Iowa Judicial Branch Request for Quotation	
PROJECT TITLE:	**Random Moment Sampling System and Title IV-E Claim Support**
REFERENCE NUMBER:	RFQ JUV-27-4E-SW-003
ISSUED BY:	Angi Hillers, Issuing Officer
DATE OF ISSUE:	Monday, May 11, 2026
CONTACT DETAILS:	Iowa Judicial Branch (IJB) 1111 East Court Avenue Des Moines, IA 50319 Angi.Hillers@iowacourts.gov
QUOTATION RETURN DATE AND TIME:	Friday June 19, 2026 no later than 3:00 PM CST
DOCUMENTATION REQUIRED:	An electronic, responsive submission broken out as outlined below. Submissions must include acknowledgement of an affirmative answer for each requirement, as well as how the proposed solution will meet requirements that require description and any additional supporting documentation required.

DETAILS

1. SUMMARY

This RFQ seeks a vendor to assist Juvenile Court Services (JCS) within the Iowa Judicial Branch (IJB) to:

1. Provide expert consultation and technical assistance with all aspects of Title IV-E claiming, including Administrative, Prevention Services, and Training.
2. Configure, implement, operate, and maintain a comprehensive web-based RMS system for Title IV-E Administrative claiming.
3. Draft, review and/or enhance Title IV-E Administrative claiming through quarterly evaluation of program and activity coding.
4. Provide appropriate reports as scheduled and/or on demand.
5. Provide technical assistance in case of an audit.

6. Complete required quality assurance (QA) activities and provide ongoing evaluation and advisement of internal JCS Title IV-E QA processes.
7. Provide assistance with the development of training programs, including preliminary training for new users, as well as ongoing evaluation and recommendations for improvement.
8. Participate in a minimum of quarterly virtual meetings to review data, trends and areas for improvement.

1.2 BACKGROUND

The mission of Juvenile Court Services (JCS) is to serve the welfare of children and their families within a sound framework of public safety. JCS is committed to providing the guidance, structure and services needed by every child under its supervision. Participation in Title IV-E claiming will continue to provide JCS with an additional funding source that can be utilized to develop and enhance youth and family programming and services.

In April of 2021, Iowa JCS implemented random moment sampling to claim federal reimbursement for certain administrative activities related to the proper and efficient administration of the Title IV-E Prevention Program. These included activities to develop necessary processes and procedures to establish and implement the provision of prevention services and programs for eligible individuals, policy development, program management, and data collection and reporting.

Additionally, Iowa has been claiming for allowable child-specific administrative activities, such as verification and documentation of program eligibility and activities that comport with or are closely related to one of the listed activities in 45 CFR 1356.60(c)(2), which include:

- Referral to services;
- Preparation for and participation in judicial determinations;
- Placement of the child;
- Development of the case plan;
- Case reviews;
- Case management and supervision;
- A proportionate share of related agency overhead; and
- Costs related to data collection and reporting. [1]

2.0 OBJECTIVES

This RFQ seeks a vendor to assist Juvenile Court Services (JCS) within the Iowa Judicial Branch (IJB) to:

2.1 Provide consultation and Subject Matter Expertise in Random Moment Sampling and all aspects of Title IV-E Claiming.

2.2 Provide JCS with timely notification of developments or changes to Title IV-E claiming.

[1] Children's Defense Fund (2020). *Implementing the Family First Prevention Services Act: A technical guide for agencies, policymakers and other stakeholders*.

2.3 Procure, as a service, an online and email-based RMS system that meets all federal and state requirements and accurately allocates JCS Title IV-E allowable costs.
2.4 Ensure JCS is maximizing claiming for all allowable Title IV-E costs.
2.5 Evaluate reporting needs on an ongoing basis and provide access to accurate reporting of Title IV-E data.
2.6 Identify and implement QA measures required to ensure compliance with Title IV-E federal and state requirements.
2.7 Collaborate with JCS staff to evaluate needs and develop and deliver training.

4. REQUIREMENTS

Responsive quotations must acknowledge an affirmative answer confirming your company and proposed solution meet all the requirements below and provide details when prompted to describe specific items.
Only quotations that meet all requirements will be considered responsive.

A. **Vendor Experience**. The vendor must have:
   A.1. Experience establishing, implementing, and providing ongoing support for at least 3 functional email-based RMS systems, which meet all state and federal requirements. **Describe**.
   A.2. A minimum of 5 years' experience in all aspects of Title IV-E claiming. **Describe**.
   A.3. A minimum of 3 years' experience in ongoing quality assurance development and implementation for Title IV-E activities. **Describe**.
   A.4. Experience evaluating and providing ongoing training to support the RMS system that ensures adequate responses to maximize federal reimbursement. **Describe**.

B. **General**. The proposed solution must:
   B.1. Provide, configure, operate, and maintain a comprehensive web-based Random Moment Sampling system (RMS), which is statistically valid, and compliant with all federal and state guidelines and requirements. **Describe**.
   B.2. Deliver technical Title IV-E administrative services, including cost reporting, accurately drafting quarterly claim for timely submission and enhancement and evaluation of program and activity coding ensuring compliance with federal and state Title IV-E guidelines. **Describe**.
   B.3. Assist JCS in properly allocating Title IV-E administrative costs to their appropriate cost centers and ensure that the costs identified are permissible for federal financial participation (FFP) and are the only costs allocated to the Title IV-E program if applicable. **Describe**.
   B.4. Ensure that any eligible population and services are included in the Title IV-E program and activities and review existing JCS programs and activities to identify and propose Title IV-E reimbursable activities currently being performed but not claimed. **Describe**.
   B.5. Evaluate reporting needs on an ongoing basis and provide access to accurate reporting of Title IV-E data. **Describe**.
   B.6. Provide technical assistance services for all aspects of Title IV-E claiming for which JCS is eligible. **Describe**.

B.7. Provide technical assistance services for implementation of the Title IV-E RMS claiming system, including identifying needs and providing initial and ongoing staff training. **Describe**.

B.8. Provide technical assistance in case of an audit. **Describe**.

C. **RMS Functional Description**. The proposed solution must:

C.1. Provide a functional RMS system that meets both state and federal requirements as an acceptable cost allocation methodology for JCS.

C.2. Generate ongoing Random Moment Samples (samples); and send them electronically to eligible participants. Responses should not require a login. Participants must receive instant confirmation that their sample has been recorded successfully.

C.3. Monitor and collect sample responses; validate sample responses; and align each sample to the appropriate program and activity code.

C.4. Ensure that program and activity codes capture all the activities performed by the participants and distinguish Title IV-E activities from similar activities that are not eligible for Title IV-E reimbursement. This should be accomplished using “parallel” program and activity codes.

C.5. Require a narrative/free-text comment description of each activity selected, along with the activity code to ensure quality assurance. The narrative/free-text comment description must be stored in a manner that makes the comments available for QA purposes.

C.6. Provide a question in the response asking if the participant is working with a specific youth, and if the answer is yes, provide space for participant to enter the youth’s Juvenile Identification number (JID).

C.7. Store and report each sample’s initiation date and time, the participant name, confirmation of receipt, submittal of response, the time of sample completion, the program and activity codes selected, as well as the free text comments provided. All information must be available for audit purposes.

C.8. Send reminder emails to unresponsive participants at required intervals. Survey moments must expire at federally required intervals. Participants must not be able to respond to samples after federally required expiration.

C.9. Ensure work schedules for each participant can be programmed and adjusted quarterly within the RMS system to ensure samples are only sent during each participant’s work hours.

C.10. Maintain and store required identifiers associated with each participant for each sample.

C.11. Provide designated JCS users with adequate permissions to (at a minimum) create, edit, and update the sample group, user information, and participant work schedules within the RMS system.

C.12. Ensure statistically sound random moment samples.

D. **RMS User Permissions**:
   D.1. Participants with standard permissions must be able to respond to samples by connecting to the website/database from a secure link in an email notification without requiring a login.
   D.2. Administrative users must have the required permissions to view initiated samples and associated submissions, including the ability to monitor participant responses, as well as the ability to view free-text comments provided in each sample. They must have the ability to create, edit, and delete participant information, as well as the ability to update work schedules for participants. They must have the ability to generate reports and create queries, in cooperation with the selected vendor.
   D.3. All edits and deletions must be recorded.

E. **Sampling Methodology**. The proposed solution must:
   E.1. In coordination with JCS, implement a federally compliant sampling plan methodology within the RMS system for selecting the random samples.
   E.2. Cover the entire sample period, such as quarters, and must account for holidays, vacations, sick time, lunch hours, and other paid time not at work.
   E.3. Assist JCS to identify and sample all eligible participants.
   E.4. Generate an adequate number of samples to ensure validity to comply with federal requirements.

F. **Quality Assurance/Monitoring.** The selected vendor must:
   F.1. Provide quality assurance and monitoring to ensure sample is statistically valid and conducted in compliance with federal and state requirements. **Describe**.
   F.2. Perform quarterly reviews to ensure proper procedures and accurate claims. **Describe**.
   F.3. Continually review the RMS methodology to assure it meets current federal regulations.
   F.4. Remain current on all Title IV-E training. **Describe**.
   F.5. Notify JCS staff of Title IV-E training opportunities as they arise.
   F.6. Validate that each sample comment matches the chosen program and activity.
   F.7. Provide JCS with a report containing a random list of 10% of eligible candidate samples each week for quality assurance review.
   F.8. Provide JCS with a report containing a random list of an additional 10% of eligible candidate samples each week for supplemental quality assurance review.
   F.9. Provide JCS with a report containing a list of samples including Juvenile Identification number (JID) each week for quality assurance review of case number accuracy.

G. **Reporting and Ability to Query.** The proposed solution must:
   G.1. Provide standard reports that sort and display data in ways most commonly requested by human service and juvenile justice agencies.
   G.2. Provide additional JCS configurable reports, defined by JCS needs, and detailed in a vendor and JCS developed script. **Describe**.
   G.3. Allow JCS to have access and the ability to run scripts against the data with cooperation and assistance of the selected vendor, as a means of analysis for which no standard report is available.

H. **Audits.** The selected vendor must:

H.1. Maintain a fully automated audit trail system with audit records for information that, at a minimum, collects data associated with each change transaction to its initiator, captures date and time of system events and types of events. The audit trail system shall protect data and the audit tool from addition, modification, and/or deletion, and should be regularly reviewed/analyzed for indications of inappropriate or unusual activity.

H.2. Provide technical assistance to JCS in the event of an audit, including, but not limited to:

H.2.1. Timely consultation.

H.2.2. Supporting applicable fiscal claim documents.

H.2.3. Supporting documentation related to development of the methodology for allocation of Title IV-E costs.

H.2.4. Records supporting initial training for participant staff.

H.2.5. Documentation related to and supporting quality assurance processes.

I. **Connectivity and Access.** The proposed solution must ensure that:

I.1. Network performance of the website hosting the RMS application meets or exceeds:

I.1.1. download 250Mbps

I.1.2. Upload 250Mbps

I.1.3. JCS performs its own application support, with cooperative recommendations from selected vendor, limited to:

a. Design and entry of questions
b. Design of entry of responses
c. JCS device updates as necessary
   i. Browser setting changes
   ii. Registry settings

I.2. Require NO installable software for participants.

I.3. Authenticate client device to secure website without requiring login to record sample.

I.4. Useable on PCs running Windows 10 and above, iPads running iOS 13.6.1 or above, MacOS 10.15.6 or above, tablets and smart phones running Android 8 and above, and iPhone 7 or above.

I.5. Useable at a minimum resolution of 1280 x 720.

J. **System Hosting Performance and Maintenance.** The proposed solution must:

J.1. Perform a service level response within a 24-hour window to correct down network, or non-responsive service during work / survey hours.

J.2. Support client responses via Outlook email and/or link to secure website delivered via email.

J.3. Perform all hosting maintenance tasks, except in case of emergency:

J.3.1. Outside JCS stated business hours;

J.3.2. Notify JCS Administrators of planned maintenance window at least 48 hours in advance;

J.3.3. Provide JCS Administrators at least 48 hours written notice of upgrade/maintenance/repairs:

a. An Emergency patch requires a 1 hour notice

b. Visible to users, including screen format changes and access to RMS.
c. Require a change in input.
d. Security upgrades, changes, breeches, known attempted breeches, and preventative measures or resolution of breeches.

J.4. Selected vendor will notify JCS Administrators, in writing, at a minimum of 3 months in advance of proposed updates that may impact:

J.4.1. Security requirements stated elsewhere in this document.
J.4.2. Browser updates or delay of browser updates.
J.4.3. O/S updates on any of the approved platforms (listed previously).
J.4.4. Other changes that require updates, configuration changes, or other IJB IT provided service to participants PC, tablet, or smartphone.

K. **Security.** Selected vendor must perform services and conform the RMS application to all Iowa Judicial Branch (IJB) security policies, and applicable federal regulations and guidelines related to security, confidentiality, and audit trails and controls, as periodically updated.

K.1. Host security

K.1.1. Vendor must submit their written security policy addressing their standards and practices to protect data and files from unauthorized access or disclosure.
K.1.2. Vendor must implement reasonable and prudent physical safeguards that are consistent with industry standards that will protect the host facility and JCS data from unauthorized access. These safeguards must also minimize the risk of damage from fire, smoke, water, vermin, and other hazards and disasters.
K.1.3. Support Security audits as required.
K.1.4. Provide immediate Security Incident Reports to JCS-identified contacts if a security incident happens within the selected vendor's purview.

K.2. Website/Web app Security

K.2.1. Nominal strength of 128 bits or higher.
K.2.2. TLS 1.3
K.2.3. JCS will provide appropriate browsers, including the current, latest released versions of, which should be supported by the application:

- Chrome
- FireFox
- Edge

L. **Compliance with Laws and Standards**.

L.1. Selected vendor must comply with all applicable federal, state, and local laws, regulations and standards including, but not limited to:

L.1.1. Iowa Consumer Data Protection Act (ICDPA), effective January 1, 2025, which governs the processing of personal data of Iowa residents (Senate File 262).
L.1.2. Iowa Code Chapter 715C, which defines security breach notification requirements for personal information, including encrypted or redacted data if decryption keys are compromised.
L.1.3. Health Insurance Portability and Accountability Act (HIPAA), if applicable.
L.1.4. Federal Information Security Modernization Act (FISMA).
L.1.5. National Institute of Standards and Technology (NIST) Special Publication 800-53 (Security and Privacy Controls).
L.1.6. Payment Card Industry – Data Security Standard (PCI-DSS), if applicable.

L.2. Adhere to industry standards such as ISO/IEC 27001 or SOC 2 Type II, with evidence of current certification or compliance.

L.3. Provide annual third-party audit reports (e.g., SOC 2, penetration testing results) to verify compliance.

M. **Data Protection**.

M.1. Encrypt all sensitive data, as defined by ICDPA (e.g., racial or ethnic origins, health data, genetic or biometric data, precise geolocation, and children's data), at rest and in transit using industry-standard encryption protocols (e.g., AES-256, TLS 1.3).

M.2. Implement access controls based on the principle of least privilege, ensuring only authorized personnel can access sensitive data.

M.3. Maintain data segregation to prevent unauthorized access between different clients or datasets.

M.4. Develop and maintain a data retention and disposal policy, ensuring secure deletion of data in accordance with state retention schedules and ICDPA requirements for consumer deletion requests.

N. **Identify and Access Management (IAM)**.

N.1. Implement multi-factor authentication (MFA) for all users accessing systems or applications containing Iowa Judicial Branch data.

N.2. Use role-based access control (RBAC) to manage user permissions.

N.3. Maintain audit logs of all access to systems and data, retaining logs for a minimum of 12 months, as aligned with Iowa Code Chapter 715C requirements for security breach investigations.

N.4. Conduct regular reviews of user access privileges, at least quarterly, to ensure compliance with access policies.

O. **Security Operations**.

O.1. Maintain a Security Operations Center (SOC) or equivalent capability to monitor systems 24/7 for security incidents.

O.2. Implement endpoint detection and response (EDR) tools to detect and mitigate threats on all devices accessing Iowa Judicial Branch data.

O.3. Perform regular vulnerability scans and remediate identified vulnerabilities as soon as reasonably possible, and not to exceed 30 days for critical vulnerabilities.

O.4. Conduct annual penetration testing by a qualified third party and provide a summary of findings and remediation plans.

P. **Incident Response**. The following definitions apply to this sections, as well as the rest of this RFQ.

- **"Security Breach"** means the loss of control, compromise, unauthorized use, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses personally identifiable information; or an authorized user accesses Customer Data for a reason other than an authorized purpose.
- **"Security Incident"** means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of (1) Customer Data, and/or (2) an information system or the information the system Processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

P.1. Develop and maintain an incident response plan aligned with NIST SP 800-61 (Incident Handling Guide) and Iowa Code Chapter 715C, which requires notification of security breaches affecting personal information.

P.2. Notify the Iowa Judicial Branch and the Iowa Attorney General of any confirmed security incident or security breach.

P.3. For breaches affecting more than 500 Iowa residents, timeframe for notification is within 24 hours of discovery, as required by Iowa Code Chapter 715C.

P.4. For all other incidents or breaches, affecting fewer than 500 Iowa residents, timeframe for notification is the shorter of

P.4.1. 72 hours

P.4.2. The timeframe listed in the Purchasing Instrument, or

P.4.3. The timeframe imposed by applicable law.

P.5. Provide a detailed incident report within 5 business days of incident resolution, including root cause analysis and mitigation steps.

P.6. The Vendor agrees, at its sole expense, to take all steps necessary to promptly remedy any Security Event and to fully cooperate with the Iowa Judicial Branch and designated security personnel in investigating and mitigating any damage from such Security Events.

P.7. Upon notice of any Security Event, the Vendor will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to the Security Event. As soon as practicable during the investigation, the Vendor will deliver to the Iowa Judicial Branch a Security Event assessment and the Vendor's plans for future mitigation.

P.8. Vendor will be responsible for all applicable consumer notification requirements in the event of a Security Event caused in whole or in part by Vendor.

P.9. Vendor will be responsible for all damages arising directly or indirectly, in whole or in part, out of any Vendor act or omission related to a Security Event. Any such damages will be construed as direct damages for purposes of this Agreement, and such damages expressly include any costs, expenses, damages, fines, legal fees (including the time and expense of the Iowa Attorney General's Office), and court costs related to the Security Event.

Q. **Cloud Security (if applicable)**.

Q.1. Use cloud service providers that are StateRAMP/GovRAMP or FedRAMP-authorized at the appropriate impact level (e.g., Moderate or High) for hosting Iowa Judicial Branch data.

Q.2. Implement cloud security controls in accordance with the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

Q.3. Provide documentation of shared responsibility model, clearly defining vendor and Iowa Judicial Branch security responsibilities.

R. Personnel Security.

R.1. Conduct background checks on all personnel with access to Iowa Judicial Branch systems or data, in accordance with state requirements.

R.2. Require all personnel to complete annual security awareness training covering topics such as phishing, data handling, and incident reporting.

R.3. Enforce nondisclosure agreements (NDAs) for all personnel handling sensitive Iowa Judicial Branch data.

S. **Business Continuity and Disaster Recovery**.

S.1. Maintain a business continuity and disaster recovery (BCDR) plan to ensure service availability in the event of a disruption.

S.2. Test BCDR plans annually and provide a summary of test results to the Iowa Judicial Branch as requested.
S.3. Ensure data backups are encrypted, stored securely, and tested regularly for restorability.
S.4. Guarantee a recovery time objective (RTO) and recovery point objective (RPO) of 4 hours RTO and 1 hour RPO, unless otherwise specified by the Iowa Judicial Branch.

T. **Subcontractor Management**.
T.1. Ensure all subcontractors comply with the same security requirements as the primary vendor, including ICDPA obligations for data processors.
T.2. Provide a list of all subcontractors that will handle Iowa Judicial Branch data, including their roles and security certifications.
T.3. Notify the Iowa Judicial Branch in advance of any changes to subcontractor arrangements.

U. **Documentation and Reporting**.
U.1. Upon request, provide detailed documentation of all security policies, procedures, and controls.
U.2. Upon request, provide quarterly security compliance reports, including metrics on vulnerabilities, incidents, and access control reviews.
U.3. Upon request, participate in regular security review meetings with Iowa Judicial Branch representatives.

V. **Consumer Data Rights (ICDPA Compliance, if applicable)**.
V.1. Provide Iowa residents with the right to access, delete, and obtain a copy of their personal data, and to opt out of the sale of personal data or targeted advertising, as required by ICDPA Section 4.
V.2. Respond to consumer data requests within 90 days, with a possible 45-day extension, as stipulated by ICDPA.
V.3. Provide a clear and conspicuous privacy notice detailing categories of personal data processed, purposes, third-party sharing, and consumer rights, as required by ICDPA Section 4(6).
V.4. For data concerning known children, comply with the federal Children's Online Privacy Protection Act (COPPA) and obtain parental consent, as required by ICDPA.

W. **Termination and Data Return**.
W.1. Upon contract termination, return or securely destroy all Iowa Judicial Branch data in accordance with state requirements and ICDPA consumer deletion rights.
W.2. Provide a certificate of data destruction, if applicable, within 30 days of contract termination.
W.3. Ensure no Iowa Judicial Branch data is retained by the vendor or subcontractors after contract termination.

X. **Technical Support.**
X.1. Selected vendor must provide assistance during normal business hours (8AM to 5 PM, M-F, Central Time, excluding holidays) via telephone and email.
X.2. High priority issues (i.e. multiple participants cannot respond to surveys) are to be resolved within 24 hours.

X.3. Selected vendor will work with JCS to cooperatively identify any RMS that need to be re-entered because of technical issues and to have those entries re-submitted so the overall count meets federal reimbursement requirements.

X.4. Normal priority issues (i.e. new, changed, or deleted users; changes to questions or permissible responses) are to be resolved within 3 working days.

X.5. Low priority requests (i.e. requests for screen color, font, format changes; requests for estimates of new features) are to be evaluated, have requirements gathered by the selected vendor, and replied to in writing to JCS within 2 weeks.

X.6. If JCS approves updates as quoted, a due date for implementation of that change will be negotiated within 5 working days. The due date will be chosen within 5 days, but the actual implementation date will depend on the work to be completed.

Y. **Training.** The selected vendor must:

Y.1. Supply written documentation, with screen shots, and step-by-step instructions for all functionality for participant users, including, but not limited to the following functions, beginning at the point a user opens an email request for RMS.

Y.1.1. Identify the sender of the email.

Y.1.2. Identify the subject line to expect.

Y.1.3. Specify the link URL:

- How to assess whether the email & link are legitimate.
- Clues within the email, a seal or logo, domain of the URL.

Y.1.4. How to recognize the RMS site and confirm it is legitimate.

Y.1.5. In cooperation with JCS, identify what tasks are included in each program and activity and which response to use in common work situations.

Y.1.6. How to operate the tool to make selections.

Y.1.7. How to enter free text, and appropriate subject matter for same.

Y.1.8. How to submit an RMS and verify that it was accepted into the database.

Y.1.9. Exiting the RMS application.

Y.1.10. Returning to work after responding to a survey:

- If a survey is missed or unaccepted
- Business consequences of not responding (reimbursement, policy).
- Reminder email.
- Time period for making a response.

Y.2. Supply written documentation, with screen shots, and step-by-step instructions for all functionality for administrator roles, including, but not limited to the following functions:

Y.2.1. Read, create, edit, and delete participants.

Y.2.2. Read, and create quarterly data reports.

Y.2.3. View RMS requests and submissions, including monitoring participant responses and free-text comments.

Y.2.4. Create, edit, and delete participant lists.

Y.2.5. Update schedules for participants.

Y.2.6. Create, and edit, questions and responses.

Y.2.7. Generate reports.

Y.3. Ensure all objectives listed in Section 2 of this RFQ are covered in both the written instruction, as well as the online trainings.

Y.4. Include other topics selected vendor knows from experience should be documented and available for participants.

Y.5. Ensure that all written training materials are accessible online and downloadable in PDF format.

Y.6. Provide initial training via virtual platform. The Respondent must provide a detailed training plan. To ensure consistent application, the Respondent must maintain and make available upon request, all training documentation including training participant lists.

Y.6.1. Respondent must provide virtual training or live webinar for participant users, and separate virtual training or live webinar for administrator users of RMS system:

- Training must include how participants can differentiate between eligible and
- ineligible administrative activities.
- Respondent will note any business or policy related questions during training, and forward to JCS staff for responses.
- Participants must have opportunity to test-drive the application in a test environment during or soon after initial training.
- Virtual training shall cover the same topics listed for the written documentation (listed above).
- Live training shall be offered within 6 weeks of contract signing.

Y.7. Provide training videos, to be stored and made available to JCS on-demand.

Y.7.1. Acceptable on-demand training video will include narration, graphics, and/or slides of all the same information listed for written documentation, contain a section of FAQs.

Y.8. Assess ongoing training needs, including identifying common errors and develop and provide, or assist with development of virtual training to correct errors identified.

Y.9. Work with JCS staff to provide a minimum of annual training for participants, and other JCS users as needed.

Z. **Ongoing User Support.** The selected vendor must:

Z.1. Respond to questions from users regarding use of the RMS tool.

Z.2. Resolve user's requests within 24 hours.

Z.3. Refer caller to Title IV-E Program Manager within the IJB for questions regarding policy or practice within 24 hours.

AA. **System Configuration/Set up.** The selected vendor must:

AA.1. Ensure demonstration is available within 3 weeks after signing of contract.

AA.2. Demonstration to include all users registered, email generator working, specified selection of responses available and properly recorded, sample reports generated and able to be saved to JCS-designated storage location.

AA.3. Resolve issues found during the pilot/demo within 2 weeks, when a second demo is to be performed.

AA.4. Ensure RMS solution is production-ready, and fully functional within 6 weeks of contract signing.

AA.5. Create separate, secure database for JCS within 3 weeks after signing of contract.

AA.6. Set up and maintain users, with JCS input.

AA.6.1. Initial user set up within 3 weeks after signing of contract.

AA.6.2. New user set up and ongoing maintenance/updates of user accounts will occur within 48 hours of request from JCS.

AA.7. Assure secure authentication is achieved without user login to website.

BB. **Mandatory Compliance Requirement – Transition Assistance and Data Ownership.**

Mandatory Requirement. Vendors shall comply with all requirements set forth below. Failure to meet or affirm compliance with this requirement shall render the Vendor non-responsive and ineligible for contract award.

BB.1. Transition Assistance Obligation. Upon expiration or termination of the Contract for any reason, or upon written notice from the Client of transition to a successor vendor, the Vendor shall provide all transition assistance necessary to ensure an orderly, timely, and uninterrupted transfer of the Random Moment Sampling (RMS) system.

BB.2. Required Transition Deliverables. At a minimum, the Vendor shall:

- Provide prompt delivery of all Client data, including historical and current RMS data, in an industry-standard, machine-readable format;
- Transfer all system documentation, technical specifications, procedures, and other materials reasonably necessary to support continued operation or transition of the RMS system; and
- Cooperate fully and in good faith with the Iowa Judicial Branch and, if applicable, any successor vendor to effectuate a complete and efficient transition.

BB.3. Data Ownership and Access. All RMS data are and shall remain the sole and exclusive property of the Iowa Judicial Branch. Under no circumstances shall the Vendor withhold, restrict, delay, encrypt, or condition access to Iowa Judicial Branch data, including in connection with payment disputes, contract termination, or transition activities.

BB.4. Non-Interference. The Vendor shall not take any action or fail to take any action that interferes with, delays, or otherwise impedes the transition of the RMS system or Iowa Judicial Branch data.

BB.5. Survival. The obligations in this Mandatory Compliance Requirement shall survive the expiration or termination of the Contract for any reason and shall remain enforceable until transition is fully completed to the Client's satisfaction.

CC. **Total Cost of Service.** Respondent must provide a cost proposal detailing the following on the Vendor Response Form posted with this RFQ:

CC.1. Initial (one-time costs) for this product.

CC.2. Additional, itemized costs for specified requirements, including, but not limited to:

CC.2.1. Consultation and implementation (including training) fees.

CC.2.2. Maintenance and/or upgrade costs.

CC.2.3. System Setup fees.

CC.2.4. Annual subscription or renewal fee for the product.

CC.2.5. Per hour Consultation fees.

CC.2.6. Any additional applicable fees, itemized.

DD. **Proposal Requirements.**

- Vendors must submit a detailed response to each requirement, including:
  - Confirmation of compliance or a plan to achieve compliance.
  - Descriptions of tools, processes, or methodologies used to meet the requirement.
  - Evidence of certifications, audit reports, or other supporting documentation.
  - **Vendor Security Questionnaire**. If not previously provided to the Iowa Judicial Branch through a procurement process, the Successful Contractor shall provide a fully completed copy of the Vendor Security Questionnaire (VSQ).

- Vendor Certification (Required) By submission of a response to this RFQ, the Vendor certifies mandatory compliance with all requirements set forth in this section without exception, limitation, or qualification.

- Failure to address any requirement may result in disqualification from the evaluation process.

4. TIMELINE

Monday, May 11, 2026	Issuance of RFQ
Friday, May, 22, 2026	Questions due
Friday, May 29, 2026	Answers to Questions posted
Friday, June 19, 2026	Due Date for Quotes

Vendors may submit written questions regarding this RFQ and the procurement process to the Issuing Officer. Answers to questions received will be posted at: https://www.iowacourts.gov/for-the-public/rfp/

Vendors shall submit quotes via email to the Issuing Officer no later than 3:00 PM CST on DATE. Any quote received after this deadline will not be considered.

5. PERIOD OF VALIDITY OF QUOTES STARTING ON THE SUBMISSION DATE

60 Days

6. TERMS AND CONDITIONS

By submitting a response to this RFQ, the parties agree to comply with the terms and conditions found at the following links, which are, by this reference, made a part of any Agreement based on this solicitation:
https://www.iowacourts.gov/static/media/cms/General_TermsIJB_Services_Contracts_FAA0F7505A5D5.pdf

7. RESTRICTION ON COMMUNICATION

If a Vendor or someone acting on a Vendor's behalf attempts to discuss this RFQ orally or in writing with any members of the IJB, any employee of the State of Iowa, or anyone other than the named Issuing Officer, then the Vendor may be disqualified.

8. ADDITIONAL INFORMATION

The costs of preparation and delivery in response to this RFQ are solely the responsibility of the Vendor.

IJB reserves the right to reject any or all submitted responses, in whole or in part, to advertise a new RFQ, to abandon the need for such RFQ, and to cancel this RFQ opportunity at any time prior to the execution of a written contract.

All information submitted by a Vendor may be treated as a public record by the IJB.

By submitting a response, a Vendor agrees that it will not bring any claim or have any cause of action against IJB or the State of Iowa based on any misunderstanding concerning the information provided within this RFQ or concerning the IJB or the State of Iowa's failure, negligent or otherwise, to provide the Vendor with pertinent information as intended by this RFQ.

If the apparent successful Vendor fails to negotiate and deliver an executed contract within a reasonable period of time following selection, then the IJB may, in its sole discretion, cancel the award and award the contract to the next highest ranked Vendor.
The IJB shall have the sole option to amend the contract resulting from this RFQ for subsequent periods, by executing a signed amendment prior to the expiration of the original contract.