during the option years. Quantities to be awarded will be determined at the time each option is exercised.

DCRB's Chief Contracting Officer may extend the term of the contract for a period of three (3) one year option periods, or successive fractions thereof, by written notice to the Contractor before the expiration of the contract; provided that DCRB will give the Contractor preliminary written notice of its intent to extend at least thirty (30) days before the contract expires. The preliminary notice does not commit DCRB to an extension. The exercise of any option is subject to the availability of funds at the time of the exercise of the option. The Contractor may waive the thirty (30) day preliminary notice requirement by providing a written waiver to the Chief Contracting Officer prior to expiration of the contract.

If DCRB exercises contract option(s), the extended contract shall be considered to include this option provision. The price for the option period(s) shall be as specified in the Price Proposal and is subject to negotiations. The total duration of the contract, including the exercise of any options under this clause, shall not exceed four (4) years.

M. Termination for Cause/Convenience

The contract may be terminated by DCRB in whole or in part for cause at any time.

If DCRB proposes terminating the contract for cause, DCRB shall first give ten (10) days prior written notice to the Offeror stating the reason for termination, and providing the Offeror an opportunity to cure the issues leading to termination. Offeror must submit a corrective action plan which outlines the methodology and timeline of each corrective action. The corrective action plan shall be provided to the COTR or his designee within ten (10) calendar days of receipt of the notice to cure. Failure to submit a corrective action plan in response to the notice to cure shall result in DCRB terminating the contract for cause.

Offeror shall not be entitled to receive payment for labor or expenses incurred prior to termination unless accepted by the Board.

The contract may be terminated in whole or in part by DCRB for convenience at any time by giving the Offeror written notice. In such event:

A. Offeror shall immediately cease performing the terminated work unless directed otherwise.

B. Offeror shall be reimbursed for agreed upon fees and expenses incurred in preparing to perform the terminated work.

C. Offeror shall not be compensated for anticipated future profit for the terminated work.

N. Rights in Data

N.1 "Data," as used herein, means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

N.2 The term "Technical Data", as used herein, means recorded information, regardless of form or characteristic, of a scientific or technical nature. It may, for example, document research, experimental, developmental or engineering work, or be usable or used to define a design or process or to procure, produce, support, maintain, or operate material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents or computer printouts. Examples of technical data include research and engineering data, engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog item identifications, and related information, and computer software documentation. Technical data does not include computer software or financial, administrative, cost and pricing, and management data or other information incidental to contract administration.

N.3 The term "Computer Software", as used herein means computer programs and computer databases. "Computer Programs", as used herein means a series of instructions or statements in a form acceptable to a computer, designed to cause the computer to execute an operation or operations. "Computer Programs" include operating systems, assemblers, compilers, interpreters, data management systems, utility programs, sort merge programs, and automated data processing equipment maintenance diagnostic programs, as well as applications programs such as payroll, inventory control and engineering analysis programs. Computer programs may be either machine-dependent or machine-independent, and may be general purpose in nature or designed to satisfy the requirements of a particular user.

N.4 The term "computer databases", as used herein, means a collection of data in a form capable of being processed and operated on by a computer.

N.5 All data first produced in the performance of this Contract shall be the sole property of the DCRB. The Contractor hereby acknowledges that all data, including, without limitation, computer program codes, produced by Contractor for the DCRB under this Contract, are works made for hire and are the sole property of the DCRB; but, to the extent any such data may not, by operation of law,

be works made for hire, Contractor hereby transfers and assigns to the DCRB the ownership of copyright in such works, whether published or unpublished. The Contractor agrees to give the DCRB all assistance reasonably necessary to perfect such rights including, but not limited to, the works and supporting documentation and the execution of any instrument required to register copyrights. The Contractor agrees not to assert any rights in common law or in equity in such data. The Contractor shall not publish or reproduce such data in whole or in part or in any manner or form, or authorize others to do so, without written consent of the DCRB until such time as the DCRB may have released such data to the public.

N.6 The DCRB will have restricted rights in data, including computer software and all accompanying documentation, manuals and instructional materials, listed or described in a license or agreement made a part of this contract, which the parties have agreed will be furnished with restricted rights, provided however, notwithstanding any contrary provision in any such license or agreement, such restricted rights shall include, as a minimum the right to:

N.6.1 Use the computer software and all accompanying documentation and manuals or instructional materials with the computer for which or with which it was acquired, including use at any DCRB installation to which the computer may be transferred by the DCRB;

N.6.2 Use the computer software and all accompanying documentation and manuals or instructional materials with a backup computer if the computer for which or with which it was acquired is inoperative;

N.6.3 Copy computer programs for safekeeping (archives) or backup purposes; and modify the computer software and all accompanying documentation and manuals or instructional materials, or combine it with other software, subject to the provision that the modified portions shall remain subject to these restrictions.

N.7 The restricted rights set forth in section N.6 are of no effect unless

(i) the data is marked by the Contractor with the following legend:

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure is subject to restrictions stated in Contract No._____with (Contractor's Name); and

(ii) If the data is computer software, the related computer software documentation includes a prominent statement of the restrictions applicable to the computer software. The Contractor may not place any legend on the computer software indicating restrictions on the DCRB's rights in such software unless the restrictions are set forth in a license or agreement made a part of the contract prior to the delivery date of the software. Failure of the

Contractor to apply a restricted rights legend to such computer software shall relieve the DCRB of liability with respect to such unmarked software.

N.8 In addition to the rights granted in Section I.5.6 above, the Contractor hereby grants to the DCRB a nonexclusive, paid-up license throughout the world, of the same scope as restricted rights set forth in Section I.5.6 above, under any copyright owned by the Contractor, in any work of authorship prepared for or acquired by the DCRB under this contract. Unless written approval of the CO is obtained, the Contractor shall not include in technical data or computer software prepared for or acquired by the DCRB under this contract any works of authorship in which copyright is not owned by the Contractor without acquiring for the DCRB any rights necessary to perfect a copyright license of the scope specified in the first sentence of this paragraph.

N.9 Whenever any data, including computer software, are to be obtained from a subcontractor under this contract, the Contractor shall use this clause, I.5, Rights in Data, in the subcontract, without alteration, and no other clause shall be used to enlarge or diminish the DCRB's or the Contractor's rights in that subcontractor data or computer software which is required for the DCRB.

N.10 For all computer software furnished to the DCRB with the rights specified in Section I.5.5, the Contractor shall furnish to the DCRB, a copy of the source code with such rights of the scope specified in Section I.5.5. For all computer software furnished to the DCRB with the restricted rights specified in Section I.5.6, the DCRB, if the Contractor, either directly or through a successor or affiliate shall cease to provide the maintenance or warranty services provided the DCRB under this contract or any paid-up maintenance agreement, or if Contractor should be declared bankrupt or insolvent by a court of competent jurisdiction, shall have the right to obtain, for its own and sole use only, a single copy of the then current version of the source code supplied under this contract, and a single copy of the documentation associated therewith, upon payment to the person in control of the source code the reasonable cost of making each copy.

N.11 The Contractor shall indemnify and save and hold harmless the DCRB, its officers, agents and employees acting within the scope of their official duties against any liability, including costs and expenses, (i) for violation of proprietary rights, copyrights, or rights of privacy, arising out of the publication, translation, reproduction, delivery, performance, use or disposition of any data furnished under this contract, or (ii) based upon any data furnished under this contract, or based upon libelous or other unlawful matter contained in such data.

N.12 Nothing contained in this clause shall imply a license to the DCRB under any patent, or be construed as affecting the scope of any license or other right otherwise granted to the DCRB under any patent.

N.13 Paragraphs N.6, N.7, N.8, N.11 and N.12 above are not applicable to material furnished to the Contractor by the DCRB and incorporated in the work furnished under contract, provided that such incorporated material is identified by the Contractor at the time of delivery of such work.

O. Successor Contract

In the event DCRB awards a successor Contract to another entity covering the same matters as those assigned to Offeror under this Contract, then Offeror shall cooperate with DCRB to effect an orderly transition to the successor entity.

P. Cancellations

In the event provisions of this RFP are violated by Offeror(s), DCRB may give written notice to the Offeror(s) stating the deficiencies. Unless deficiencies are corrected within five (5) working days, DCRB reserves the right to issue an immediate termination notice in writing to the Offeror(s).

DCRB reserves the right to require personnel changes at any time during the term of the contract. Such a request shall be issued in writing by DCRB and the Offeror shall have five (5) business days to provide a substitute acceptable to DCRB. Failure to do so shall result in DCRB issuing and immediate termination notice in writing to the Offeror.

Q. Security and Background Checks

Due to the sensitive nature of the information that the Offeror's staff will be supporting, a background check shall be performed on all personnel and employees who are assigned to work on this contract. A background check will be performed initially and every two years thereafter consistent with DCRB's policies. The Offeror shall not assign anyone to work on this contract and shall immediately remove from work on this contract anyone who has been convicted within the past seven years of fraud or any felony or who is currently under arrest warrant. Any exceptions to this provision must be approved in writing by the Contracting Officer.

The background check must be returned in a favorable status prior to the Offeror commencing work on this contract. The background check shall be performed by the District of Columbia's Metropolitan Police Department located at 300 Indiana Avenue, N.W., Washington, DC 2001. The cost of the background check is $35.00 per individual and must be paid directly by Offeror.

In the event that the Offeror is located outside the DC Metropolitan area (Washington, DC, Maryland, Virginia), they must propose for DCRB's review and acceptance alternate means for conducting background check(s).

In addition to the aforementioned background check requirement(s), each Offeror shall provide a risk mitigation plan, including but not limited to, the processes employed by the Offeror to provide data and personnel security in compliance with Privacy Act of 1974, 5 U.S.C. § 552a, and the Department of the Treasury's system of records notice TREASURY/DO .214 Fed Reg. 46284 (2005).The Offeror shall provide as part of the risk mitigation plan how it will meet the requirements of DCRB's Personally Identifiable Information (PII) Policy included as Appendix C by providing the following:

- A list of the anticipated threats and hazards that the contractor must guard against;
- A description of the safeguards that the contractor must specifically provide; and

- Requirements for a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

Offeror and all personnel working on this contract must sign a confidentiality statement provided by DCRB as prescribed above in Section B. Confidentiality.

R. Dispute Resolution

A. The parties waive the right to trial by jury in any judicial action, proceeding or counterclaim arising from this Contract that is not resolved by mutual Contract.

B. Any legal proceedings involving this contract shall be filed with a District of Columbia court with subject matter jurisdiction, and District of Columbia law shall apply, excluding its choice of law provisions.

C. Pending a final settlement of or a final decision from a court on an action or appeal of, a dispute or a claim asserted by the Offeror against DCRB, the Offeror shall proceed diligently with performance of the Contract in accordance with its terms and conditions.

S. Governing Laws

This Contract shall be governed by and construed in accordance with the laws of the United States and the District of Columbia.

T. Freedom of Information Act

Offeror understands and acknowledges that DCRB is subject to the District of Columbia Freedom of Information Act ("Act") and consents to the disclosure of its proposal, this Contract, and any information, recommendations, or advice received by DCRB from Offeror under this Contract, or such information, recommendations, or advice is subject to disclosure under the Act. DCRB shall use reasonable efforts to give notice of any demand for disclosure to Offeror as soon as reasonably practicable after demand for disclosure is made upon DCRB.

U. Insurance Requirements

The Offeror selected for contract award shall procure and maintain, during the entire period of performance under this contract, the types of insurance specified below. The Offeror shall have its insurance broker or insurance company submit a Certificate of Insurance to the DCRB giving evidence of the required coverage prior to commencing performance under this contract. In no event shall any work be performed until the required Certificates of Insurance signed by an authorized representative of the insurer(s) have been provided to, and accepted by, the DCRB. All insurance shall be written with financially responsible companies authorized to do business in the District of Columbia or in the jurisdiction where the work is to be performed and have an A.M. Best Company rating of A-VIII or higher. The Offeror shall ensure that all policies provide that the DCRB shall be given thirty (30) days prior written notice in the event the stated limit in the declarations page of the policy is reduced via endorsement or the policy is canceled prior to the expiration date shown on the

certificate. The Offeror shall provide the DCRB with ten (10) days prior written notice in the event of non-payment of premium.

a. Commercial General Liability Insurance. The Offeror shall provide evidence satisfactory to the DCRB with respect to the services performed that it carries $1,000,000 per occurrence limits; $2,000,000 aggregate; Bodily Injury and Property Damage including, but not limited to: premises-operations; broad form property damage; Products and Completed Operations; Personal and Advertising Injury; contractual liability and independent Offerors. The policy coverage shall include the DCRB as an additional insured, shall be primary and non-contributory with any other insurance maintained by the DCRB, and shall contain a waiver of subrogation. The Offeror shall maintain Completed Operations coverage for five (5) years following final acceptance of the work performed under this contract.

b. Workers' Compensation Insurance. The Offeror shall provide Workers' Compensation insurance in accordance with the statutory mandates of the District of Columbia or the jurisdiction in which the contract is performed.

   Employer's Liability Insurance. The Offeror shall provide employer's liability insurance as follows: $500,000 per accident for injury; $500,000 per employee for disease; and $500,000 for policy disease limit.

c. Errors and Omissions Insurance. The Offeror shall provide evidence satisfactory to the DCRB with respect to the services performed that it carries $1,000,000 per occurrence limits; $2,000,000 aggregate; Data Breach/Loss and IT Security coverage including but not limited to: software installations, network, mistakes and oversights that creates financial harm to DCRB. The policy coverage shall include the DCRB as an additional insured, shall be primary and non-contributory with any other insurance maintained by DCRB, and shall contain a waiver of subrogation. The Offeror shall maintain E&O coverage at this level for five (5) years following final acceptance of the work performed under this contract.

The Offeror shall carry all required insurance until all contract work is accepted by the DCRB, and shall carry the required General Liability; any required Professional Liability insurance for five (5) years following final acceptance of the work performed under an awarded contract.

These are the required minimum insurance requirements established by the District of Columbia.

HOWEVER, THE REQUIRED MINIMUM INSURANCE REQUIREMENTS PROVIDED ABOVE WILL NOT IN ANY WAY LIMIT THE OFFEROR'S LIABILITY.

The Offeror are solely responsible for any loss or damage to their personal property, including but not limited to tools and equipment, rented machinery, or owned and leased equipment. A waiver of subrogation shall apply in favor of the DCRB.

The DCRB shall not make any separate measure or payment for the cost of insurance and bonds. The Offeror shall include all of the costs of insurance and bonds in the contract price.

The Offeror shall immediately provide the DCRB with written notice in the event that its insurance coverage has or will be substantially changed, canceled or not renewed, and provide an updated certificate of insurance to the CO.

The Offeror shall submit certificates of insurance giving evidence of the required coverage as specified in this section prior to commencing work. Evidence of insurance shall be submitted to:

Yolanda Smith
Contract Specialist
District of Columbia Retirement Board
900 7th Street, NW, 2nd Floor
Washington, DC 20001; (202) 343-3200

The Offeror agrees that the DCRB may disclose the name and contact information of its insurers to any third party which presents a claim against the District for any damages or claims resulting from or arising out of work performed by the Offeror, its agents, employees, servants or sub Offerors in the performance of this contract.

V. Order of Precedence

A conflict in language shall be resolved by giving precedence to the document in the highest order of priority that contains language addressing the issue in question. The following documents are incorporated into the contract by reference and made a part of the contract in the following order of precedence:

(1) An applicable Court Order, if any
(2) Contract document
(3) Contract attachments
(4) RFP, including amendments
(5) BAFOs (in order of most recent to earliest)
(6) Offeror's Proposal

APPENDIX A

Functional Requirements

The following matrix outlines specific requirements by product for the solution. Requirements are broken out into Business, Functional and Technical requirements. Offerors will complete the following table outlining how their solution meets each requirement according to the legend below. If additional information is necessary for the Offeror to communicate how requirements are met or how the solution delivers the requirement, a comments field has been provided.

Mandatory/Desirable	Pass / Fail Factor for Evaluation	
Offeror Response	Check the appropriate column using the following key.	
	CC	**Client Configurable**: Requirement is available and can be configured by the client without offeror support or involvement.
	VC	**Integrator Configurable**: Requirement is available and can be configured by the offeror.
	M	**Modifiable**: Requirement is available and can be configured by the Integrator, but will require some level of modification.
	EE	**Expandable/Extensible**: Software/solution can be easily expanded or extended with a third-party product to meet new requirements
	C	**Custom:** Requirement is not available and would have to be customized for DCRB.
	NS	**Not Supported:** Requirement is not supported and will not be modified or expanded to meet the requirement during this project.
In Productive Use?	Enter Yes or No. Each requirement must be in production and currently in use by a client.	
Comments	Offeror may include a brief statement as to whether it meets or exceeds each requirement; if the response is "**M**" or "**C**", indicate whether it will meet the required timeline. Include the cost of customization in the Financial Proposal/Pricing Schedule.	

Requirements indicated as Mandatory will be required for the proposal to be accepted. If a Mandatory requirement cannot be met, the proposal will fail the evaluation.

Desirable requirements will be evaluated individually on implementation type (VC, CC, etc.) with a weighted importance of “In Productive Use”.

NOTE: When giving responses, the guidelines below should be followed. A comments column is provided in the spreadsheet for clarification, when necessary.

Offerors are cautioned not to indicate functionality as "included in standard offering" when, in fact, that particular feature is in development. When that is the case, offerors should note that fact in the comments column of the “Data Management RFP Questionnaire for District of Columbia Retirement Board" and indicate the expected date that such a feature will be made available.

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
Business Requirements										
1	Integration with Standard Database Solutions: The solution shall be able to integrate with and leverage current systems such as SQL Server, Oracle, etc. in place at DCRB.	M								
2	Integration with Standard Application Systems: The solution shall be able to integrate with PeopleSoft, SharePoint, FileNet, and other data warehousing solutions.	M								
3	Multiple Upload Capabilities: The solution shall provide mechanisms to upload existing data from multiple solutions regardless of the technology platform on which they operate.	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
4	Connectivity: Standard Communications Platform: The solution should possess industry standard communication protocols that are agnostic of the output solutions. Data should be input and output for multiple systems regardless of technology or platform (i.e., web services).	M								
5	Support: Product end support should be best in class and available 24/7 as part of the solution.	M								
6	Performance Standards: The solution shall meet the Service Level Agreement (SLA) and other performance standards set by DCRB.	M								
Functional Requirements										

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
7	Connectivity: Relational Databases: The solution shall connect to data stored in relational database management systems. Specifically, the solution must connect to Microsoft SQL Server (2014, 2012, and 2008 R2) and Oracle 11g.	M								
8	Connectivity: Flat File Formats: The solution shall connect to a variety of delimited flat files such as .csv, .txt, or .xls, as well as XML and JSON formats.	M								
9	Connectivity: Emergent Data Types/ Semi-Structured Data: The solution shall connect to data stored in non-traditional source types, such as web sites, Microsoft Office productivity tools, and content repositories such as FileNet 5.1, SharePoint 2013, Tamale RMS, Dynamics GP, and other tools used by the agency.	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
10	Connectivity: Multiple Protocols & Data Structures: The solution shall connect to data stored in SOAP, REST, WSDL, and UDDI structures and any other industry standard formats.	M								
11	Communication: Solution must have a platform that establishes an interoperability layer that supports interactions among components via a variety of protocols (HTTP/HTTPS, XML, SOAP, Internet Inter-ORB Protocol [IIOP], .NET remoting, message-oriented middleware [MOM] protocols, file transfer protocols [FTP/SFTP], JMS/MQ, RDBMS, REST, WSDL, UDDI, etc.) and interaction styles (request/reply, conversational, publish and subscribe, asynchronous messaging, etc.).	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
12	Mediation: The solution must have features that enable in-flight message manipulation, such as transformation (typically XML-based), intelligent routing, naming and addressing, and dynamic service virtualization.	M								
13	Orchestration: The solution shall support designing the service interfaces, the rules (transformation, routing), the orchestration (virtualization flows), and the adapter configurations required to implement services.	M								
14	Exchange Integration: The solution shall access and extract data from email messages and their attachments from a Microsoft Exchange Server environment. Data stored in attachment may include semi-structured data such as flat file, XML, and JSON formats.	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
15	Management, Administration, Monitoring, and Control: The proposed solution must have the functionality to assist operations personnel in keeping the resultant system (applications, services, and infrastructure) running at peak efficiency at all times.	M								
16	Management, Administration, Monitoring, and Control: The proposed solution must support access and control for information exchange and provide support of business applications to enforce access controls.	M								
17	Management, Administration, Monitoring and Control: The proposed solution must support error handling, provide capability to send alerts to notify team members of failed processes, and possess ability to send alerts based on non-receipt of files or messages.	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
18	Security Solutions: The solution shall meet industry, NIST, and FIPS security standards as required.	M								
19	Connectivity: Legacy and Non-Relational Databases: The system shall provide interface connections for legacy and non-relational database systems.	D								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
20	Adapters: The proposed solution should have the technology that combines design tools and runtime software to implement programs such as transforming among protocols, connecting to any data source, technology (messaging, databases, etc.), applications, or trading partner through a unified connectivity framework and linking pre-SOA ease and power-packaged composite applications and packaged APIs to the SOA backplane using industry standards, packaged application adapters, legacy adapters, technology adapters, and adapter development integrating processes.	D								
21	Advanced Semantic Transformation: The solution must have the ability to perform syntactic and semantic hub-based transformation of messages.	D								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
22	File Formats: The proposed solution must provide the ability to handle multiple document formats—scanned images, PDF, XML, CSV. etc.	D								
23	Advanced Semantic Transformation: The proposed solution shall have infrastructure tooling that enables users to represent semantic models, identify model-to-model relationships, and execute the necessary translations to reconcile data with differing semantic models.	D								
24	Management, Administration, Monitoring, and Control: The proposed solution must provide for performance monitoring tools that can be used with the product (built-in or third party).	D								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
25	Management, Administration, Monitoring, and Control: The proposed solution must be widely compatible with existing applications and operating environments.	D								
26	Management, Administration, Monitoring, and Control: The proposed solution must provide the ability to monitor external interfaces as well as interfaces built on the ESB for responsiveness, queuing issues, etc. The ESB should be able to generate alerts if deviations from specified parameters are detected.	D								
27	Management, Administration, Monitoring, and Control: The proposed solution shall provide a simulation engine or tool that identifies potential process bottlenecks before a process is deployed.	D								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
Technical Requirements										
23	Connectivity: Bi-Directional Interface Modalities: The solution shall support common bi-directional interface modalities including generic web services or APIs.	M								
24	Data Extracts: The solution shall provide data extracts in multiple formats such as Excel, XML, flat file, CSV, CD, or DVD to support audit and reporting requirements.	M								
25	Support of Industry Standard Data Formats: The solution shall support the current version of XML, CSV, REST, and other industry standard data formats.	M								
26	Web Services: The solution must support a distributed computer environment (Web Services, API).	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
27	Security: The proposed solution must clearly articulate how the solution will provide maximum security for the users and transactions involved through the following: authentication, authorization, encryption/encryption, digital signatures, credential mapping	M								
28	Architecture & Technology & Scalability: The proposed solution must have the potential to be scaled in the future so that additional resources could be acquired and attached to the system easily allowing other systems to integrate.	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
29	Architecture, Technology, and Scalability: The proposed architecture must be scalable and must provide a minimum of 99.999% ESB server availability. Options and recommendations for measuring and reporting on availability as defined are encouraged.	M								
30	Queuing: The system should enable for message/data queuing in the event that a receiving system is down or network connectivity errors exist.	M								
31	Communication: The solution must have a messaging platform that enables communication among applications via the reliable delivery of messages.	M								
32	Architecture, Technology, Scalability: The proposed architecture must include separate development, test, and production environments.	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
33	Architecture: The proposed architecture must achieve DCRB integration via web-based technologies that, at a minimum, include the following architectural components: connectivity, data access and control, security, confidentiality, management and control, and networking.	M								
34	Security: Encryption Standard: The proposed solution must ensure that all DCRB network data crossing over a public network segment or Internet connections includes at least 128 bit encryption using FIPS 140-2 compliant modules. The solution must be capable of using cryptographic modules that are compliant with Federal Information Processing System (FIPS).	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
35	Security: Encryption: The proposed solution must incorporate secure data exchange mechanisms and technologies such as cryptography, key management, access control, authentication, and data integrity where appropriate.	M								
36	Security: Authentication: The proposed solution must provide the ability to authenticate users and messages with AD/LDAP or ID provider.	M								
37	Security: The offeror shall propose implementation of web services security standard and must clearly articulate the standard, which components of the standard will be implemented, and how each component fulfills a technological or business requirement identified by DCRB.	M								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
38	Security: The proposed solution shall provide the tools and technologies required to implement the necessary authentication and authorization to control.	M								
39	Architecture: The proposed architecture must flexibly adapt to, integrate, and use ever-evolving policies, best practices, and operating procedures from the agency's integration participants (EDQ/MDM).	D								
40	Adapters: The solution must provide the ability to create adapter services with coding tools.	D								

ESB Requirements										
ID	**Requirement**	**Mandatory/ Desirable**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
41	Connectivity: Web Services: The proposed solution must include request/reply, publish/subscribe, and synchronous/asynchronous functionality to facilitate the information sharing between DCRB systems and applications including other entities and the ESB.	D								
42	Security: The security included in the proposed solution must be scalable and capable of being configured to accommodate different levels of security on a per user, application, or endpoint basis.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
Business Requirements										
43	Standardize and De-Duplicate Data: The solution shall be able to standardize and de-duplicate data across multiple solutions regardless of the data.	M								
44	Support: Product end support should be best in class and available 24/7 as part of the solution.	M								
45	Performance Standards: The solution shall meet the Service Level Agreement (SLA) and other performance standards set by DCRB.	M								
Functional Requirements										
46	SSN: The solution shall be configurable for a quality check on Social Security Numbers (SSN) to ensure both the format and veracity of the data (e.g., 000-00-000).	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
47	SSN: The solution shall cross reference and validate unique SSN against Berwyn datastore (or other validation source) and master data record.	M								
47	Profiling: Profiling of Data External to Sources: The solution shall have the ability to profile data external to existing databases by importing the data into the tool.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
48	Profiling: Column-Based Analyses: The solution shall provide the ability to analyze pre-built patterns for individual attributes, columns, and fields. The analysis should include 1) general functions such as min, max, frequency distributions of value, and patterns; 2) specific functions for common attributes like SSN, e-mail address, phone number, part numbers, dates, city, postal code, and more; and 3) indicators on the selected column, such as number of nulls, row counts, duplicate counts, blank counts, summary statistics, pattern matching indicators, etc.	M								
49	Profiling: Data Quality Thresholds: The solution shall allow users to define expected thresholds for data, including minimum/maximum values, dates, or lengths. Trend analysis should be able to identify outliers within the data.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
50	Manual Override: The solution shall provide manual override for authorized users to resolve improper matches (and mismatches) and to preserve the override for that data record for future use.	M								
51	Bulk Processing: The solution shall provide mechanisms for bulk processing of issues similar to the manual override requirement.	M								
52	Profiling: Dependency Analyses: The solution shall provide the ability to perform a range of pre-built analyses to identify relationships, patterns, integrity gaps, and duplication between and across multiple attributes, fields, tables, databases, and files.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
53	Profiling: Redundancy Analysis: The solution shall provide the ability to compare the data of two sets of columns. The analysis will be used to verify foreign key/primary key relationships or to compare the content of two tables. Preferably, the system will enable redundancy analysis across multiple database systems.	M								
54	Processing: Real-Time or Batch: The solution shall facilitate the extraction and validation of data through a batch system or on a real-time basis.	M								
55	Parsing: The system shall have pre-built functionality for the decomposition of textual data.	M								
56	Parsing: Delimiter Parsing: The solution shall provide the ability to split text fields based on delimiters, such as tabs, spaces, and commas.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
57	Parsing: Name Parsing: The solution shall parse names, determine gender, and detect vulgar words. The solution shall be able to parse full, dual, inverse, and mixed full name.	M								
58	Parsing: Customized Parsing: The system shall allow for facilities that configure user-defined parsing rules.	M								
59	Matching: Linking "Households": The system shall have the ability to create logical groups of records by relating those with user-determined properties.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
60	Matching: Removing Duplicates/De-Duplication: The system shall provide automatic removal of duplicate records based on rules for determining survivorship. The identification of semantic duplicates in a rules-based process that enables an end user to determine what constitutes a match and perform de-duplication will also be provided.	M								
61	Matching: Merge Records: The system shall have facilities for implementing and customizing rules by which duplicate or related records can be merged into a single "survivor." The final record can take the best parts of all related records to form an optimal best-of-breed record.	M								
62	Matching: Fuzzy De-Duplication: The system must be able to create a database with only unique records, leveraging fuzzy matching algorithms.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
63	Resolving Conflict: The system should enable users to fill in missing data and resolve other data quality issues.	M								
64	Metadata: The system should have the ability to capture, reconcile, and interoperate metadata relating to the data quality process.	M								
65	Metadata: User Interface: The system must provide business analyst/end-user interfaces that view and work with metadata.	M								
66	Data Cleansing: Interval Matching: The system will look for number of outliers in the number of times items appear in an attribute.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
67	Threshold: The solution will use thresholds for matching and will identify records that are matches, records that are unique, and records that need manual inspection to determine match status.	M								
68	Data Duplication Systems: The system must recognize duplicate records and provide a facility for identifying, merging, or resolving duplicates before they are accepted into the system.	M								
69	Address Validation/Geocoding: The system must cleanse common address attributes like name, address, state, city, and postal code using included patterns and reference data. The system should leverage any trusted source to standardize and enrich data.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
70	Libraries: The system must provide validation libraries certified by relevant authorities such as the U.S. Post Office.	M								
71	Library Updates: The system will provide a mechanism by which updates to all validation libraries are delivered and applied.	M								
72	Address Parsing: The system will parse unstructured and structured address data, will standardize address elements, will format postal addresses, and will facilitate the process of address validation.	M								
73	Event Logging: The system must have complete event tracking for all events including user name, date, and time.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
74	Console: The system should have a multi-user interface capable of managing scheduled jobs, activating unscheduled tasks, monitoring and reporting on current tasks, and leveraging performance reporting for metrics.	M								
75	Staged Data: The solution should use a staged database system so that changes can be backed out when an issue is identified.	M								
76	PII (Personally Identifiable Information): The solution should automatically recognize, protect, and log PII data, changes, views, etc.	M								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
77	Matching: Knowledge Base: The system shall have the ability to interpret the meaning of text fields based upon the matching of characters strings against a knowledge base. In addition, the system shall have the ability to customize that knowledge.	M								
78	Security Solution: The solution shall meet industry, NIST, and FIPS security standards as required.	M								
79	Data Validation: The system needs to be able to sample data in fields ensuring that each field is not contaminated by integration efforts.	D								
80	Threshold Tolerance Limits: The solution will enable users to modulate the sensitivity of matching algorithms by assigning weights.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
81	Profiling: In-Place Profiling and Cleansing: The solution shall provide the ability to profile data in existing databases without the need to extract, move the data, or create a repository of results.	D								
82	Profiling: Scheduled/Batch Execution: The solution shall provide the ability to schedule profiling or cleansing processes to occur at any given interval or when a file is received by the ESB.	D								
83	Profiling: Drill Down into Data: The solution shall provide the ability for users to drill down into individual data sources and view specific records using a data viewer tool.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
84	Profiling: Historic Analyses: The solution shall store the results of a data profiling analysis in a data repository so that the history of data quality can be viewed and the improvement or degradation in data quality can be tracked.	D								
85	Profiling: In-Place Profiling and Cleansing: The solution shall provide the ability to profile data in existing databases without the need to extract the data, move the data, or create a repository of results.	D								
86	Pattern Matching: The solution shall ensure that data conforms to specific shapes and patterns.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
87	Parsing: Knowledge Base Creation and Maintenance: The system shall provide facilities for adding to or customizing terms in packaged knowledge bases and shall provide the ability to create new knowledge bases.	D								
88	Matching: Relationship Identification: The system shall provide functionality for the configuration and execution of rules and schemes to identify related data entities.	D								
89	Matching: Tune and Weight Matching: The system shall provide the ability to weight, prioritize, and tune matching rules (for example, to optimize the frequency and number of potential matches or the "tightness" or "looseness" of matching) so that one attribute may have more priority over another in any given record.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
90	Matching: Matching Types: The system shall use probabilistic, deterministic, and custom algorithms for finding, matching, merging, linking, and deleting relationships and duplicates within the data.	D								
91	Matching: Performance Matching: The solution should provide strategies for matching very large data sets using techniques such as blocking keys (AKA bucketing or pre-matching). The product should provide tools for setting up and activating these techniques.	D								
92	Data Stewardship: Role-Based Task Resolution: The solution should assign tasks to a cross-functional team to help mitigate match results or address specific records that do not comply with data quality rules.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
93	Data Stewardship: Assigning Tasks: The system should enable administrators to assign tasks to a cross-functional team.	D								
94	Console Application: Resolve Conflict: The system should provide a data steward console for resolving data conflicts and entering missing data elements.	D								
95	Console Application: Resolve Matching Records: The system should enable users to visually review whether two records match if there is uncertainty in the matching algorithms.	D								
96	Console: Web Accessible: The system should support a cross-functional team with an easy-to-use web-based work environment.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
97	Common Metadata: The system should offer an open metadata repository shared across all data sources.	D								
98	Metadata Synchronization: The system must offer automated bi-directional synchronization of metadata across multiple instances of the tools and data sources.	D								
99	Metadata Discovery: The system shall provide automated discovery and acquisition of metadata from various data sources, applications, and other tools.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
100	Postal Address Details: The solution must provide support for address extensions (such as the U.S. Postal Service's ZIP+4 code look-up service), change of address notification, and delivery-point validation. The solution must use address, ZIP code, and state to verify or supplement missing ZIP codes and postal codes. The solution must also check and format individual addresses.	D								
101	Third Party Libraries: The solution must leverage third-party address validation integrators to check addresses and validate them for postal discounts.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
102	Data Integration Automation: The system will obtain, cleanse, and deliver data in any latency or mode (e.g., federated SQL, web services, messaging, event-based alerts, and ETL) depending on the application's requirements.	D								
103	Case Management: The system will provide a case management approach to data cleansing that will facilitate multi-select assignments, disallow assignment to users without case/alert permission, support multiple links in a single attribute, support links in comments, permit control to view alerts, import and export filters, and provide quick option to delete all cases.	D								

EDQ Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
104	Dashboard: The system should have a dashboard system that can be customized for data sets that show trend analysis and error reporting. The dashboard should be easily configurable without requiring external programming.	D								
105	Parsing: Third-Party Tools: The system shall have the ability to perform parsing operations using knowledge bases from third-party sources.	D								
Technical Requirements										
106	Matching by Character String: The solution shall provide the ability to split text fields by matching character strings against packaged knowledge bases of terms, names, and more.	M								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
Business Requirements										
107	Data Consolidation: The solution shall be able to consolidate data across multiple solutions that will include data feeds, data management applications, and other solutions it connects to and will provide a single view of data records.	M								
108	Search: The solution shall be able to provide simple search and identification of data records.	M								
109	Probabilistic and Partial Search: The solution shall identify data records through probabilistic and partial search mechanisms with a toolset of solution rules and data-based rules set by DCRB.	D								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
110	Match Thresholds: The solution shall allow the setting of match thresholds by source and use.	D								
111	Security: The solution shall support IP range, role-based AD, and agency-based security access to the data.	M								
112	Resolution of Data Discrepancies: The solution shall be able to resolve data discrepancies in the data received across multiple solutions based on the rule set that has been defined.	D								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
113	Data Management: The solution shall be able to manage the data through effective and efficient: • data collection, • data aggregation, • data matching, • data transformation and standardization, • data checking (QA), • data storing, and • data sharing.	D								
114	Manual Override: The solution shall provide manual override for authorized users to resolve improper matches (and mismatches) and to preserve the override for that data record for future use.	M								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
115	Bulk Processing: The solution shall provide mechanisms for bulk processing of issues similar to the manual override requirement.	D								
116	Support Data Standards:- The solution shall support data standards such as Web Services, XML, CSV, TIPS, and any possible Federal standards that may be required.	D								
117	Synchronize Deltas: The solution shall synchronize with the changes that happen to any of the data records on any of the participating solutions through both batch and real-time mechanisms.	D								
118	Auditing: The solution shall provide an audit log [who, what, where, when, and why] of all manual updates to data.	M								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
119	Traceable Audit Mechanisms: The solution shall have an auditing mechanism to log and record the source of each activity related to the data including the distinct records that were used to arrive at the master record.	M								
120	Historical Data Management: The solution shall maintain both an historical record of all derived master records and associated detailed records.	M								
121	Consolidation to Master Record: The solution shall be able to resolve to one single record through multiple unique identifiers from different solutions.	M								
122	Fraud Detection: The solution shall be able to provide fraud detection mechanisms.	D								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
123	Data Flow: The solution shall provide a workflow analysis and diagram for each tool to demonstrate how the tool will be used and the interaction points for additional tools.	D								
Functional Requirements										
124	Support: Product end support should be best in class and available 24/7 as part of the solution. The SLA should be quantitatively proven and must be established to ensure that minimum acceptable standards are met.	M								
125	PII (Personally Identifiable Information): The solution should automatically recognize and protect PII data. It should also capture audit logs for PII data that has been viewed, modified, and deleted.	M								
Technical Requirements										

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
126	Service BUS Interface: The solution shall have a Service Oriented Architecture (SOA) that interfaces with a Service Bus by receiving and transmitting data through XML.	M								
127	Modular Services: The solution shall have modular and reusable services and components.	D								
128	Flexible Architecture: The solution shall have a flexible architecture that can easily incorporate changes (modify and create datasets quickly) and new features.	D								
129	Performance Standards: The solution shall meet the Service Level Agreement (SLA) and other performance standards set by DCRB.	M								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
130	Security Solutions: The solution shall meet industry, NIST, and FIPS security standards as required.	M								
131	Integration with EDQ: The solution shall be easily and seamlessly integrated with an ESB, EDQ engine, data warehousing, and other solutions that are a part of the DCRB enterprise architecture.	M								
132	Scalability: The system will meet scalability standards for both data size as well as demand for data.	M								
133	Maximum Uptime: The solution should leverage a base operating system (OS) that maximizes up-time and enables a scalable solution with multiple internal and external resources. Servers should enable isolation from other network devices and should provide a high security level to protect the PII information contained within.	M								

MDM Requirements										
ID	**Requirement**	**Mandatory**	**CC**	**VC**	**M**	**EE**	**C**	**NS**	**In Productive Use?**	**Comments**
134	System Support: The solution should be supportable through DCRB's internal technical support organization and should not require re-training of personnel beyond the tool; although, additional expertise may be required for the specific product line.	D								
135	OS: If multiple OSs are supported, a preferred, optimal OS should be recommended and be capable of integrating with DCRB's current environment.	M								
136	Enterprise Class: Because of the vital nature of the information constrained in this system, the solution must be enterprise-class capable of supporting millions of transactions on a daily basis regardless of the current user set.	M								

APPENDIX B

Board Lock-Out Rule

The Board of Trustees has established guidelines by which Board Members and staff will communicate with prospective service providers during a search process. The Policy is referred to as the Lock-Out Rule.

The Offeror shall not intentionally engage in unauthorized contract with Members or employees of the District of Columbia Retirement Board until such time as the offeror is notified an award has been made or the solicitation has been canceled, whichever occurs first.

"Unauthorized contact" means communication between the offeror and a Member or employee of the Board other than:

1. In the ordinary course of performing an existing contract;

2. In connection with an expired or terminated contract;

3. In the ordinary course of participating in the source selection process (e.g., responding to an invitation from the Board to submit written questions at a pre-Offerors conference or participating in contract discussions;

4. Regarding a matter unrelated to procurement; or

5. As a matter of public record.

A violation of this provision may disqualify the Offeror from participating in the source selection process.

APPENDIX C – Procurement and Conflict of Interest Rules

CHAPTER 2

Ethics

2.1 Policy

2.2 General Standards of Ethical Conduct

2.2.1 Employees

2.2.2 Non-Employees

2.3 Sanctions

2.3.1 Employees

2.3.2 Non-Employees

2.4 Conflict of Interest

2.4.1 Employees

2.5 Personal Gain

2.5.1 Employees

2.6 Restrictions on Employment of Present and Former Employees

2.6.1 Employees

2.6.2 Offeror, Contractor, or Subcontractor

2.1 Policy

Employees involved in the procurement process must conduct business impartially and in a manner above reproach, with preferential treatment for none. Employees must strictly avoid any conflict of interest or the appearance of a conflict of interest in the procurement process.

2.2 General Standards of Ethical Conduct

2.2.1 Employees

Any attempt to realize personal gain through employment with the Board or by conduct inconsistent with proper discharge of the employee's duties is a breach of ethical standards.

2.2.2 Non-Employees

Any attempt to influence any Board employee to breach the standards of ethical conduct set forth in this Chapter or in §§1602- 1604 of the Board's Procurement Regulations is a breach of ethical standards.

2.3 Sanctions

2.3.1 Employees

Disciplinary action may be taken against employees who violate any provision of §§1602- 1604 of the Board's Procurement Regulations or this Chapter. Any employee who violates any provision of §§1602- 1604 of the Board's Procurement regulations or this Chapter will be subject to discipline up to and including termination of the relationship with the Board.

2.3.2 Non-Employees

Any effort made by or on behalf of a non-employee, including an offeror or contractor, to influence an employee to breach the ethical standards set forth in §§1602- 1604 of the Board's Procurement Regulations or in this Chapter is prohibited and may be referred to appropriate authorities for civil enforcement or criminal prosecution. A violation by a contractor or subcontractor of §§1602- 1604 of the Board's Procurement Regulations or this Chapter constitutes a major breach of each Board contract or subcontract to which the violator is a party. In addition, an offeror or contractor that violates or whose representative violates any provision of §§1602- 1604 of the Board's Procurement Regulations or this Chapter may be determined to be non-responsible in future solicitations.

2.4 Conflict of Interest

2.4.1 Employees and Trustees

No employee or Trustee shall participate in or attempt to influence any procurement when the employee or Trustee knows or has reason to know:

The employee or Trustee or any relative of the employee or Trustee has a financial interest pertaining to the procurement;

The employee or Trustee or any relative of the employee or Trustee has a financial interest in a business or organization pertaining to the procurement; or

The employee or Trustee or any relative of the employee or Trustee has an agreement or arrangement for prospective employment with a business or organization involved with the procurement.

2.5 Personal Gain

2.5.1 Employees

It is a breach of ethical standards for any employee to receive or attempt to realize personal gain or advantage, either directly or indirectly, as a result of their participation in any action related to any procurement. No employee may solicit or accept, directly or indirectly, on his or her own behalf or on behalf of a relative, any benefit, such as a gift, gratuity, favor, compensation, or offer of employment from any person or entity having or seeking to have a contractual, business, or financial relationship with the Board.

In the event an employee is offered or receives any benefit, the employee shall report the matter to DCRB's ethics officer who shall determine the disposition of the benefit. The failure to report such offer or benefit to the ethics officer is a breach of these ethical standards.

2.6 Restrictions on Employment of Present and Former Employees

2.6.1 Employees

An employee who participates in the selection of a contractor, participates in the approval process of a contract or contract modification, or supervises contract implementation shall not be employed by the contractor in question with respect to the performance of the contract in which the employee participated.

2.6.2 Offeror, Contractor, Subcontractor

An offeror, contractor, subcontractor shall not:

1. Employ for a period of 24 months after separation a Board employee to work on a Board project on which the employee directly worked. The Executive Director may change this limitation period if it is determined that it is in the Board's best interests after review and recommendation by the General Counsel.

2. At any time after granting employment to any Board employee who participated in the selection of the contractor, participated in the approval of a contract or contract modification with the contractor, or supervised the contract implementation, allow such employee to work under the Board's contract resulting from the selection or approval.

3. Offer to perform work for the Board premised on the hiring of a Board employee to perform part of the work that may reasonably be expected to participate in the selection of that contractor, participate in the approval of a contract or contract modification with that contractor, or supervise contract implementation.

4. Perform work for the Board under the supervision, direction, or review of a Board employee who was formerly employed by the contractor without notifying the contracting officer in writing.

5. Allow the relative of a Board employee or Trustee to work on a contract for which the employee has any direct responsibility or supervision.

6. Permit any person whose employment the Board terminated, except pursuant to a reduction in force by the Board, other than pursuant to a reduction in force, to work on any Board contract or project.

7. Offer or grant a Board employee relative of Board employee, directly or indirectly, any benefit such as a gift, gratuity, favor, compensation, offer of employment, or any other thing having more than nominal monetary value or any other thing of value.

APPENDIX D

DCRB's PII Policy dated August 28, 2013

Information Technology

District of Columbia Retirement Board

Personally Identifiable Information Policy

in compliance with ISO 20000

August 28, 2013
Version 1.0

Table of Contents

Revision History

Version	Description of Change	Author/Reviewer	Date
0.1	Technical Authoring	Clay Pendarvis	8/14/13
0.2	Knowledge Editing	Tony Phan Ferdinand Frimpong Mark Bojeun	8/16/13
0.3	Review of Knowledge Editing	Tony Phan Mark Bojeun	8/16/13
0.4	Language Edit and Layout Editing	Justin Baker	8/19/13
0.5	Review of Language and Layout Editing	--	--
0.6	Management Editing	Leslie King	8/27/13
0.7	Review of Management Editing	Justin Baker	8/28/13
0.8	Final Editing	Justin Baker	8/28/13
1.0	Delivery	Peter Dewar	8/28/13

Approval

Peter Dewar, Director of Information Technology, DCRB

8/28/13
Date

Personally Identifiable Information Policy

1.0 Purpose

DCRB information technology (IT) recognizes its need to maintain the confidentiality of personal identifiable information (PII) and understands that such information is unique to each individual. This policy addresses PII that is managed and produced from various types of DCRB work activities and applies to DCRB employees, contractors, consultants, and vendors, including PII maintained on the DCRB customer base (District of Columbia teacher, police, and firefighter retirees).

2.0 Scope

The scope of this policy is intended to be comprehensive and includes requirements for the security and protection of PII throughout the agency and its approved vendors both onsite and offsite. All applicable DCRB departments will develop and implement specific processes and procedures for protecting PII when necessary. Such policies will be governed by applicable District of Columbia and Federal laws. These laws govern in the event of any conflict between these laws and DCRB policies.

3.0 Policy

In the DCRB organizational environment, PII is unique, personal data that includes, but is not limited to, the following:

- Social Security Numbers (or their equivalent issued by governmental entities outside the United States)
- Employer Identification Numbers (or their equivalent issued by government entities outside the United States)
- State or foreign driver's license numbers
- Date(s) of birth
- Government or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records

PII may reside in hard copy or in electronic records; both forms of PII fall within the scope of this policy.

3.1 Vendors

Individual(s) or companies that have been approved by DCRB as a recipient of organizational and member PII and from which DCRB has received certification of their data protection practices that conform to this policy. Vendors include all external providers of services to the agency as well as proposed vendors. No PII can be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information.

3.2 PII Retention

DCRB understands the importance of minimizing the amount of PII it maintains and will retain PII only as long as necessary. A joint task force comprising members of the DCRB Legal, Finance, IT, Contracts and Human Resources Departments will maintain organizational record retention procedures, which will dictate the length of data retention and data destruction methods for both hard copy and electronic records.

3.3 PII Training

All employees and contractors at DCRB who may have access to PII will be provided with introductory training regarding PII policy, will be provided a copy of this PII policy, and will be provided a copy of PII-related procedures for the department to which they are assigned. Employees in positions with regular ongoing access to PII or those transferred into such positions will be provided with training that reinforces this policy and reinforces the procedures for the maintenance of PII. Employees will receive annual training regarding the security and protection of PII and company proprietary data

3.4 PII Audit(s)

DCRB will conduct audits of PII maintained by DCRB in conjunction with fiscal year closing activities to ensure that this PII policy remains strictly enforced and to ascertain the necessity for the continued retention of specific PII throughout DCRB. Where the need no longer exists, PII will be destroyed in accordance with protocols for destruction of such records and logs will be maintained that record the dates of the specific PII destruction. The audits will be conducted by the DCRB Finance, IT, Procurement, and Human Resources Departments under the auspices of the DCRB Legal Department.

3.5 Data Breaches/Notification

Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, DCRB will notify all affected individuals whose PII may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible and will be provided no later than the commencement of the payroll period after which the breach was discovered.

3.6 Data Access

DCRB maintains multiple IT systems in which PII resides; thus, user access to such IT resources will be the responsibility of the DCRB IT Department. The DCRB IT Department will create internal controls for such IT resources to establish legitimate access for users of data, and access will be limited to those users approved by IT. Any change in vendor status or the termination of an employee or contractor with access to PII will immediately result in the termination of the user's access to all systems where the PII resides.

3.7 Data Transmission and Transportation

1. Within DCRB: DCRB will have defined responsibilities for onsite access of data that may include access to PII. DCRB IT Security will have oversight responsibility for all electronic records and data access to those electronic records. DCRB will be responsible for implementing the access and terminating the access of individual users to PII within the organization and providing timely notice to IT.

2. Agencies and Vendors: DCRB may share data with other agencies and vendors such as the Office of Personnel Management, the U.S. Department of the Treasury, and the DCRB independent actuary who have legitimate business needs for PII data. Where such sharing of data is required, the DCRB IT Department will be responsible for creating and maintaining data encryption and protection standards to safeguard all PII during transmission to those agencies and vendors. An approved vendor list will be maintained by the DCRB Procurement Department, which will be responsible for notifying DCRB IT of any changes to vendor status.

3. Portable Storage Devices: DCRB will reserve the right to restrict the PII it maintains in the workplace. In the course of doing business, PII data may also be downloaded to laptops or other computing storage devices to facilitate agency business. To protect such data, the agency will require that those devices use DCRB IT Department-approved encryption and security protection software while such devices are in use on or off company premises. The DCRB IT Department will be responsible for maintaining data encryption and data protection standards to safeguard PII that resides on these portable storage devices.

4. Off-Site Access to PII: DCRB understands that employees may need to access PII while off site or on business travel, and access to such data shall not be prohibited subject to the provision that the data to be accessed is minimized to the greatest degree possible while still meeting business needs and that such data shall reside only on assigned laptops/approved storage devices that have been secured in advance by the DCRB IT Department with data encryption and data protection standards.

4.0 Policy Enforcement

Failure to follow this policy may result in disciplinary action and/or contract termination.

5.0 Policy Owner

DCRB IT Security is responsible for this policy.

6.0 Policy Review

This policy will be reviewed annually by DCRB IT management. All employees, contractors, consultants, and vendors will review this policy, and will acknowledge in writing that they have read this policy.

Issue Date of Policy: February 2013
Next Management Review Date: February 2014

7.0 Policy References

- ISO 20000
- Information Technology Infrastructure Library (ITIL) standards
- DCRB IT Information Security Policy (February 15, 2013)
- DCRB Employee Handbook (November 2012)

APPENDIX E

DCRB's Information Security Policy 001

Dated August 28, 2013

Information Technology

District of Columbia Retirement Board

Information Security Policy

in compliance with ISO 20000

August 28, 2013
Version 1.0

Table of Contents

Revision History

Version	Description of Change	Author/Reviewer	Date
0.1	Technical Authoring	Mark Bojeun Tony Phan	10/18/2012 8/11/13
0.2	Knowledge Edit	Clay Pendarvis Ferdinand Frimpong Mark Bojeun	8/15/13
0.3	Review of Knowledge Edit	Mark Bojeun	8/15/13
0.4	Language Edit and Layout Edit	Justin Baker	8/16/13
0.5	Review of Language and Layout Edit	--	--
0.6	Management Review	Peter Dewar Leslie King	8/21/13 8/27/13
0.7	Final Editing	Justin Baker	8/28/13
1.0	Delivery	Justin Baker	8/28/13

Approval

Peter Dewar, Director of Information Technology, DCRB

8/28/13
Date

Information Security Policy

1.0 Purpose

This policy provides guidance on information security for the District of Columbia Retirement Board (DCRB) information technology (IT) network and information on the DCRB network. This policy is in alignment with International Organization of Standardization (ISO) 20000 requirements and any applicable Federal and District of Columbia laws.

2.0 Scope

This policy applies to all DCRB employees (full-time permanent employees, part-time permanent employees who work at least 20 hours per week, and any full- or part-time temporary or term employees), contractors, consultants, and vendors who use, manage, monitor, or maintain DCRB computer resources and devices. Parts of this policy also apply to DCRB trustees.

3.0 Policy

DCRB computer systems, including computer software, computer hardware, telecommunications equipment, and voice/data networks, and the information communicated, transferred, accessed, and/or stored via such systems will be secured and protected against unauthorized access and other forms of misuse. The use of DCRB information resources will be subject to monitoring and disclosure by DCRB at any time with or without notice. DCRB specifically reserves the right to access and disclose electronic communications and computer files when necessary for government investigations into allegations of misconduct, fraud, or other wrongdoing. In addition, computer files and electronic communications may be accessed for technical maintenance purposes to assure system security, compliance with agency policy and applicable legal requirements, and for any other legitimate agency purpose. The policies referenced in this document are designed to comply with applicable laws and regulations, which will govern if there is any conflict between this policy and applicable laws and regulations. These policies are the minimum requirements for providing a secure IT operational environment for DCRB.

3.1 General Information Security

DCRB IT will do the following to ensure general information security:

- Adequately and appropriately protect DCRB information resources against unavailability, unauthorized access, modification, destruction, or disclosure
- Appropriately provision authorized access to DCRB information resources
- Prevent disruption of business processes or service delivery caused by information security inadequacies
- Appropriately, efficiently, and effectively communicate DCRB's information security policies
- Define and assign responsibilities for protecting information technology resources

3.2 Agency Security

DCRB IT will do the following to ensure agency security:

- Provision an Information Security Incident Response Team with appropriate resources to exercise the DCRB information security incident response plan when appropriate.
- Designate a knowledgeable information security point of contact (POC) in accordance with the information security requirements. This POC (security administrator) will act as the central communications figure regarding information security within the agency.

3.3 Asset Classification and Control

All information resource assets owned by DCRB will be classified to ensure that they receive an appropriate level of protection from unauthorized disclosure, use, modification or destruction. Classified assets shall be protected in a manner consistent with their value, sensitivity, and criticality to the business and operation of DCRB and those it serves or as specified by any governing District of Columbia or Federal law or regulation.

3.4 Authentication

Authentication for remote access will use two-factor authentication as a minimum security control.

3.5 Remote Device Protection

DCRB IT will do the following to ensure remote device protection:

- Prevent remote PCs, laptops, and iPads devices from compromising the agency network by installing security software on all devices
- Installing and implementing firewall software on all devices to prevent them from being compromised by a virus or any kind of "back door" software
- Configure anti-virus software to automatically download and install the latest approved virus signatures

3.6 Personnel Security

Pursuant to the DCRB Employee Handbook, all DCRB employees, contractors, consultants, or vendors will be required to go through a background check process as a condition of employment. Only those who successfully pass the background check or provide other satisfactory documentation as required by DCRB will be allowed on site to perform their job functions.

3.7 Physical Security

DCRB IT will do the following to ensure physical security:

- Restrict physical access to the DCRB information resource assets and infrastructure to individuals who require that access to perform their job function

- Prevent unauthorized access, damage, or interference to DCRB premises and information by not giving unauthorized individuals access to the DCRB physical IT environment without formal escort
- Prevent loss, damage, or compromise of processing equipment or network components
- House critical, sensitive business information processing facilities in secure areas that are protected by a defined security perimeter with appropriate security barriers and entry controls that protect them from unauthorized access, damage, and interference
- Protect, at a minimum, all other processing facilities with a single security perimeter from unauthorized access, damage and interference
- Locate equipment in secured areas (Equipment located in areas where DCRB is unable to maintain a secure perimeter shall be locked in a secured cabinet with access controlled by DCRB IT Security. Secured cabinets or facilities shall support further segregation within the DCRB IT organization based on role and responsibility.)
- Protect infrastructure and related computing equipment from power failures and other electrical anomalies
- Protect power and telecommunications cables carrying data or supporting information services from unauthorized interception or damage
- Configure all endpoints that provide access to all systems so that a screensaver with password protection engaged or another lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended
- Orient all computing platforms with attached displays away from direct line of sight from unauthorized viewers

3.8 Communication and Operations Management

DCRB IT will do the following to ensure good communication and operations management:

- Document and maintain standard security operating procedures and configurations for the respective operating environments
- Reduce the risk of liability for the unauthorized use of unlicensed software, and minimize the threat of exposure due to software weaknesses and/or configurations
- Prevent the automated propagation of malicious code and contamination of sterile environments attached to the enterprise network
- Sanitize media resources containing sensitive data before transferal or reuse, and destroy the media resources when they are decommissioned
- Protect critical agency information resource assets, including hardware, software, and data from unauthorized use, misuse, or destruction
- Treat operating procedures relating to security as formal documents, and ensure changes are authorized by management
- Control and monitor changes to information processing facilities and systems for security compliance (Formal management responsibilities and procedures using a Change Management system shall exist to ensure satisfactory control of all changes to equipment, software, configurations, or procedures that affect the security of DCRB's operational environment.)

- Retain all written documentation generated by the change control policies via the Change Management system as evidence of compliance
- Support segmentation and layered security technologies and configurations based on role, risk, sensitivity, and access control rules in the DCRB operational environment

3.9 Virtual Private Network (VPN) Policy/Remote Access

DCRB uses the District of Columbia Government's virtual private network (VPN). TheDistrict Government's VPN gateways are established and managed by the Office of the Chief Technology Officer (OCTO). OCTO only allows access to its resources from external connections through an approved VPN with two-factor authentication method. DCRB will do the following to ensure protected VPN remote access:

- DCRB employees, contractors, consultants, and vendors with VPN privileges will ensure that unauthorized users are not allowed access to DCRB internal networks via their VPN.
- DCRB will not allow dual (split) tunneling. Only one network connection will be allowed per user VPN session.
- All computers connected to DCRB internal networks via VPN or any other technology will use the most up-to-date anti-virus software according to administrative standard. This applies to personal computers, laptops, and mobile devices.
- All computers connected to DCRB internal networks via VPN will have the latest operating system security patches applied.
- Any person or group accessing DCRB using the OCTO VPN will recognize and adhere to the responsibility to preserve the security, integrity, availability, and confidentiality of the DCRB information assets. Such information will be accessed and used strictly for conducting DCRB business or as appropriately authorized.
- DCRB will monitor each remote session, and the date, time duration, and user ID for each remote session will be audited. Inactive sessions will be timed out after a predetermined amount of time.

3.10 Personally Identifiable Information (PII)

DCRB IT will protect personally identifiable information (PII). PII within the DCRB environment includes the following:

- Social Security Numbers (or their equivalent issued by governmental entities outside the United States)
- Employer Identification Numbers (or their equivalent issued by government entities outside the United States)
- State or foreign driver's license numbers
- Date(s) of birth
- A combination of names and addresses that can be used to uniquely identify a person
- Government or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational records or approved vendor records
- Credit card numbers

4.0 Policy Enforcement

Failure to follow this policy may result in disciplinary action and /or contract termination in accordance with District of Columbia and Federal laws.

5.0 Policy Owner

DCRB IT Security is responsible for this policy.

6.0 Policy Review

This policy will be reviewed and updated annually and as needed by DCRB IT Security. All users will be responsible for reviewing this policy and related updates and will acknowledge in writing that they have read this policy.

Issue Date of Policy: February 2013
Next Management Review Date: February 2014

7.0 Policy References

- ISO 20000
- Information Technology Infrastructure Library (ITIL) standards
- DCRB IT Asset Classsification and Control Policy (February 15, 2013)
- DCRB IT VPN Access Control Policy (February 15, 2013)
- DCRB IT Physical Access Control Policy (February 15, 2013)
- DCRB IT Anti-Virus Access Control Policy (February 15, 2013)
- DCRB IT Information Security Incident Management Policy (February 15, 2013)
- DCRB IT Access Control Policy (February 15, 2013)
- DCRB IT Pesonally Identifiable Information (PII) Policy (February 15, 2013)
- DCRB IT Internet Access and Use Policy (February 15, 2013)
- DCRB IT Data Retention and Destruction Policy (February 15, 2013)
- DCRB Employee Handbook (November 2012)

APPENDIX F - DCRB's Task Order Template

DCRB CONTRACT NO. XX-##X-###
TASK ORDER No. ##-##

1.0 SCHEDULE:

[Task Number] [Task Name] [Pricing Model] NTE $ ##,##

2.0 BACKGROUND AND OBJECTIVES

[Define the overall background and purpose for the initiative]

[Describe the specific tasks or goals that the task will accomplish and the end-state to be achieved]

3.0 STATEMENT OF WORK

[Describe the tasks and effort necessary to meet the objectives]

3.0 PERIOD OF PERFORMANCE

[Date of Initiation through Completion]

4.0 DELIVERABLES

[Describe the specific deliverables to be achieved by the Task Order:

Deliverables are tangible achievements that the offeror will complete.

Deliverables are stand-alone in nature and should be testable and verifiable.

Deliverables may be part of a larger deliverable or can be distinct]

5.0 SPECIAL INSTRUCTIONS

[Describe any contract variations, assumptions, exclusions, or specific instructions provided to the integrator]

6.0 ESTIMATED HOURS AND COSTS

The following table provides an estimate of the hours and fees for accomplishing this task order.

Staff	**Rate**	**Hours**	**Fees**
Total			

AGREED:

Integrator

By: _____ _____

Program / Project Manager Date

DISTRICT OF COLUMBIA RETIREMENT BOARD

By: _____ _____

Contract Officer Date