DEPARTMENTAL INPUT
CONTRACT/PROJECT MEASURE ANALYSIS AND RECOMMENDATION

Rev 1

☒ New contract □ OTR □ CO □ SS □ BW □ Emergency

Previous Contract/Project No. EPP-RFP8570

□ Re-Bid □ Other

LIVING WAGE APPLIES: __YES _X_NO

Requisition/Project No: RQET1600052

TERM OF CONTRACT: _3_ years with _2_ two-year options-to-renew

Requisition/Project Title Agenda Management System

Description: for the purchase of an Agenda Management System to plan, coordinate, track, and manage Miami Dade County's legislative activities

User Department(s): Office of Agenda Coordination (OAC), Clerk of Courts (COC), CAO, COM

Issuing Department: ITD

Contact Person: Julian Manduley

Phone: (305) 596-8610

Estimated Cost: $150,000.00

Funding Source: Capital Outlay Reserve Funds

REVENUE GENERATING: No

ANALYSIS

Commodity/Service No: 920-45 SIC:

Trade/Commodity/Service Opportunities

Contract/Project History of Previous Purchases For Previous Three (3) Years
Check Here ___if this is a New Contract/Purchase with no Previous History

	EXISTING	2ND YEAR	3RD YEAR
Contractor:	Granicus	Granicus	Granicus
Small Business Enterprise:	N/A		
Contract Value:	$311,570	$100,000	$100,000

Comments: Initial Term Sum ($311,570) OTRs Sum to Date ($834,000) Total to Date ($1,145,570)

Continued on another page (s): ______Yes _______No

RECOMMENDATIONS

SBE	Set-Aside	Sub-Contractor Goal	Bid Preference	Selection Factor
		%		
		%		
		%		
		%		

Basis of Recommendation:

Signed: Tiandra Wright

Date to SBD: February 7, 2017

Date Returned to PM: ______________

2.0 Scope of Services

2.1 Introduction

Miami-Dade County, hereinafter referred to as the County, as represented by the Miami-Dade Information Technology Department, hereinafter referred to as "ITD" is soliciting proposals for the purchase of a hosted Agenda Management System (System) inclusive of software license, implementation, configuration, hosting, maintenance support, and professional services. The proposed System shall include a web-based, automated legislative workflow solution developed for the legislative process in governments. The proposed System that is designed to expand and accommodate the future needs of the County, and should include a highly intuitive user interface that is menu driven and flexible. The purpose of the System is to allow staff to easily manage the entire legislative process from start to finish including the ability to create and manage agendas and minutes for multiple Boards and subcommittees.

2.2.1 Technical Environment

To support the legislative process, Miami-Dade County currently uses the Legistar system written by Daystar Computer Systems, a provider of agenda management products and services to government agencies. Legistar is a comprehensive, integrated document management and information retrieval system designed specifically to support the legislative process in cities, towns, and counties. The system is comprised of a Microsoft Access 2000 front end and a SQL Server backend. Miami-Dade County purchased the source code from Daystar Computer Systems in 1999 and has been maintaining and enhancing the system since then. Granicus Inc., a government media provider, acquired Daystar Computer Systems in 2011. The code base for the system is about 17 years old. Microsoft no longer supports the version of Access required to run Legistar, therefore, the County has continued to maintain Legistar internally.

2.2.2 Operational Environment

Miami-Dade County's legislative process allows legislative matters (resolutions, ordinances, reports, presentations, discussion items, etc.) to be placed on an agenda by a County Commissioner, a Commission Committee, the County Attorney, Clerk of the Board and the Mayor. Items placed on an agenda by a County Commissioner, Commission Committee and/or the County Attorney are drafted and processed for placement on an agenda by the County Attorney's Office. Items placed on an agenda by the Clerk of the Board are prepared by the Clerk of the Board and processed for placement on an agenda by the Office of Agenda Coordination. Moreover, items placed on an agenda by the Mayor are drafted by departments. These items are approved by the Mayor's staff prior to being submitted to the Office of agenda Coordination for placement on an agenda. The proposed System is not required to use a "Per User" license model, however, the proposed System must accommodate an estimated 50-75 Concurrent Users. Users draft items simultaneously, while other items are in various stages of the approval process, agendas are being generated and minutes are being prepared. It is common for staff to work on multiple agendas simultaneously. Annually, the County processes about 2,000 - 3,000 legislative matters and generates between 100 - 125 agendas and minutes for the Commission. The size of items range from a single page to in excess of 500 pages. The County utilizes multiple workflows which are dependent on item type. Workflows are subject to changes based on Board approval or Chairperson approval. Therefore, it is important the proposed System provides workflow flexibility.

2.2 System Functionality

The proposed System should include the following functionality:

General

1. Create (data entry and generate) and manage agendas and minutes for approximately 138 Boards and subcommittees
2. Migrate data in our current legislative database into the new agenda management system
3. Provide unlimited data hosting and storage
4. Create and maintain multiple levels of security for users
5. Maintain an audit trail for administrative changes to legislative records
6. Accommodate simultaneous multiple-user access to all components of the system
7. Enable users to monitor the status of items
8. Make available legislative data, via Application Program Interface (API) or direct access, to other County websites and systems currently using legislative data
9. Provide secured storage of data and user credentials
10. Provide secured data communications between client workstations and main host

Preparation of Agenda Items

1. Provide standard Microsoft Word templates for drafting resolutions, ordinances, and reports
2. Provide Agenda item templates that include drop-down boxes as well as other features to reduce the amount of manual data entry
3. Provide spell checking that includes words in all capitals
4. Allow the attachment of files in various formats
5. Ability to create electronic versions of paper documents included as part of an agenda item submission
6. Enable user to identify the Prime Sponsor, Co-Prime Sponsor, Co-Sponsor as well as the departmental requester of legislative items
7. Ability to lock records (files) to prevent accidental modifications

Submission of Agenda Items

1. Simple and user-friendly interface for submitting items
2. Enforce submittal deadlines
3. Provide the ability to attach files in multiple file formats (Word, PDF, GIF, JPEG, etc.)
4. Allow agenda items to be moved as one package with all associated attachments

Workflow

1. Enable the County to define multiple configurable workflows
2. Allow reviewer to modify workflow to forward item to users that are not in the standard workflow
3. Allow assignments to delegates/backups when the reviewer is not available
4. Route items to reviewers automatically
5. Restrict access to items that are being reviewed
6. Enforce deadline for review of items
7. Allow for future redesign of workflow

Review and Approval

1. Allow reviewers to see list of pending items and have the ability to select the item that they would like to process
2. Show comments and track changes on documents
3. Provide automatic notification when document is revised
4. Once approved by a reviewer, only the approved version of the item flows to the next level for review
5. All document approvals of final items with approval code, electronic signature, or digital signature

Notification

1. Use email to notify reviewers that item is being prepared
2. Use email to notify reviewers that an item is pending their review
3. Use email to send reminders to appropriate staff to facilitate workflow
4. Allow for reviewer assignment escalation when items are not completed timely and management notifications based on deadlines
5. Use email to notify Agenda Coordinator that item has been submitted
6. Ability to customize notification message for specific tasks
7. Notify administrator if a reviewer in a defined workflow is no longer in active email directory

Agenda Publication

1. Allow items to appear on multiple agendas
2. Allow secured draft agendas to be created
3. Allow flexible formatting of agendas such as font and order of items
4. Allow user to set the order that sponsors appear on the agenda
5. Assemble all items into final agenda packet (e.g. packet should include agenda and agendas items with attachments)
6. Automatically convert all documents to PDF (OCR version) for printing and website publication
7. Link agenda items to the titles on the agenda
8. Insert page numbers on individual agenda items including attachments
9. Publish automatically to website
10. Publish to different media for distribution such as tablets or smartphones

11. Ability to notify Commission, staff and the public of the availability of an agenda and packet
12. Notify Commission, staff and the public when the status of the agenda changes such as Preliminary Agenda to Official Agenda
13. Notify Commission, staff and the public when a meeting is cancelled or rescheduled
14. Notify interested parties when certain subjects are on an agenda
15. Provide a method for downloading and printing an agenda with individual items, including any attachments
16. Provide the ability to download and/or view an agenda to any mobile device such as a tablet or smartphone
17. Ability to convert the final agendas to PDF and Word files
18. Ability to export agenda into Granicus Media Manager
19. Allow the public to receive agendas by email via subscription services.

Meeting Minutes

1. Convert agenda template into minutes format
2. Real-time recording of roll call and voice votes
3. Real-time recording of notes
4. Ability to capture vote per individual item or entire agenda section such as Consent Agenda
5. Ability to create Board actions

Post Meeting Follow-up and Research

1. Ability to use workflow post meeting for tracking and numbering items as well as signing documents
2. Provide for tracking of directives requested by the Board during meeting
3. Provide legislative history for each item
4. Allow user to search and access past and current items by keywords, dates or date range
5. Provide for full text search of agenda items
6. Ability to print search results
7. Ability to search on titles, body of an agenda item, and attachments
8. Ability to search records related to a vote
9. Ability to search records regarding meeting attendance

Reporting Features

1. Ability to generate reports with information consistent with the Changes Memo, Municipal Notices, and File Status Reports currently available in the existing system.
2. Generate listing of items scheduled for upcoming Board meetings by date of meeting and department
3. Ability to support flexible user-friendly searches based on user-defined criteria
4. Ability to export reports to Microsoft Excel and Word
5. Print reports

Reports

1. Generate Report that tracks Board and Committee actions
2. Generate Report that contains the information consistent with the current Pull List and Reasonable Opportunity Reports
3. Generate Public Hearing Report as sent to the BCC Chairman for approval
4. Generate daily, monthly and yearly management statistical reports including number of agendas, minutes and items processed.

Information Security

1. System uniquely identifies each user
2. System provides integration with Microsoft Active Directory for user authentication for Internal users (FIM/MIM)
3. System uniquely identify each process (system) account.
4. Default system accounts are either disabled or capable of being renamed. (e.g. administrator/admin, guest)
5. Accounts are automatically disabled after a configurable period of inactivity (e.g. 90 days).
6. Solution utilize account passwords for authentication.
7. Account Password complexity shall be configurable to allow for a minimum of 8 characters comprised of upper and lower alpha, numeric and special characters (e.g. !, @, #, $, %, &, *)

8. Passwords suppressed (not echoed back) when entered by users.
9. Passwords stored by the system must be encrypted with a minimum of AES 256 bit encryption
10. User login credentials (user account/password) encrypted in transmission with a minimum of AES 256 bit encryption
11. System supports implementation of configurable password aging (e.g. passwords expire every 90 days)
12. System supports password history functionality whereby password re-use is prohibited for a configurable number of prior passwords between 6 and 12.
13. System supports administrative Passwords Aging of 30 days.
14. Administrative accounts have the capability of resetting passwords
15. System provides user self-service password reset functionality utilizing a challenge and response authentication
16. Self-service challenge and response comprised of 8 challenge questions and store users responses during registration. Responses stored encrypted with a minimum of AES 256 bit encryption.
17. Self-service password reset present user with a configurable number of random challenge questions which when answered correctly will enable password to be reset.
18. System supports the ability to limit unsuccessful login attempts to 5. If the number of unsuccessful login attempts is exceeded, system lock out or disable user account.
19. System supports limiting concurrent user sessions to 1 by default. Number of concurrent user sessions shall be configurable by administrators.
20. System provides administrative capability to lock or disable accounts whenever necessary.
21. System displays a configurable warning, pre-login banner during solution login which indicates the unauthorized access is prohibited
22. System supports the ability to manage users based on group membership (role based privileges) in addition to assigning/revoking specific user based privileges
23. System provides tools and reporting to enumerate user rights/privileges, group membership, access to locations/functions or user profiles
24. System provides audit logging capability which captures successful logins, unsuccessful logins, records viewed, printed, added, deleted or modified and have the capability to retain logs for a period of 5 years plus current.
25. System audit logs captures date and time, user account, source IP address, audit event and success or failure of event
26. System prohibits administrators from disabling the audit mechanism
27. System ensures the audit log is protected from unauthorized access (i.e. logs are capable of simultaneously being sent to a logging server in addition to being maintained locally)
28. System prevents users or administrators from editing the audit log (modifying, deleting or adding log entries)
29. System provides software version controls to prevent outdated versions of software access to Database Management System (DBMS).
30. System generates outbound communications with data contained in messages (i.e. email alerts, automated reports, SMNP trap)
31. If the solution's database is relational, referential integrity is enforced by the RDBMS
32. The system prohibits users, developers, DBA's or system administrators from making changes to posted, completed or closed transaction records
33. The system provides rollback processes incorporated into the vendor hosted database for all critical transactions
34. The system ensures sensitive data (data that falls under the scope of FSS 539.003, CJIS, PII, SOX, HIPPA, and PCI requirements) is encrypted during transmission over the client's network (minimum AES 256 bit encryption)
35. The system ensures sensitive information (data that falls under the scope of FSS 539.003, CJIS, PII, SOX, HIPPA, and PCI) which is vulnerable to unauthorized access, encrypted while in storage (minimum AES 256 bit encryption)
36. The system ensures sensitive information (data that falls under the scope of FSS 539.003, CJIS, PII, SOX, HIPPA and PCI) is encrypted for transmission over external networks or connections. (minimum AES 256 bit encryption)
37. Hosted system is hosted in an audited data center complying with ISO 27001, SAS 70, SSAE 16 or SOC 3 audit standards

38. Hosted systems has controls in place which prohibit Hosting / Systems employees or 3rd party vendor technical support personnel access to or the ability to access, view or modify customer confidential data in compliance with FSS 536.003.
39. Hosted systems shall be physically located within the Continental United States.
40. Hosted system shall be a high availability solution with either active / active or active / passive failover between geographically dispersed data centers
41. Hosted system shall reside in a data center with appropriate physical access security controls in place.
42. Hosted system is accessible from the County network and Proxy infrastructure
43. Web based Hosted system encrypts all sessions from initiation to termination using current valid encryption cipher (SSL/TLS 1.1 or higher)
44. Hosted system must be scanned for vulnerabilities on a regular basis (monthly) using commercially available vulnerability scanners such as Nessus, Qualys etc. Monthly vulnerability reports must be shared with the County.
45. Hosted system must be regularly patched with appropriate OS/database/application security patches within 30 days of vendor release.
46. Hosted system must have "Critical" security patches applied within 7 (seven) calendar days of release from vendor.
47. Hosted system must be running on current supported release of OS/database/applications. End of Life (EOL) versions will be upgraded prior to end of vendor support date.
48. Hosted system must be scanned for Application vulnerabilities on a regular basis (monthly) using commercially available vulnerability scanners such as HP WebInspect, or IBM Ration AppScan, etc.
49. Hosted system has a change control processes implemented to provide application vulnerability scanning (OWASP top 20) prior to production migration of any changes. All "Critical and Severe" vulnerabilities will be remediated prior to migration. Application vulnerability reports will be shared with the County.
50. Hosted system protected using Intrusion Detection and Prevention technology (IDS/IPS)
51. Hosted system protected against Distributed Denial of Service (DDOS) Attack

2.3 Implementation Services

The selected Proposer shall be responsible for providing on-site or remote installation and configuration services for the proposed System. Additionally, implementation should include migrating the data in our current legislative database into the new agenda management system. The selected Proposer shall be responsible for testing the proposed System and insuring proper functionality prior to launching the proposed System.

2.4 Training Services

The selected Proposer shall provide on-site and web meeting-based training to staff on the use of the proposed System as well as customized documentation on the use of the proposed System. It is anticipated that this training shall include up to 10 members of staff. The County will provide an on-site facility and computer workstations available to the selected Proposer. Additional training shall be made available via on-line videos or other resources on an ongoing basis throughout the term of the contract awarded as a result of this solicitation.

2.5 Software Escrow

The selected Proposer shall be required to enter into a software escrow agreement with a licensed third party agent to house the source code associated with the proposed System at the time of Final System Acceptance.

2.6 Hosting Services

The selected Proposer shall provide hosting services, inclusive of data back-up, redundancy and data recovery capabilities, to include security updates, operating system patches, database and application level patching as well as backup management and disaster recovery testing. Hosting services may be either Proposer-hosted or cloud-hosted. The proposed System should be available 24 hours per day, 7 days per week to allow employees access, including remote access, if applicable, to the system. The selected Proposer shall assure 99.98% uptime 24/7, 365 days a year. The 99.8% uptime is calculated on a monthly basis. If this metric is not met then the County is due a hosting refund equal to the monthly hosting amount following the month in which less than 99.98% uptime occurred.

2.7 Training

The selected Proposer shall provide training services for approximately 70 administrators and users (initial and follow-up). The Proposer shall provide all necessary training documents (electronic and hard copy). The training sessions shall include but not be limited to the following groups:

- Search only users
- Users who draft and modify legislative items
- Users who approve legislative items
- Users who create agendas
- Users who create minutes
- System Administrators
- "Train the Trainers"

2.8 Maintenance Services

The selected Proposer shall provide maintenance services for the System throughout the term of the contract. These services shall include updates, patches, bug-fixes, corrections of defects, and upgrades to the System to ensure that the System will operate according to the specifications of the resultant contract and to maintain compatibility with future County hardware and software infrastructure. All software must be of the most recent release and all software upgrades issued by the selected Proposer must be available to the County at no additional charge.

2.9 System Support Services

The selected Proposer shall provide system support services Monday – Friday, 8:00 a.m. – 5:00 p.m., Eastern Standard Time, with access to support personnel after hours and weekends. Software support must be available and provided by vendor via a telephone hotline with a minimum of three support personnel available and a complete line of computers hardware able to test and recreate software situations.

2.10 Technical Support Services

The selected Proposer should have a technical support help desk available Monday through Friday, from 8 a.m. to 5 p.m. EST, in addition to email and web meeting support.

The County's preferred escalation process is outlined below:

Severity	Definition	Response Time	Resolution Time	Status Frequency Update
1=Critical	A major component of the System is in a non-responsive state and severely affects Users' productivity or operations. A high impact problem which affects the Users.	One (1) Hour	Four (4) Hours	One (1) Hour
2=Urgent	Any component failure or loss of functionality not covered in Severity 1, which is hindering operations, such as, but not limited to: excessively slow response time; functionality degradation; error messages; backup problems; or issues affecting the use of a module or the data.	Two (2) Hours	Eight (8) Hours	Two (2) Hours
3=Important	Lesser issues, questions, or items that minimally impact the work flow or require a work around.	Four (4) hours	Seventy two (72) Hours	Four (4) Hours
4=Minor	Issues, questions, or items that don't impact the work flow. Issues that can easily be scheduled such as an upgrade or patch.	Twenty-four (24) hours	One (1) Month for an acceptable work around until final resolution	Weekly Status Call