State of Iowa OCIO -- RFP #0822-721-01
RFP Scoring Methodology

RFP Technical Proposal Section	Scored Specification	Points Available
4.4.1	Describe the proposed solution, including product features/capabilities, alignment with the Agency's goals, system design, user experience, and other information supporting a determination that the proposed solution will meet the needs of the Agency for a Voter Registration and Election Management solution similar in nature to the background provided in Section 1.3 and the Mandatory Specifications in Section 4.3.	**74**
4.4.2	Provide contact information for at least three references for a completed Voter Registration and Election Management system (as described in Section 1.3) where you served as the prime contractor for the engagement or similar services for a governmental entity (city, county, state agency, or federal agency) within the last four years.	**17**
4.4.3	Provide a description of how you will respond to system malfunctions, security breaches, and diagnose and solve problems with the network, hardware, or software. Responses should include the plan to be provided to the State, which would include identifying the team responsible to resolve problems, a description of their actions, and the approach to that resolution.	**90**
4.4.4	Describe how the solution is optimized for use on mobile devices. Explain how the solution will provide functionality while also maintaining security for mobile access.	**6**

4.4.5	Describe how the proposed solution uses GIS information to maintain the most recent address information available in the state of Iowa.	**79**
4.4.6	Provide a solution that accommodates separate environments for production, testing, development, and training. The configuration allows a particular system component to exist in simultaneous, secure versions: (a) a production version, (b) a version undergoing testing, and (c) development.	**57**
4.4.7	Describe your experience in using an information technology lifecycle management process for work of the same scope as this project. Describe the lifecycle processes used to manage hardware and software. How will these processes ensure that updates appropriately address security considerations?	**170**
4.4.8	Describe how the proposed solution facilitates efficient communication from users to voters to keep them informed of things like registration status, absentee ballot status, polling locations, etc.	**124**
4.4.9	Describe the customization abilities designed into the proposed solution to enhance the user experience (for example, setting tabs or shortcuts for commonly used modules).	**68**
4.4.10	Describe how the proposed solution allows users to efficiently administer multiple elections simultaneously.	**107**
4.4.11	Describe how the proposed solution assists users with election scheduling and organizing/managing the timelines for each election.	**51**

4.4.12	Describe how the proposed solution provides useful warnings or prompts to users to ease use and maintain election and voter records.	**90**
4.4.13	Describe how system administrators can customize the notifications for alerts related to errors, performance, and usage volume.	**40**
4.4.14	Provide information about your capability to scale during higher peak election periods.	**130**
4.4.15	Describe how the proposed solution facilitates easy, quick, and efficient data entry (e.g. automated data formatting, highlighting required fields, positional cursor control, predictive/suggested text or addresses, etc.).	**113**
4.4.16	Describe the application programming interface (API) capabilities within the proposed solution, such as connecting to the state Department of Transportation for validation of voter information and ID number. Additionally, explain the process for creating new interfaces as external systems are created or change. Describe the security controls for the API.	**181**
4.4.17	Describe how the search function in the proposed solution aids users in locating information in an easy, swift, and efficient manner.	**130**
4.4.18	Describe the analytics capabilities of the proposed solution	**28**

4.4.19	Describe the process for creating, saving, and refining user-created reports in the proposed solution, emphasizing the ease of use for new or unfamiliar users.	**79**
4.4.20	Demonstrate how users can access reporting tools quickly and easily from any part of the proposed solution.	**57**
4.4.21	Describe how the proposed solution facilitates reconciliation of voter registrations after redistricting.	**34**
4.4.22	Describe how your solution facilitates the easy setup of an election, including selecting the correct districts for an election, and conversely, the elections relevant to a given district. Also include how the solution facilitates the combination of precincts and polling locations in order to coordinate elections.	**158**
4.4.23	Describe how the proposed solution conspicuously indicates if a voter is currently ineligible to vote, but will be eligible in time for the election, per Section 4.3.162.	**40**
4.4.24	Describe how the proposed solution handles UOCAVA requests for an extended period of time.	**181**
4.4.25	Describe how the proposed solution notifies users to follow up on absentee ballots not yet received and complete.	**23**
4.4.26	Explain how the solution will assist users in creating PEO records and assigning PEOs to the polls for a given election.	**45**

4.4.27	Describe your project management plan for implementation of the proposed solution.	**158**
4.4.28	Provide a detailed description of your training plan for both state-level and county-level staff, including system administrators.	**141**
4.4.29	Provide a description of processes you use for testing, patching, and anomaly handling.	**249**
4.4.30	Describe the security environment for the proposed solution, including the measures designed to prevent unauthorized access to voter and election records.	**283**
4.4.31	Describe the internal control structure of the proposed solution, as relates to the prevention of voter fraud.	**136**
4.4.32	Describe how the proposed solution assists Users in determining NVRA status, active vs. inactive voter status, eligible vs. ineligible, etc.	**181**
4.4.33	Provide all work locations and descriptions of physical and logical security requirements, handling of sensitive materials, and emergency and disaster backup provisions. Describe how you will manage various work locations from the perspective of election security. This includes adherence to the State requirements that all work and data storage be maintained in the United States, as applicable.	**198**

4.4.34	Describe the security audits and penetration analysis performed on a regular basis. If conducted, provide annual security audit reports conducted by an independent auditor. Provide examples of prior security testing and evaluation reports, vulnerability assessment reports, and any related reports.	**209**
4.4.35	Provide evidence of certification or registration according to national quality or security standards. Describe your adherence to standardized quality principles, such as through registration as ISO 9001 (general quality) and ISO/IEC 27001 (information security). Both are strongly preferred. If you do not follow a standardized quality principle, provide your documented processes and evidence that you monitor adherence to those processes.	**204**
4.4.36	Detail your approach to supply chain management, including the selection process for suppliers.	**158**
4.4.37	Describe how information sensitivity is categorized and how access to sensitive information is managed and documented for each category, including your ability to create reports and machine-readable data extracts for both private and public dissemination. Clearly designate responsibilities, obligations, and procedures for key aspects of a data governance plan (data owner, data steward, data retention, information sensitivity, etc.). Demonstrate your understanding of this jurisdiction’s data governance policies and practices and propose a data governance approach as part of your submission.	**255**

4.4.38	Describe in detail the controls placed on data and access to data. Include requirements for location, access rights, maintenance and enforcement of access rights, encryption, incident response and backup capabilities, and logging and forensics capabilities.	**271**
4.4.39	If the solution will be hosted in a cloud or multi-tenant environment provided by Azure, AWS, or Google, include information on the adherence to the appropriate CIS Benchmark for Cloud Service Offerings. Explain the reason for any deviation from that Benchmark and provide any additional options that are available. If using another cloud provider, include the full menu of security options and services offered by the hosting provider, and which specific security options and services are included in the proposal.	**271**
4.4.40	For user- and client-specific software and applications, confirm on which types of systems and, where applicable, browsers the product will have full functionality. In general, products should be fully functional on a host of systems, to include netbooks (such as Chromebooks) and all major browsers. If managing voter or ballot data, provide the data format(s) you are using and identify common functions supported with those formats (e.g., risk-limiting audits).	**232**
4.4.41	Provide a full description of the proposed solution's security architecture. Describes completely how architecture will ensure security of election infrastructure.	**277**

4.4.42	Describe your approach to cryptography, including which cryptographic modules and protocols you use, and how you conduct key management and manage the secrecy of private keys, if applicable.	**119**
4.4.43	If the proposal includes commercial off-the-shelf (COTS) or modified off-the-shelf (MOTS) software, address ownership of the software and design assets both during the project and afterward. Also, address whether source code and other artifacts will be held in escrow or delivered to the State during the project, and ownership of IP rights at the end of the project.	**170**
4.4.44	Detail certifications obtained for the solution(s) you intend to deploy and how these meet applicable federal, state, or local security standards.	**136**
4.4.45	If personal information will be handled, describe how you will manage the minimization, collection, storage, and transmission of that PII. Describe confidentiality and privacy approaches with regard to personal information.	**181**
4.4.46	Confirm that you have advanced endpoint protection for any server or workstation that is part of the core service offering.	**187**
4.4.47	Define specific levels of service for key work activities including performance standards for each service. These should include, but not be limited to:	**221**

4.4.48	Provide a description of the threat environment as it applies to the systems and their interconnections that are addressed in your proposal. Provide an assessment of the severity of threats, and identify and align mitigation approaches to the threats. Also, provide an assessment of the residual risks following mitigation actions.	**175**
4.4.49	Describe how you monitor ongoing security threat changes and respond to evolving threats, including monitoring common vulnerabilities and exposures (CVEs) and any ability to receive and share real-time threat information.	**249**
4.4.50	Provide detailed information regarding cybersecurity controls relevant to the vendor's selected framework throughout the life of the Contract.	**232**
4.4.51	Clearly describe expected scope of cybersecurity-related tasks under this contract and who (e.g., contractor, State) is responsible for executing those tasks.	**243**
4.4.52	Describe your process for moving data, whether digitally or physically, while maintaining appropriate security protection and data integrity.	**192**
	Total Possible Points for Technical Proposal	**7500**
RFP Attachment #1 Cost Proposal	**Cost Criteria**	**Possible Cost Points**

Total Possible Cost Proposal Points	The qualified Respondent with the lowest all-inclusive total cost will be awarded the maximum points. All other Respondents will receive a Cost Proposal score proportional to the lowest cost proposal.	**2500**