STATE OF TENNESSEE
TENNESSEE BUREAU OF INVESTIGATION

REQUEST FOR INFORMATION
FOR
CLOUD-HOSTED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM SOLUTION

RFI # 34800-081126
08/18/2026

1. STATEMENT OF PURPOSE:

The State of Tennessee, Tennessee Bureau of Investigation issues this Request for Information ("RFI") for the purpose of gathering information and industry feedback regarding the acquisition, cloud hosting, migration, and ongoing maintenance of a comprehensive Automated Fingerprint Identification System (AFIS) that meets stringent FBI Criminal Justice Information Services security mandates and high-performance throughput requirements. We appreciate your input and participation in this process.

2. BACKGROUND:

The State of Tennessee is seeking information regarding modernization, secure cloud-hosting, and ongoing maintenance and support for an Automated Fingerprint Identification System (AFIS). The objective of this initiative is to replace the current AFIS with a scalable, highly available cloud-hosted environment that supports rigorous production and testing workflows while seamlessly integrating with the other State systems.

The scope encompasses comprehensive cloud provisioning, dynamic resource scaling, robust disaster recovery capabilities, and strict adherence to federal and state security mandates, including the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and Electronic Biometric Transmission Specification (EBTS) standards. Additionally, the project involves the large-scale migration and synchronization of legacy AFIS containing millions of records, the digitization and indexing of unindexed hard-copy fingerprint cards, and the deployment of fully compatible hardware, workstations, and peripherals.

Vendors are invited to provide insights, technical approaches, and industry best practices regarding cloud architecture design, seamless data migration methodologies, high-performance transaction throughput, and long-term system maintenance. Feedback gathered through this Request for Information will assist the State in refining its technical specifications, evaluating market capabilities, and structuring a competitive procurement strategy.

3. COMMUNICATIONS:

3.1. Please submit your response to this RFI to:

AFISRFI@tbi.tn.gov

3.2. Please feel free to contact the Tennessee Bureau of Investigation with any questions regarding this RFI. The main point of contact will be:
AFISRFI@tbi.tn.gov

3.3. Please reference RFI # 34800-081126 with all communications to this RFI.

4. RFI SCHEDULE OF EVENTS:

EVENT		TIME (Central Time Zone)	Date (all dates are State business days)
1.	RFI Issued		08/18/2026
2.	RFI Response Deadline		09/02/2026

5. GENERAL INFORMATION:

5.1. Please note that responding to this RFI is not a prerequisite for responding to any future solicitations related to this project and a response to this RFI will not create any contract rights. Responses to this RFI will become property of the State.

5.2. The information gathered during this RFI is part of an ongoing procurement. In order to prevent an unfair advantage among potential respondents, the RFI responses will not be available until after the completion of evaluation of any responses, proposals, or bids resulting from a Request for Qualifications, Request for Proposals, Invitation to Bid or other procurement methods. In the event that the state chooses not to go further in the procurement process and responses are never evaluated, the responses to the procurement, including the responses to the RFI, will be considered confidential by the State.

5.3. The State will not pay for any costs associated with responding to this RFI.

6. INFORMATIONAL FORMS:

The State is requesting the following information from all interested parties. Please fill out the following forms:

RFI #34800-081126 TECHNICAL INFORMATIONAL FORM
1. RESPONDENT LEGAL ENTITY NAME:
2. RESPONDENT CONTACT PERSON: Name, Title: Address: Phone Number: Email:
3. BRIEF DESCRIPTION OF EXPERIENCE PROVIDING SIMILAR SCOPE OF SERVICES/PRODUCTS
4. Describe your approach and architectural design for AFIS provisioning, configuring, and maintaining a scalable cloud-hosted solution, storage, and networking resources dedicated to production and testing environments, and explain how you will establish these segregated environments.
5. Explain your methodology for implementing dynamic resource scaling across all hosted cloud infrastructure layers to accommodate annual capacity growth without degrading application performance, throughput, or availability metrics. It is estimated that the AFIS data grows at around 7% per year.
6. Describe your process and timeline for producing comprehensive technical documentation of the cloud architecture, configuration settings, and provisioning procedures, including the submission of the architecture package within ninety calendar days of Contract execution.
7. Detail your plan for delivering and installing new hardware, turn-key capture and latent workstations, and required peripherals such as batch scanners and printers, and explain how you ensure full operational compatibility with the cloud-based AFIS and Windows operating system environments (matching or exceeding Windows 10 baseline).
8. Describe how you will provide and manage all necessary software licenses and third-party software, including how you test and verify updates and patches to maintain uninterrupted CJIS and EBTS compliance prior to deployment.
9. Detail your approach for developing and submitting a High Availability and Disaster Recovery Plan within sixty calendar days of receiving a Notice to Proceed, including failover protocols, data replication mechanisms, and recovery point objectives.
10. Describe the architecture and operational mechanisms of your automated cloud-based disaster recovery environment, detailing how it meets a Recovery Time Objective of four hours and a Recovery Point Objective of zero data loss during an unplanned outage.
11. Describe your procedures for conducting semi-annual disaster recovery failover and failback simulations, including how you validate system resilience and data integrity and deliver post-test performance reports within fifteen calendar days.
12. Explain your comprehensive strategy for executing a seamless migration of the current AFIS database comprising over five million records, ensuring the preservation of historical data, palm responses, and mugshot transmission, while adhering strictly to FBI CJIS Security Policy and EBTS standards.

13. Describe your methodology for performing database synchronization, backing up legacy databases, securely transferring them, and executing a residual migration following Go-Live to capture remaining records.
14. Detail your process for scanning, indexing, and converting approximately two hundred fifty thousand unindexed hard-copy fingerprint cards, and explain how you will ensure data integrity and full searchability within criminal and applicant workflows.
15. Describe how you will provide technical assistance for auditing the data migration process and detail your plan for submitting a data migration and conversion execution plan within sixty calendar days of execution of Contract.
16. Describe your 24/7 operational monitoring protocols for the hosted environment to ensure immediate detection of performance degradation, security anomalies, or infrastructure failures.
17. Explain your approach for maintaining compliance CJIS Security Policy and other state and federal requirements, including data encryption standards for stored and transmitted biometric information implemented within sixty calendar days of Contract execution.
18. Describe how you will implement and enforce multi-factor authentication and role-based access controls and detail the security access policy to be submitted within thirty calendar days of contract execution.
19. Detail your procedures for conducting periodic vulnerability assessments and compliance audits of the cloud environment, including your process for delivering formal remediation reports within fifteen business days of identifying a finding.
20. Describe how your solution supports all required system workflows—including criminal livescan, hard copy criminal card entry, TAPS, law enforcement applicant livescan, DNA collection, mobile submissions, sex offender registry, and Rap Back subscription and notification services—in compliance with FBI EBTS standards.
21. Provide your technical specifications and capabilities for daily search capacity and throughput—specifically for Ten Print to Ten Print, Ten Print to Unsolved Latent, and Latent fingerprint to Ten Print searches—and explain how you will scale capacity by at least five percent annually.
22. Describe how the AFIS enables the State to view, request, and print multiple FBI NGI Ten Print and Palm Print cards on a single subject, access and retrieve records from FBI databases, maintain separate forward and reverse latent search queues for submitting agencies, and perform manual record modifications.
23. Detail your incident management and operational protocols for maintaining at least 99.9% system availability per calendar month, including response times within fifteen minutes and restoration within two hours for critical severity incidents during unplanned outages.
24. Describe your preventive maintenance, system patching, and administrative update procedures, including how you schedule and obtain written approval for maintenance windows and submit change management plans at least fourteen calendar days prior to non-emergency modifications.
25. Detail your tiered technical support services, dedicated help desk availability for state administrators, severity-based escalation timeframes, and your process for delivering root-cause analysis reports within five business days of resolving a critical incident.
26. Describe your cost proposal breakdown structure for initial search costs and average daily throughput pricing across all specified search categories, to be submitted within sixty calendar days of receiving a Notice to Proceed.

27. Explain how you will configure and utilize State-owned network circuits within sixty calendar days of receiving a Notice to Proceed, including your coordination and approval process for circuit adjustments and third-party connectivity modifications.
28. Describe your approach for establishing and maintaining secure data tunnels, integration interfaces, and data exchanges with third-party AFIS vendors and external state systems such as the Computerized Criminal History, message switch, TBI mugshots to NGI, and FBI IRQ/IRR palm responses.
29. Detail your collaborative planning process for introducing new external systems or modifying existing network touchpoints, including the submission of an interface integration and testing plan within forty-five calendar days of project initiation while ensuring zero degradation of interface throughput.
30. Describe how your solution achieves transparent integration with designated third-party systems and workstations through standardized APIs and secure communication protocols in accordance with applicable state administrative rules.
31. Describe your strategy for delivering ongoing technology updates, platform patches, and software version upgrades to ensure alignment with emerging biometric identification standards, including the annual submission of a technology roadmap update.
32. Detail your approach for providing a comprehensive system integration and lifecycle management plan within thirty calendar days of receiving a Notice to Proceed, covering testing, validation, and deployment procedures for third-party workstation modifications.
33. Explain the security controls, audit logging mechanisms, and system hardening procedures you will implement within the cloud-hosted AFIS environment to monitor access, data transmission, and system modifications in accordance with CJIS mandates, and detail the security compliance report to be submitted within sixty calendar days of NTP.
34. Describe the architecture and operational management of the dedicated test environment separate from production, detailing how it enables the State to validate software updates, configuration changes, and integrations in compliance with FBI CJIS security requirements.
35. Describe your internal pre-delivery testing protocols and ongoing system performance and data integrity checks utilized during data migration to guarantee zero record loss.
36. Explain the tools and reporting mechanisms you will provide to support ongoing system auditing protocols for periodic checks of database synchronization, search accuracy, and workflow execution throughout the contract term.
37. Detail how you will ensure continuous access to the latest deployed version of AFIS technology, software licensing, updates, patches, and third-party software necessary for system efficiency throughout the contract term.
38. Describe your ongoing technical support and maintenance service delivery model, detailing how you maintain system availability and resolve technical issues in accordance with service level agreements and FBI CJIS standards.
39. Describe how the AFIS will be configured to accept and populate drop-down menus for criminal offenses originating from incoming livescan submissions.
40. Describe your training plan and methodology for delivering in-person training to system users and administrators for the new AFIS environment.

COST INFORMATIONAL FORM
1. Describe what pricing units you typically utilize for similar services or goods (e.g., per hour, each, etc.:
2. Describe the typical price range for similar services or goods
3. Provide a detailed cost proposal itemizing the resources, configuration, maintenance, and dynamic scaling fees associated with provisioning and managing the dedicated cloud compute, storage, and networking environments for production and testing workflows.
4. Provide pricing details for delivering and installing all necessary new hardware, turn-key capture and latent workstations, required batch scanners, printers, software licenses including any third-party software, including ongoing costs for maintaining Windows compatibility across operating system versions.
5. Detail the costs for developing, implementing, and maintaining the automated cloud-based disaster recovery environment, including failover mechanisms, data replication, and the execution of semi-annual disaster recovery simulations and post-test reporting.
6. Submit a comprehensive cost breakdown for executing the complete legacy database migration of over five million records, system interface development, network circuit configuration, third-party connectivity, and residual migration activities following Go-Live.
7. Provide itemized pricing for scanning, indexing, and converting approximately two hundred fifty thousand (250,000) unindexed hard-copy fingerprint cards into searchable records within the AFIS workflows.
8. Provide cost information associated with the ongoing twenty-four-seven (24/7) operational monitoring, security compliance mandates, multi-factor authentication implementation, role-based access controls, and periodic vulnerability assessments and remediation reporting.
9. Detail the pricing model for supporting all required system workflows, including criminal livescan, hard copy criminal card entry, TAPS, applicant livescan, DNA collection, handheld device submissions, sex offender registry, and Rap Back subscription and notification services.
10. Submit a detailed cost proposal itemizing initial search costs and average daily throughput pricing across all required search categories, including Ten Print to Ten Print, Ten Print to Unsolved Latent, Palm Print to Unsolved Latent Palm Print, Latent fingerprint to Ten Print, Latent Palm Print to Palm Print, Latent Palm Print to Unsolved Palm Print, and Latent fingerprint to Unsolved Latent fingerprint, along with pricing adjustments for annual capacity growth.
11. Provide cost details for configuring and utilizing State-owned network circuits, establishing secure data tunnels and integration interfaces with third-party vendors and external systems such as CCH and the message switch, and maintaining interface throughput during system expansions.
12. Detail the pricing for delivering ongoing technology updates, platform patches, software version upgrades, annual technology roadmap updates, tiered technical support services, dedicated help desk availability, and the resolution of technical support tickets based on severity escalation timeframes.
13. Provide cost information for conducting in-person training for state personnel on the new Automated Fingerprint Identification System.

ADDITIONAL CONSIDERATIONS

1. Please provide input on alternative approaches or additional things to consider that might benefit the State: