REQUEST FOR PROPOSALS
FOR

Telephone System and Support Services

Issued by:
New Jersey Higher Education Student Assistance Authority

Date Issued:

May 20, 2026

Question Cut-off Date:

June 1, 2026

Proposals Due:

June 22, 2026

Jerry Traino
Acting Executive Director
Chief Financial Officer

Higher Education Student Assistance Authority
4 Quakerbridge Plaza
P.O. Box 545
Trenton, New Jersey 08625

Contact:
Marnie Grodman, Esq.
Director, Legal & Governmental Affairs

Table of Contents

1.0 PURPOSE AND INTENT

The New Jersey Higher Education Student Assistance Authority ("HESAA" or the "Authority") is a public body corporate and politic, which is "in but not of" the State of New Jersey, Department of State and is an instrumentality of the State. The Authority is seeking proposals from vendors for a Unified Communications as a Service (UCaaS), and Contact Center as a Service (CCaaS), cloud-based enterprise platforms with integrated quality management/recording (QM) and workforce management (WFM) capabilities, plus ongoing managed services.

The solution must be scalable, secure, resilient, accessible by adhering to the Web Content Accessibility Guidelines 2.1 AA, and interoperable with HESAA's existing security stack, including Cisco Firepower and Umbrella and identity provider, Microsoft Entra ID/Azure AD SSO with multi-factor authentication (MFA). The platform shall support open standards, including but not limited to: Secure Session Initiation Protocol (SIP) that uses Transport Layer Security (TLS) to encrypt and secure SIP; Secure Real-Time Transport Protocol (SRTP); Application Programming Interface conforming to Representational State Transfer (REST APIs); webhooks; Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) for single sign-on; and deliver high availability with documented disaster recovery.

HESAA is seeking a Cisco-based or comparable platform, involving an integrated suite of hardware and software that manages enterprise-level communications, including voice, video, and data security. Any proposed solution must meet the capability, security, accessibility, and integration requirements in this RFP.

2.0 DEFINITIONS

The following definitions will be part of any contract awarded as a result of this RFP.

Addendum or Addenda – Written clarification or revision to this RFP issued by HESAA.

Agent Assist – Real-time guidance to human agents (e.g., suggested responses, next-best actions, and knowledge lookups).

AI (Artificial Intelligence) – Software that performs tasks requiring human-like perception, understanding, prediction, or decision support (e.g., ASR, NLU/NLP, and LLMs).

Amendment – A change in the scope of services to be provided by the Contractor. An amendment is not effective until it is signed by the Authority.

API (Application Programming Interface) – A set of protocols and tools that allow different software applications to communicate with each other.

ASR (Automatic Speech Recognition) – A technology that converts speech to text.

BHCA (Busy Hour Call Attempts) – The total number of call attempts made during the single busiest hour in a full twenty-four-hour day.

Bidder – An individual or business entity that submits a proposal in response to this RFP.

Business Day – Any weekday, excluding Saturdays, Sundays, State legal holidays, and State-mandated closings unless otherwise indicated.

Call Paths – The maximum number of concurrent call sessions supported on trunks/carrier services (e.g., SIP) typically governing simultaneous inbound and outbound calls.

CCaaS (Contact Center as a Service) – A cloud-based solution providing software for managing customer communications while offering scalability, cost-efficiency, and integration of automation and AI.

Configuration Change – Any alteration made to hardware, software, network, (including moves, adds, changes, and decommissions) to maintain or improve its functionality and security.

Configuration Management – The process that tracks and controls how system configuration items are modified over time to ensure a stable, secure, and consistent environment.

Contract – This RFP, addenda to this RFP, the HESAA Standard Terms and Conditions, the Contractor's proposal submitted in response to this RFP (including any best and final offer), contractual language agreed to by the Contractor and HESAA governing the implementation of the services to be provided, and HESAA's Notice of Intent to Award.

Contractor – The bidder awarded a contract resulting from this RFP.

DID (Direct Inward Dial) – A telephone number that allows callers to reach a specific person or endpoint without going through the automated menu.

DR Regions (Disaster Recovery Regions) – Geographically separate regions used for disaster recovery (DR), where a secondary site can take over operations if the primary site fails.

E-Fax Account – An account that enables sending and receiving electronic faxes, typically through email or a hosted service.

E911 – Emergency calling compliance, including Kari's Law, 47 U.S.C. § 623, and the RAY BAUM'S Act, also known as the (Repack Airwaves Yielding Better Access for Users of Modern Services Act of 2018).

Entitlements – The set of privileges/features granted to a user based on their license or subscription.

Evaluation Committee – A group of individuals assigned by the Authority to review and evaluate proposals submitted in response to this RFP and recommend a Contract award to the HESAA Board.

Firm Fixed Price – A price that is all-inclusive of direct cost and indirect costs, including but not limited to, direct labor costs, counsel fees, overhead, fee or profit, clerical support, equipment, materials, supplies, managerial (administrative) support, all documents, reports, forms, travel,

reproduction, and any other costs. No additional fees or costs shall be paid by the Authority unless there is a change in the scope of services.

GenAI (Generative AI) – Models that generate text or other content (e.g., summaries, draft responses) from prompts and context.

IVR (Interactive Voice Response) – An automated telephony system that allows callers to interact with a computer system through voice or keypad inputs.

IVR Port – A capacity resource that allows a single caller to interact with an automated IVR session (menus, data collection, queueing) prior to transfer to a live agent.

Joint Venture – A business undertaking by two or more entities to share risk and responsibility for a specific project.

KPI (Key Performance Indicator) – A quantifiable measure used to track progress toward specific business objectives.

May – Denotes that which is permissible, not mandatory.

MFA (Multi-Factor Authentication) – A security method requiring at least two verification factors to enable log-in.

NLP (Natural Language Processing) – A field of artificial intelligence that enables computers to understand, interpret, and generate human language.

NLU (Natural Language Understanding) – A subfield of artificial intelligence that focuses on a computer's ability to comprehend the actual meaning, intent, and context behind human language.

OAuth 2.0 – An open standard for authorization that allows a third-party application to access a user's data on another service without the user needing to share the password.

OIDC (OpenID Connect) – An authentication layer built on top of the OAuth 2.0 authorization protocol that enables single sign-on.

Patch/Firmware Updates – Upgrades to a system or device's underlying software to fix bugs, improve performance, enhance security, and add new features.

PII (Personally Identifiable Information) – As defined by the State information security manual (https://www.nj.gov/it/docs/ps/2021-Statewide_Information_Security_Manual.pdf) any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PII Redaction – Automated removal or masking of PII from transcripts, audio, or text.

Project – The services and deliverables that are the subject of this RFP.

PSTN (Public Switched Telephone Network) – The public telephony network that connects calls through carrier infrastructure.

RFP (Request for Proposal) – This document which establishes the bidding and contract requirements, and solicits proposals to meet the needs of the Authority.

RBAC (Role-Based Access Control) – A security method limiting system access based upon a user's role within a company or organization, which is used instead of granting individual permissions.

REST (Representational State Transfer) – An architectural style in designing networked applications that utilizes the World Wide Web.

RPO (Recovery Point Objective) – The maximum acceptable data loss that an organization can manage following a disrupting event.

RTO (Recovery Time Objective) – The maximum acceptable amount of downtime for an application or system following a disrupting event.

SAML (Security Assertion Markup Language) – An open standard for exchanging authentication and authorization data between an identity provider and a service provider using XML-based assertions.

Shall or Must – Denotes that which is a requirement. Failure to meet a material requirement will result in the rejection of a proposal as non-responsive.

Should – Denotes that which is recommended, not mandatory.

SIP (Session Initiation Protocol) – A signaling protocol used for initiating, maintaining, modifying, and terminating communication sessions that involve multimedia elements such as voice, video, and messaging.

SIP Trunks – A virtual connection using the SIP and the internet to provide voice and multimedia communication.

SLA (Service Level Agreement) – A contract term defining the level of service expected from the provider, including metrics for measuring performance, and applicable remedies.

SMS (Short Message Service) – The standard technology for sending text-only messages of up to 160 characters between mobile phones using a cellular network.

SOC 2 Type II – An independent controls attestation report covering the design and operating effectiveness of controls over a defined period.

SRTP – Secure Real-time Transport Protocol, which is a protocol that secures data like voice and video calls in real-time by providing authentication, confidentiality, and replay protection.

SSO – Single Sign-On (SAML 2.0 or OIDC).

State – State of New Jersey.

Subtask – A detailed activity comprising part of the performance of a task.

Subcontractor – An entity having an arrangement with a Contractor, whereby the Contractor uses the products and/or services of that entity to fulfill some of its obligations under its contract with the Authority, while the Contractor retains full responsibility for the performance of all of its obligations under the contract, including payment to the subcontractor. The subcontractor has no legal relationship with the Authority, only with the Contractor.

Task – A discrete unit of work to be performed.

TLS (Transport Layer Security) – A cryptographic protocol that provides end-to-end security for data transferred over networks.

UCaaS (Unified Communications as a Service) – A cloud-based platform integrating communication tools for an operating business into a single usable interface.

Virtual Agent / Bot – An automated conversational interface (voice or chat) that handles interactions using NLU/NLP and scripted/business rules.

Voice over Internet Protocol (VoIP) – Technology that converts voice signals into digital signals, and back to voice, as needed to communicate over the IP networks or regular telephone systems.

WFM (Workforce Management System) – A system that forecasts demand, schedule agents, and monitors performance to ensure appropriate staffing to meet service goals.

WCAG 2.1 AA (Web Content Accessibility Guidelines) – A set of international standards to make digital content accessible to people with disabilities.

Zero-Data Retention – A processing mode in which the provider does not retain prompts, outputs, audio, or derived data for model training or product improvement.

3.0 BACKGROUND

As part of its mission of administering student financial aid and loan programs for the State, HESAA supports a call center that fields approximately three-hundred phone calls each day with seasonal surges. On these calls students and families provide HESAA with PII. The HESAA security stack includes Cisco Firepower and Umbrella; therefore, the proposed solution must integrate with this stack and meet the requirements of the Statewide Information Security Manual: https://www.nj.gov/it/docs/ps/2021-Statewide_Information_Security_Manual.pdf

4.0 SCOPE OF SERVICES

The Authority is seeking a Unified Communications as a Service (UCaaS), a cloud-based enterprise, and Contact Center as a Service (CCaaS) platform with integrated quality management/recording (QM) and workforce management (WFM) capabilities, plus ongoing managed services to include 24/7 system monitoring, incident detection, providing end-user support and troubleshooting services, and monthly KPI reporting.

The solution must be a Cisco-based or comparable platform. The solution must also be scalable, secure, resilient, accessible by adhering to the Web Content Accessibility Guidelines 2.1 AA, and interoperable with HESAA's existing security stack, including Cisco Firepower and Umbrella and identity provider, Microsoft Entra ID/Azure AD SSO with multi-factor authentication (MFA). The platform shall support open standards, including but not limited to: Secure Session Initiation Protocol (SIP) that uses Transport Layer Security (TLS) to encrypt and secure SIP; Secure Real-Time Transport Protocol (SRTP); Application Programming Interface conforming to Representational State Transfer (REST APIs); webhooks; and Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) for single sign-on; and deliver high availability with documented disaster recovery.

As such, the proposed platform must include all of the following:

4.1 System Requirements: Core UCaaS Requirements

The UCaaS shall include and/or be capable to support the following:

A. **Licenses/Seats**: Up to 250 manned users (mix of softphone, desktop, and meeting features), scalable +/- 25% at contracted unit rates.

B. **Endpoints**: Support standards-based SIP desk, shared area, and conference phones for Windows/Mac/iOS/Android soft clients with feature parity, including but not limited to busy lamp, sidecars, and power over Ethernet.

C. **Public Switched Telephone Network/Carrier Services**: Provide SIP trunks and cloud calling with at least:
    1. 35 concurrent Call Paths based on Busy Hour Call Attempts (BHCA) and seasonal peaks.
    2. 1 Toll Free Number.
    3. 10 E-Fax Accounts.
    4. 175 Direct Inward Dials (DIDs).

D. **E911 Compliance:** Compliance with Kari's Law and RAY BAUM's Act (see 47 CFR, Ch. I, Subch. A, Pt. 9, Subpt. F) for fixed and nomadic users; dispatchable location; testing and validation prior to cutover.

E. **Standards & Interop**: SIP over TLS and SRTP; REST APIs and webhooks; calendaring and presence; voicemail-to-email; hunt groups; auto attendants.

4.2 System Requirements: Contact Center as a Service (CCaaS)

The CCaaS shall include and/or be capable to support the following:

A. **Seats**: 75 named users (20 supervisors and 55 standard agents), scalable.
B. **Core Features**: Skills-based routing; queue and agent key performance indicators (KPIs); real-time and historical dashboards; callback in queue; overflow; silent, whisper and barge monitoring features; and post-call surveys.
C. **Omnichannel**: Voice required; email, chat, and short message service (SMS) options listed as separately priced line items.
D. **Interactive Voice Response (IVR)**: Custom menu builder with API data integration, dual input (voice and dual tone multi-frequency), automated scheduling, and exportable call flows.
E. **Accessibility**: WCAG 2.1 AA for supervisor and agent Uis; screen-reader and keyboard navigation; relay compatibility.

4.3 Quality Management (QM), Call Recording and Workforce Management (WFM)

The Contractor shall manage the capacity and performance of the UCaaS and CCaaS platform and supporting infrastructure via the implementation of processes and controls necessary to protect against avoidable impacts to operations.

A. **Call recording**: Up to 100 users (or policy-based all-call) with pause and resume (PII protection), encryption at rest, searchable metadata, export in open format.
B. **Unified Review**: Single interface to review UCaaS & CCaaS recordings with Role-Based Access Control (RBAC).
C. **Retention**: Configurable retention 7 years, options up to 10+ with legal hold.
D. **WFM**: Forecasting, scheduling, adherence, exception management; import and export of schedules; supervisor tools.

4.4 Security, Privacy & Compliance

The Contractor shall implement administrative, technical, and physical controls necessary to safeguard information technology assets from threats to their confidentiality, integrity, and/or availability, whether internal or external, deliberate or accidental. The Contractor shall develop and implement processes to ensure its compliance with all statutory, regulatory, contractual, and internal policy obligations applicable to this Contract.

At a minimum the system must include the following:

A. **Encryption**: TLS 1.2+ in transit; SRTP for media; encryption at rest for recordings and configurations.
B. **Identity:** Single sign-on (SSO) via SAML 2.0 and OIDC to Microsoft Entra ID; MFA enforced per HESAA policy.
C. **Audit & Logging**: Immutable logs; 365-day online search; archive options up to 7 years.
D. **Attestations:** Annual SOC 2 Type II (or ISO 27001 equivalent) report; vulnerability management and penetration testing attestation.
E. **Data Residency:** U.S. data centers; disclose primary and disaster recovery (DR) regions.

F. **State Requirements:** Alignment with the Statewide Information Security Manual and HESAA Privacy Policy; adherence to PL 2005, c.92 (U.S. performance) and other statutes listed in §5.4.
G. **Data Ownership & Training** – HESAA retains ownership of all audio, transcripts, metadata, prompts, and outputs, system logs, usage data, analytics, configurations, derivatives, and any other data or information obtained, generated, processed, stored or created in connection with HESAA's use of the system. There shall be no model training, tuning, product improvement, benchmarking, or other use of HESAA data without HESAA's explicit, written opt-in via a separate agreement.
H. **Zero-Retention Mode** – AI components must support a zero-data-retention processing option; any temporary caches must be encrypted and purged per agreed schedules.
I. **Sub-processors & Residency** – Identify all Artificial Intelligence (AI), Automatic Speech Recognition (ASR), and Natural Language Processing (NLP) sub-processors and model providers; all processing and storage must occur within the U.S. unless HESAA approves otherwise in writing.
J. **Ability to be Explained & Auditability** – Provide reason codes or source citations for AI recommendations; maintain tamper-evident logs of prompts, context injected, outputs, and user actions.
K. **Accessibility & Notices** – Any AI-generated content shown to users or agents must meet WCAG 2.1 AA. If transcription or AI is in use, call opening and IVR messages must include required recording and transcription disclosures.
L. **Risk Management** – Document controls for bias, toxicity, prompt injection, data leakage, and hallucination. The Contractor shall provide a model update and change-control process and rollback plan.

4.5 Availability, DR, and Service Level Agreements (SLAs)

The Contractor shall develop, implement, test, and maintain a contingency plan to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the Contractor.

A. **Service Availability: Minimum 99.95% uptime per monthly per major service (UCaaS, CCaaS).**
B. **Incident SLAs (24×7):**
   - P1 (service outage and critical impact): Acknowledge ≤ 15 min; restore ≤ 4 hrs.
   - P2 (degraded/major feature loss): Acknowledge ≤ 30 min; restore ≤ 8 hrs.
   - P3 (minor issue): Acknowledge ≤ 4 hrs; restore per plan.
   - Include service credits schedule and chronic failure remedies.
C. **DR**: Recovery Time Objective (RTO) ≤ 4 hrs., Recovery Point Objective (RPO) ≤ 15 min; semiannual failover test report.
D. **ASR Accuracy Reporting** – Quarterly report of ASR accuracy (e.g., Word Error Rate (WER) on agreed sample sets), language coverage, and redaction miss rates.
E. **Virtual Agent KPIs** – Containment rate, escalation rate, correct-answer rate, average handle time impact; monthly review and tuning plan.
F. **Agent Assist KPIs** – Adoption rate, suggestion acceptance rate, and measured impact on handle-time or first-contact resolution (where applicable).

(Service credits shall remain tied to uptime/incident SLAs; AI KPI shortfalls drive tuning plans, not credits.)

4.6 Managed Services

The Contractor shall comply with the following system service standards. The Contractor shall be responsible for preparing reports each month and providing them to the HESAA Contract Manager. All monthly reports shall be made available at the end of the reporting period within 30 calendar days.

A. **Time and Services**: 24 hours a day, 7 days a week monitoring, incident management, problem and configuration management, proactive patching with change windows and rollback plans.
B. **Monthly Reports**: Tickets by priority, SLA performance, capacity and usage, security patches; quarterly business reviews with KPIs and roadmap.

4.7 Professional Services (Implementation)

A. **Discovery and detailed design:** Number porting; IVR design; test plans; user acceptance testing; go-live hyper-care; as-built documentation; administrator run-books.
B. **Training and Adoption**: Role-based training for administrators, supervisors, agents, and end users; accessible materials (WCAG 2.1 AA).

4.8 Acceptance Measurements

A. **Criteria:** Successful execution of cutover plan; E911 validation; pass and fail of test scripts; KPI baselines.
B. **Time:** 30-day stabilization and hyper-care; remediation of Severity 1 and Severity 2 defects.
C. **Pilot:** Run a limited AI pilot (e.g., ASR + summarization or virtual agent on defined intents) with agreed success criteria (quality thresholds, escalation behavior, user satisfaction). Proceed to scale only upon written acceptance.

4.9 Scalability & Growth

The Contractor shall submit for approval, via written request to the HESAA Contract Manager, new services/features to keep pace with technology and changes in the communications and relay services industry. The Contractor shall propose any of these new services/features which have come into standard availability after contract award that are enhancements to existing services or networks. If a nexus to an existing contract item cannot be made, the request will be denied.

A. **Ability to scale:** Licenses, call paths, channels seasonally; clear overage/burst pricing.
B. **Future integrations:** Via documented APIs.
C. **Requests for integration of new services/features:** Such written requests shall include the following items:
   i. Description of the proposed method or technology;
   ii. Adherence to service level and standards of service described in this RFP;
   iii. Outreach plan with budget requirements;
   iv. Implementation plan, with deployment dates;
   v. Statement of impact on currently offered services; and
   vi. Cost.

5.0 Data Security Requirements – Contractor Responsibility

5.1 Security Plan

The Contractor shall submit a detailed Security Plan that addresses the Contractor's approach to meeting each applicable security requirement outlined below, to the Authority, no later than thirty (30) calendar days after the award of the Contract. The Authority's approval of the Security Plan shall be set forth in writing. In the event that HESAA reasonably rejects the Security Plan after providing the Contractor an opportunity to cure, the Director may terminate the Contract pursuant to the SSTC.

5.2 Information Security Program Management

A. The Contractor shall establish and maintain comprehensive information security strategies aligned with industry-recognized frameworks, including but not limited to: NIST CSF, or ISO 27001, and consistent with the Statewide Information Security Manual. AI-enabled components are subject to the data governance, auditability, residency, and zero-retention requirements in Section 4.4.

5.3 Compliance

The Contractor shall develop and implement processes to ensure its compliance with all statutory, regulatory, contractual, and internal policy obligations applicable to this Contract. Examples include but are not limited to General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), IRS-1075. Contractor shall timely update its processes as applicable standards evolve.

A. Within ten (10) Calendar Days after award, the Contractor shall provide the Authority with contact information for the individual or individuals responsible for maintaining a control framework that captures statutory, regulatory, contractual, and policy requirements relevant to the organization's programs of work and information systems;
B. Throughout the solution development process, Contractor shall implement processes to ensure security assessments of information systems are conducted for all significant development and/or acquisitions, prior to information systems being placed into production; and
C. The Contractor shall also conduct periodic reviews of its information systems on a defined frequency for compliance with statutory, regulatory, and contractual requirements. The Contractor shall document the results of any such reviews.

5.4 Privacy and Data Protection

If there is State Data associated with the Contract, this section is applicable.

A. *Data Ownership.* The State owns State Data. Contractor shall not obtain any right, title, or interest in any State Data, or information derived from or based on State Data.
B. Data usage, storage, and protection of Personal Data are subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for HIPAA, Tax Information Security

Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, N.J.S.A. § 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:11-44 et. seq., the federal Drivers' Privacy Protection Act of 1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. § 39:2-3.4. Contractor shall also conform to PCI DSS, where applicable.

C. *Security:* Contractor agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information. Contractor shall ensure that State Data is secured and encrypted during transmission or at rest.

D. *Data Transmission:* The Contractor shall only transmit or exchange State Data with other parties when expressly requested in writing and permitted by and in accordance with requirements of the Contract or the State of New Jersey. The Contractor shall only transmit or exchange State Data with the State of New Jersey or other parties through secure means supported by current technologies.

E. *Data Storage:* All data provided by the State of New Jersey or State data obtained by the Contractor in the performance of the Contract must be stored, processed, and maintained solely in accordance with a project plan and system topology approved by the State Contract Manager. No State data shall be processed on or transferred to any device or storage medium including portable media, smart devices and/or USB devices, unless that device or storage medium has been approved in advance in writing by the State Contract Manager. The Contractor must not store or transfer State of New Jersey data outside of the United States.

F. *Data Re-Use:* All State Data shall be used expressly and solely for the purposes enumerated in the Contract Data shall not be distributed, repurposed or shared across other applications, environments, or business units of the Contractor. No State Data shall be transmitted, exchanged or otherwise passed to other contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by the State Contract Manager.

G. *Data Breach:* In the event of any actual, probable or reasonably suspected Breach of Security, or any unauthorized access to or acquisition, use, loss, destruction, compromise, alteration or disclosure of any Personal Data, Contractor shall: (a) immediately notify the State of such Breach of Security, but in no event later than 24 hours after learning of such security breach; (b) designate a single individual employed by Contractor who shall be available to the State 24 hours per day, seven (7) days per week as a contact regarding Contractor's obligations under Bid Solicitation Section 6.34 - Incident Response; (c) not provide any other notification or provide any disclosure to the public regarding such Breach of Security without the prior written consent of the State, unless required to provide such notification or to make such disclosure pursuant to any applicable law, regulation, rule, order, court order, judgment, decree, ordinance, mandate or other request or requirement now or hereafter in effect, of any applicable governmental authority or law enforcement agency in any jurisdiction worldwide (in which case Contractor shall consult with the State and reasonably cooperate with the State to prevent any notification or disclosure concerning any Personal Data or Breach of Security); (d) assist the State in investigating, remedying and taking any other action the State deems necessary regarding any Breach of Security breach and any dispute, inquiry, or claim that concerns the Breach of Security; (e) follow all instructions provided by the State relating to the Personal Data affected or potentially affected by the Breach of

Security; (f) take such actions as necessary to prevent future Breaches of Security; and (g) unless prohibited by an applicable statute or court order, notify the State of any third party legal process relating to any Breach of Security including, at a minimum, any legal process initiated by any governmental entity (foreign or domestic).

H. *Minimum Necessary.* Contractor shall ensure that State Data requested represents the minimum necessary information for the services as described in this Bid Solicitation and, unless otherwise agreed to in writing by the State, that only necessary individuals or entities who are familiar with and bound by the Contract will have access to the State Data in order to perform the work.

I. *End of Contract Data Handling:* Upon termination/expiration of this Contract the Contractor shall first return all State Data to the State in a usable format as defined in the Contract, or in an open standards machine-readable format if not. The Contractor shall then erase, destroy, and render unreadable all Contractor backup copies of State Data according to the standards enumerated in accordance with the State's most recent Media Protection policy, https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf, and certify in writing that these actions have been completed within 30 days after the termination/expiration of the Contract or within seven (7) days of the request of an agent of the State whichever should come first.

J. In the event of loss of any State Data or records where such loss is due to the intentional act, omission, or negligence of the Contractor or any of its subcontractors or agents, the Contractor shall be responsible for recreating such lost data in the manner and on the schedule set by the State Contract Manager. The Contractor shall ensure that all State Data is backed up and is recoverable by the Contractor. In accordance with prevailing federal or state law or regulations, the Contractor shall report the loss of State data.

5.5 Encryption

The Contractor shall employ cryptographic safeguards to protect sensitive information in transmission, in use, and at rest, from a loss of confidentiality, unauthorized access, or disclosure. Cryptographic protections shall include at a minimum:

A. Using industry standard encryption algorithms;
B. Establishing requirements for encryption of data in transit;
C. Establishing requirements for encryption of data at rest; and
D. Implementing cryptographic key management processes and controls.

5.6 Remote Access

The Contractor shall strictly control remote access to the Contractor's internal networks, systems, applications, and services. Appropriate authorizations and technical security controls shall be implemented prior to remote access being established. Remote access controls shall include at a minimum:

A. Establishing centralized management of the Contractor's remote access infrastructure;
B. Implementing technical security controls (e.g. encryption, multi-factor authentication, IP whitelisting, geo-fencing); and
C. Training users in regard to information security risks and best practices related remote access use.

In the event the Contractor shall be approved to utilize State-provided remote access connectivity to conduct work on systems, networks, and data repositories managed and hosted within the New Jersey Garden State Network (GSN) for State approved business, the Contractor shall collaborate with the State in accordance with State defined usage restrictions, configuration/connection requirements, and implementation guidance for remote access into the GSN.

5.7 Cloud Security

The Contractor shall establish security requirements that govern the use of private, public, and hybrid cloud environments to ensure risks associated with a potential loss of confidentiality, integrity, availability, and privacy are managed. This shall ensure, at a minimum, the following:

A. Security is accounted for in the acquisition and development of cloud services;
B. The design, configuration, and implementation of cloud-based applications, infrastructure and system-system interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations;
C. Security roles and responsibilities for the Contractor and the cloud provider are delineated and documented; and
D. Controls necessary to protect sensitive data in public cloud environments are implemented.

5.8 Contingency Planning

The Contractor shall develop, implement, test, and maintain a contingency plan to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the Contractor. The plan shall address the following:

A. Backup and recovery strategies;
B. Continuity of operations;
C. Disaster recovery; and
D. Crisis management.

5.9 Incident Response

The Contractor shall maintain an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities shall include, at a minimum, the following:

A. Information security incident reporting awareness;
B. Incident response planning and handling;
C. Establishment of an incident response team;
D. Cybersecurity insurance;
E. Contracts with external incident response services specialists; and
F. Contacts with law enforcement cybersecurity units.

6.0 REQUIRED COMPONENTS OF THE PROPOSAL

6.1 General Information

Please include information relating to your organization, personnel, and experience, including, but not limited to, references, together with contact names and telephone numbers, illustrating your organization's qualifications and capabilities to perform the services required by this Bid Solicitation. The Bidder's answers should include the level of detail necessary to assist the Evaluation Committee in its review of your organization's proposal.

Please provide **complete but concise** answers to the following questions:

(a) Provide a summary, listing any background information, on your company that you believe is relevant, including but not limited to number of years of UCaaS/CCaaS and managed cybersecurity experience and services, to be provided.

(b) Provide the following information for the people in your company with whom HESAA will be dealing:

Name
Phone number and email address
Title & Responsibility
Total Years of Experience

Please indicate which person will have ultimate responsibility for this contract.

(c) Provide three references that currently use your services, including name of the organization and a contact's name and title, telephone number, and email address. HESAA may contact references to evaluate their experiences with the bidder.

(d) Consideration will be given to minority-owned and women-owned companies, and to companies owned by disabled veterans. Provide any information about your company relevant to these considerations.

(e) Provide any additional information you feel uniquely qualifies your company for this contract.

6.2 Services and Approach

Please set forth the Bidder's overall technical approach and plans to meet the requirements of the Bid Solicitation in a narrative format. This narrative should demonstrate to the Evaluation Committee that your organization understands the objectives that the Contract is intended to meet, the nature of the required work, and the level of effort necessary to successfully complete the Contract. The narrative should demonstrate that the Bidder's approach and plans to undertake and complete the Contract are appropriate to the tasks and subtasks involved.

Mere reiterations of Bid Solicitation tasks and subtasks are strongly discouraged, as they do not provide insight into the Bidder's approach to complete the Contract. The response to this section should demonstrate to the Evaluation Committee that the Bidder's detailed plans and approach proposed to complete the Scope of Work are realistic, attainable and appropriate, and that the Quote will lead to successful Contract completion.

(a) Indicate how your company performs 24/7 incident monitoring and describe its problem-resolution approach, including tools, an escalation matrix, and a sample monthly report.

(b) Indicate how your company handles configuration and change management, including reactive firmware and patch policy, backup of device configurations, and restore frequency. Include a sample run-book Table of Contents.

(c) Describe your approach to onboarding and training. Include a sample curricula and job aids.

(d) Provide a security program summary, including SOC 2 Type II (or equivalent) letter, data residency, and E911 compliance controls.

(e) Capacity planning: Provide BHCA assumptions, call path sizing, and a seasonal surge strategy.

(f) AI Architecture and Governance – Describe models/services used (ASR/NLU/LLM), zero-retention modes, redaction pipeline, RBAC, tenant isolation, and audit logging.

(g) Responsible AI – Describe your bias testing, hallucination safeguards, jailbreak/PII-exfiltration defenses, and abuse filters.

(h) Tuning & Change Control – Describe your approach to knowledge updates, prompt/policy changes, and how model version upgrades are tested, approved, and rolled back.

(i) Measurement Plan – Describe your proposed KPIs (see Section 4.5), baselining method, and cadence for improvement.

(j) AI – Describe the AI enabled features currently available or under development that improve service quality, accessibility, and efficiency including, but not limited to, speech-to-text transcription, real-time agent assist, intent detection, predictive forecasting, automated quality scoring, conversation summarization, virtual agents for voice and chat. Confirm that all AI features meet the data governance and security requirements in this RFP, are auditable, support human oversight, and will not use HESAA data for model training.

Specifically, if applicable, describe your current and/or forthcoming AI features that specifically address the following:

i. Speech Analytics & Transcription

1. Real-time and post-call ASR with configurable PII redaction before storage.
2. Exportable transcripts (open format) with timestamps and confidence scores.

3. Vendor shall disclose baseline accuracy (e.g., word-error rate) for EN-US and any additional languages proposed, and provide a process to monitor and improve accuracy over time.

ii. Agent Assist

1. Real-time suggestions (knowledge snippets, next-best actions, policy reminders) with source citations from an approved HESAA knowledge base.
2. Human override at all times; content must be logged, attributable, and reviewable.
3. No content may be shown to callers directly by Agent Assist.

iii. Automated Quality Management

1. Auto-scoring against configurable rubrics (compliance statements, empathy, disclosure scripts, call handling).
2. Side-by-side human QA override and calibration reports (correlation between auto-scores and human scores).

iv. Virtual Agents and Bots

1. Voice and/or chat bots for front-door triage, status checks, FAQs; mandatory, immediate failover to live agents on errors, escalation requests, or E911-related triggers.
2. Clear guardrails: topic boundaries, profanity filters, hallucination mitigation, and answer containment metrics.
3. Integrations via APIs to HESAA systems (read-only unless otherwise authorized).

v. Summarization & Notetaking

1. Post-interaction summaries that can be pushed to ticketing/Customer Relationship Management (CRM), with attribution and confidence; never a substitute for official records unless approved.
2. Automated quality scoring and coaching.
3. AI-assisted forecasting and schedule optimization.

6.3 Additional Terms

A Contractor may submit additional terms as part of its Proposal. Additional terms are Bidder proposed terms or conditions that do not conflict with the scope of work required in this RFP, the terms and conditions of this RFP, or the HESAA Standard Terms and Conditions. Bidder proposed terms or conditions that conflict with those contained in the HESAA Standard Terms and Conditions will render a Proposal non-responsive. It is incumbent upon the Bidder to identify and remove its conflicting proposed terms and conditions prior to Proposal submission.

6.4 Fees

Prices submitted are to be firm for the term of the contract. Bidders shall submit their fees using the Fee Schedule attached hereto as Exhibit A, Pricing Matrix. All methods of pricing that differ from the pre-established methods listed in Exhibit A should be clearly identified for each priced item.

6.5 Additional Information

The selected firm will need to register with ***NJSTART***. If your firm is already registered with ***NJSTART***, please provide your contractor ID number.

Bidders should provide the following information, forms, and certifications with their Quote:

A. A copy of a valid New Jersey Business Registration must be submitted by the selected firm. To facilitate proposal evaluation and contract award process, the bidder shall submit the Business Registration form with the proposal. If not already registered with the New Jersey Division of Revenue, registration can be completed online at the Division of Revenue website: https://nj.gov/treasury/revenue/gettingregistered.shtml.

B. Pursuant to Public Law 2005, Chapter 51 ("Chapter 51"), to avoid any appearance that the selection of State Contractors is based on the Contractors' political contributions, State departments, agencies and authorities are precluded from awarding contracts exceeding $17,500 to contractors who make, or have made, certain political contributions on and after October 15, 2004. Chapter 51 also requires the disclosure of all contributions to any political organization organized under 26 U.S.C. 527 that also meets the definition of a continuing political committee within the meaning of N.J.S.A. 19:44A-3(n) and N.J.A.C. 19:25-1.7. Bidders shall submit the required certification form(s) and disclosure form(s) with their proposals. Failure to submit such forms and/or failure of such forms to evidence compliance with Chapter 51 shall be cause for rejection of a bidder's proposal. Any bidder selected shall maintain compliance with Chapter 51 during the term of its engagement. The disclosure form can be found at: https://nj.gov/treasury/purchase/forms.shtml

C. Pursuant to Public Law, 2005 Chapter 271 (Chapter 271) firms must disclose their (and their principals') political contributions within the immediately preceding twelve (12) month period. No prospective firm will be precluded from being awarded a contract by virtue of the information provided in the Chapter 271 disclosure provided the form is fully and accurately completed. Prior to formal appointment the firm anticipated to be selected will be required to submit Chapter 271 disclosures. To facilitate proposal evaluation and contract award process, the contractor shall submit the Chapter 271 disclosure with the proposal. The disclosure form can be found at: https://nj.gov/treasury/purchase/forms.shtml

Please also be advised of your responsibility to file an annual disclosure statement on political contributions with the New Jersey Election Law Enforcement Commission (ELEC), pursuant to N.J.S.A. 19:44A-20.13 if your firm receives contracts in excess of $50,000 from a public entity during a calendar year. It is your firm's responsibility to determine if filing is necessary. Failure to file can result in the imposition of financing penalties by ELEC. Additional information about this requirement is available from ELEC at (888) 313-3532 or https://www.elec.state.nj.us/

D. In accordance with N.J.S.A. 52:34-13.2 (Public Law 2005, Chapter 92), all services performed pursuant to this engagement shall be performed within the United States of America.

E. Pursuant to Public Law 1995, Chapter 159, effective January 1, 1998, and notwithstanding the provision of any other law to the contrary, whenever any taxpayer, partnership or S corporation under contract to provide goods or services or construction projects to the State of New Jersey or its agencies or instrumentalities, including the legislative and judicial branches of State government, is entitled to payment for those goods or services at the same time a taxpayer, partner or shareholder of that entity is indebted for any State tax, the Director of the Division of Taxation shall seek to set off so much of that payment as shall be necessary to satisfy the indebtedness. The amount set-off shall not allow for the deduction of any expense or other deduction which might be attributable to the taxpayer, partner, or shareholder subject to set-off under this Act.

   The Director of the Division of Taxation shall give notice of the set-off to the taxpayer, partner or shareholder and provide an opportunity for a hearing within thirty (30) days of such notice under the procedures for protests established under N.J.S.A. 54:49-19. No request for conference, protest, or subsequent appeal to the Tax Court from any protest shall stay the collection of the indebtedness.

F. A copy of a Disclosure of Investigations and Other Actions Involving the Contractor Form must be submitted by all bidders. The certification can be found at: https://nj.gov/treasury/purchase/forms.shtml.

G. Pursuant to N.J.S.A. 52:32-58, the bidder must certify that neither the bidder, nor one of its parents, subsidiaries, and/or affiliates (as defined in N.J.S.A. 52:32-56(e)(3)), is listed on the Department of the Treasury's List of Persons or Entities Engaging in Prohibited Investment Activities in Iran and that neither is involved in any of the investment activities set forth in N.J.S.A. 52:32-56(f). If the bidder is unable to so certify, the bidder shall provide a detailed and precise description of such activities.

H. Pursuant to P.L.2022, c. 3, a person or entity seeking to enter into or renew a contract for the provision of goods or services shall certify that it is not Engaging in Prohibited Activities in Russia or Belarus as defined by P.L.2002, c. 3, sec. 1(e). The certification form is available at: https://nj.gov/treasury/purchase/forms.shtml.

I. Prior to award, the intended Contractor and its named Subcontractor(s) must submit a copy of a New Jersey Certificate of Employee Information Report, or a copy of Federal Letter of Approval verifying it is operating under a federally approved or sanctioned Affirmative Action program. If the Contractor and/or its named Subcontractor(s) are not in possession of either a New Jersey Certificate of Employee Information Report or a Federal Letter of Approval, it/they must complete and submit the Affirmative Action Employee Information Report (AA-302). Information, instruction and the application are available at https://www.state.nj.us/treasury/contract_compliance/index.shtml.

J. In accordance with N.J.S.A. 52:25-24.2, in the event the Bidder is a corporation, partnership or limited liability company, the Bidder must disclose all 10% or greater owners by (a)

completing and submitting the Ownership Disclosure Form with the Quote; (b) if the Bidder has submitted a signed and accurate Ownership Disclosure Form dated and received no more than six (6) months prior to the Quote submission deadline for this procurement, the Division may rely upon that form; however, if there has been a change in ownership within the last six (6) months, a new Ownership Disclosure Form must be completed, signed and submitted with the Quote; or, (c) a Bidder with any direct or indirect parent entity which is publicly traded may submit the name and address of each publicly traded entity and the name and address of each person that holds a 10 percent or greater beneficial interest in the publicly traded entity as of the last annual filing with the federal Securities and Exchange Commission or the foreign equivalent, and, if there is any person that holds a 10 percent or greater beneficial interest, also shall submit links to the websites containing the last annual filings with the federal Securities and Exchange Commission or the foreign equivalent and the relevant page numbers of the filings that contain the information on each person that holds a 10 percent or greater beneficial interest. N.J.S.A. 52:25-24.2. A Bidder's failure to submit the information required by N.J.S.A. 52:25-24.2 will result in the rejection of the Quote as non-responsive and preclude the award of a Contract to said Bidder.

K. Pursuant to N.J.S.A. 52:34-12.2, the Contractor must certify that it either has no ongoing business activities in Northern Ireland and does not maintain a physical presence therein or that it will take lawful steps in good faith to conduct any business operations it has in Northern Ireland in accordance with the MacBride principles of nondiscrimination in employment as set forth in N.J.S.A. 52:18A-89.5 and in conformance with the United Kingdom's Fair Employment (Northern Ireland) Act of 1989, and permit independent monitoring of their compliance with those principles.

L. The Terms and Conditions set forth in the "HESAA Terms & Conditions" are incorporated into any contract resulting from this RFP. The HESAA Terms & Conditions can be found on the HESAA website at:
https://www.hesaa.org/Documents/Procurements_TermsandConditions.pdf

7.0 PROPOSAL SUBMISSION

7.1 Delivery

Proposals must be emailed to Procurements@hesaa.org by the 4:00 pm deadline on June 22, 2026. Please type "Telephone System and Support Services" in the subject line.

7.2 Questions and Addendums

HESAA will accept questions pertaining to this RFP from all potential bidders electronically. Questions shall be directed to Procurements@hesaa.org.

Questions will be accepted until 4:00 pm on June 1, 2026. In the event that it becomes necessary to clarify or revise this RFP, such clarifications or revisions will be by Addendum. Any Addendum to this RFP will become part of this RFP and part of any contract entered as a result of this RFP.

The Authority also reserves the right to distribute additional background information or material to all bidding firms.

All RFP Addenda will be posted on the HESAA website. It is the sole responsibility of the bidder to be knowledgeable of all addenda related to this RFP.

7.3 Cost liability

HESAA will not be responsible for any expenses in the preparation and/or presentation of the proposals and oral interviews, if any, or for the disclosure of any information or material received in connection with the solicitation, whether by negligence or otherwise.

8.0 SPECIAL TERMS & CONDITIONS

8.1 Term

The contract entered as a result of this RFP will be for a three-year term.

HESAA will have the option to extend the contract for two (2) two-year periods, or any portion thereof, if deemed in its best interests to do so.

8.2 Termination

Unless otherwise provided herein, HESAA reserves the right to terminate any agreement entered into as a result of this RFP provided written notice has been given to the Contractor at least thirty days prior to such proposed termination date. The Contractor may terminate the contract upon sixty days' notice to the Authority. In the event a new Contractor is selected, the prior Contractor shall facilitate transfer of all necessary information, including databases, files, and other information needed for the continued operation of the application, to the new Contractor, and otherwise cooperate with HESAA and the new Contractor to effectuate an orderly transition. The old Contractor shall provide this information to the new Contractor no later than thirty days after contract termination.

8.3 Transition

In the event the services are scheduled to end either by contract expiration or by termination, it shall be incumbent upon the firm to continue the service, if requested by HESAA, until new services can be completely operational. At no time shall this transitional period extend more than 180 days beyond the expiration date of the existing contract. The firm will be reimbursed for this service at the rate in effect when this transitional period clause is invoked by HESAA.

8.4 Contract

The Contract awarded, and the entire agreement between the parties, as a result of this Bid Solicitation shall consist of: (1) the final Bid Solicitation, (2) Higher Education Student Assistance Authority Standard Terms and Conditions (3) the Quote, and if applicable, (4) any Bidder responses to clarifications, (5) a Bidder's Best and Final Offer, (6) other negotiated document, and/or (7) third party document. In the event of a conflict in the terms and conditions among the documents comprising this Contract, the order of precedence, for purposes of interpretation thereof, shall be as listed from highest ranking to lowest ranking as noted above.

Any other terms or conditions, not included with the Bidder's Quote and accepted by HESAA, shall not be incorporated into the Contract awarded. Any references to external documentation, including those documents referenced by a URL, including without limitation, technical reference manuals, technical support policies, copyright notices, additional license terms, etc., are subject to the terms and conditions of the Bid Solicitation and the Higher Education Student Assistance Authority Standard Terms and Conditions. In the event of any conflict between the terms of a document incorporated by reference, the terms and conditions of the Bid Solicitation and the Higher Education Student Assistance Authority Standard Terms and Conditions shall prevail.

In the event that it becomes necessary to revise, modify, clarify or otherwise alter the contract resulting from the RFP, amendments will be in writing signed by an authorized representative of HESAA and the Contractor.

Any statistics or values shown in the RFP are either based on past history or best estimates and are not a guarantee of future volumes and trends. The future quantities, values or activities may be more or less than those noted herein and could change during the course of the contract term. HESAA will make no allowances or concessions to a bidder for any alleged misunderstanding because of quantity, character or other conditions.

8.5 Open Public Records Act

Pursuant to the New Jersey Open Public Records Act (OPRA), N.J.S.A. 47:1A-1 et seq., or the common law right to know, all documents submitted in response to this RFP are subject to disclosure by HESAA as "government records" in accordance with N.J.A.C. 17:12-1.2(b) and (c).

Contractor should submit a completed and signed Confidentiality/Commitment to Defend Form with the proposal. In the event that Contractor does not submit the Confidentiality form with the proposal, HESAA reserves the right to request that the Contractor submit the form after proposal submission. The Confidentiality/Commitment to Defend Form can be found at: ConfidentialityForm.pdf (nj.gov).

After the opening of the proposals, all information submitted by a Contractor in response to this RFP is considered public information notwithstanding any disclaimers to the contrary submitted by a Contractor. Proprietary, financial, security, and confidential information may be exempt from public disclosure by OPRA and/or the common law when the Contractor has a good faith legal or factual basis for such assertion.

When the RFP contains a negotiation component, the proposal will not be subject to public disclosure until a notice of intent to award a Contract is announced.

As part of its proposal, a Contractor may request that portions of the proposal be exempt from public disclosure under OPRA and/or the common law. Contractor must provide a detailed statement clearly identifying those sections of the proposal that it claims are exempt from production, and the legal and factual basis that supports said exemption(s) as a matter of law. The State will not honor any attempts by a Contractor to designate its price sheet, price list/catalog, and/or the entire proposal as proprietary and/or confidential, and/or to claim copyright protection for its entire proposal. If HESAA does not agree with a Contractor's designation of

proprietary and/or confidential information, HESAA will use commercially reasonable efforts to advise the Contractor. Copyright law does not prohibit access to a record which is otherwise available under OPRA.

In order not to delay consideration of the proposal or HESAA's response to a request for documents, HESAA requires that Contractor respond to any request regarding confidentiality markings within the timeframe designated in HESAA's correspondence regarding confidentiality. If no response is received by the designated date and time, HESAA will be permitted to release a copy of the proposal with HESAA making the determination regarding what may be proprietary or confidential.

HESAA reserves the right to make the determination as to what to disclose in response to an OPRA request. Any information that HESAA determines to be exempt from disclosure under OPRA will be redacted.

In the event of any challenge to the Contractor's assertion of confidentiality that is contrary to HESAA's determination of confidentiality, the Contractor shall be solely responsible for defending its designation, and in doing so, all costs and expenses associated therewith shall be the responsibility of the Contractor. HESAA assumes no such responsibility or liability.

8.6 Price Alteration

Proposal prices must be typed or written in ink. Any price change (including "white-outs") must be initialed. Failure to initial price changes shall preclude a contract award from being made to the bidder.

8.7 Proposal Errors

A bidder may request that its proposal be withdrawn prior to the proposal submission opening. Such request must be made, in writing, to Procurements@hesaa.org. If the request is granted, the bidder may submit a revised proposal as long as the proposal is received prior to the announced date and time for proposal submission and at the place specified.

If, after the proposal submission opening but before contract award, a bidder discovers an error in its proposal, the bidder may make a written request to Marnie Grodman for authorization to withdraw its proposal from consideration for award. Evidence of the bidder's good faith in making this request shall be used in making the determination. The factors that will be considered are that the mistake is so significant that to enforce the contract resulting from the proposal would be unconscionable; that the mistake relates to a material feature of the contract; that the mistake occurred notwithstanding the bidder's exercise of reasonable care; and that HESAA or the State will not be significantly prejudiced by granting the withdrawal of the proposal. After the proposal submission opening, while pursuant to the provisions of this section, a bidder may request to withdraw its proposal and HESAA may, in its discretion, allow the bidder to withdraw it; HESAA also may take notice of repeated or unusual requests to withdraw by a bidder and take those prior requests to withdraw into consideration when evaluating the bidder's proposals.

All requests to withdraw a proposal must identify the RFP, "Telephone System and Support Services," include the final proposal submission date, and be sent to Procurements@hesaa.org.

If during a proposal evaluation process, an obvious pricing error made by a potential contract awardee is found, HESAA shall issue a written notice to the bidder. The bidder will have three days after receipt of the notice to confirm its pricing. If the bidder fails to respond, its proposal shall be considered withdrawn, and no further consideration shall be given it.

If it is discovered that there is an arithmetic disparity between the unit price and the total extended price, the unit price shall prevail. If there is any other ambiguity in the pricing other than a disparity between the unit price and the extended price and the bidder's intention is not readily discernible from other parts of the proposal, HESAA may seek clarification from the bidder to ascertain the true intent of the proposal.

8.8 Joint Venture

If a joint venture submits a proposal, the agreement between the parties relating to such joint venture should be submitted with the joint venture's proposal. Authorized signatories from each party comprising the joint venture must sign the proposal. Each party to a joint venture must submit a separate Ownership Disclosure Form, Disclosure of Investigations and Actions Involving Bidder form, Disclosure of Investment Activities in Iran form, and Affirmative Action Employee Information Report. Each party comprising the joint venture must also possess a valid Business Registration Certificate issued by the Department of the Treasury, Division of Revenue prior to the award of a contract. Refer to Section 5.4 of this RFP.

8.9 Prime Contractor Responsibilities

The selected Contractor, **and any successor Contractor**, (in the event of merger/acquisition or other change in operating status), will be required to assume sole responsibility for the complete effort of any contract(s) awarded to the Contractor subsequent to its bid submission, and assume all cost incurred by HESAA, directly or indirectly, in connection with or as a result of the transition. If a merger/acquisition has been announced prior to or during the Contractor's proposal preparation period, the bidder shall identify all relevant or emerging dates surrounding the merger relative to official name change, system changes, account number changes, etc., if known at the time of bid submission.

HESAA will consider the prime Contractor to be the sole point of contact with regard to contractual matters. The prime Contractor is responsible for the professional quality, technical accuracy, and timely completion of all services awarded to the Contractor as a result of this solicitation, and will, without additional compensation, correct or revise any errors, omissions, or other deficiencies in their products, services, reports, equipment, information, etc. in order to meet the requirements as specified herein. The successful Contractor will furnish the names of the officers and management personnel who will be utilized in the fulfillment of any agreement resulting from this request.

8.10 Subcontracting and Assignment

All subcontractors must be approved by HESAA. If the Contractor has knowledge prior to the proposal submission date that any part of the work covered by this request will be subcontracted,

the Contractor must identify the subcontracting organization, its officers, and the contractual arrangements made therewith, and state what services are to be subcontracted.

If, during the contract term, the Contractor desires to employ or replace any subcontractor, the Contractor must provide ninety days written notice to HESAA. HESAA will evaluate the replacement firm's qualifications. No replacement firm shall begin work without prior HESAA approval.

The prime Contractor is totally responsible for adherence by the subcontractor to all provisions of the contract between the Contractor and HESAA. Nothing contained in these specifications or subsequent specifications shall be construed as creating any contractual responsibility between the subcontractor(s) and HESAA.

The Contractor is prohibited from assigning, transferring, conveying, subletting, or otherwise disposing of this agreement or its rights, title, or interest therein or its power to execute such agreement to any other person, company, or corporation without the previous consent and approval, in writing, by HESAA. Unless otherwise agreed to in writing by HESAA, the assignee shall bear all cost incurred by the Authority, directly or indirectly, in connection with or as a result of such an assignment.

8.11 Security and Confidentiality

A. DATA CONFIDENTIALITY

All data contained in the source documents supplied by the Authority are to be considered confidential and shall be solely for the use of the Authority. The Contractor shall establish and maintain a framework to provide assurance that information security strategies are aligned with and support the State's business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, in an effort to manage risk. The Contractor will be required to use reasonable care to protect the confidentiality of the data. Any use, sale or offering of this data in any form by the Contractor, or his/her employees or assignees will be considered in violation of this contract and will cause the infraction to be reported to the State Attorney General for possible prosecution. Penalties for violations of such guarantees will include, but are not limited to, cancellation of the contract and/or legal action with no damages paid by the Authority or the State of New Jersey.

All financial, statistical, personnel, customer, and/or technical data supplied by HESAA to the Contractor are confidential. The Contractor must secure all data from manipulation, sabotage, theft, or breach of confidentiality. The Contractor is prohibited from releasing any financial, statistical, personnel, customer, and/or technical data that is deemed confidential. The following shall not be considered confidential information and shall not be subject to the provisions of this section 7.11. Any information that (a) was in Contractor's possession before receipt from a data owner; (b) is independently developed or acquired by or for Contractor without use of a data owner's proprietary information; (c) is rightfully received by Contractor from a third party without a duty of confidentiality; (d) was disclosed by a data owner to a third party not under an obligation of confidentiality; or (e) is or becomes available to the public through no fault of Contractor. Contractor will not release any confidential information to a third party without the consent of the data owner unless required to do so in order to comply with judicial or administrative process.

Prior to releasing a data owner's confidential information in response to judicial process, the Contractor shall give the data owner advanced written notice of the subpoena, if not legally prohibited, and provide the data owner the opportunity to object to the required disclosure. Any other use, sale, or offering of this data to a third party without the data owner's consent in any form by the Contractor, or any individual or entity in the Contractor's charge or employ, will be considered a violation of this contract and may result in contract termination and the Contractor's suspension or debarment from State contracting. In addition, such conduct may be reported to the State Attorney General for possible criminal prosecution. The Contractor shall be liable to HESAA for a breach of confidentiality subject to the insurance requirements set forth in this RFP.

The Contractor shall assume total financial liability incurred by the Contractor associated with any breach of confidentiality.

When requested, the Contractor and all project staff, including its subcontractor(s), must complete and sign confidentiality and non-disclosure agreements provided by HESAA. The Contractor shall require all staff to view yearly security awareness and confidentiality training modules provided by the Contractor. It shall be the Contractor's responsibility to ensure that any new staff sign the confidentiality agreement and complete the security awareness and confidentiality training modules within one month of the employee's start date.

To protect the State of New Jersey from losses resulting from Contractor employee theft, fraud or dishonesty, security clearance/background check for all Contractors and project staff must be obtained and provided to HESAA upon request. Refer to the National Institute of Standards and Technology (NIST) Special Publication (SP) 300-12, An Introduction to Computer Security: The NIST Handbook, Section 10.1.3, Filling the Position – Screening and Selecting.

B. SECURITY STANDARDS

The Bidder should complete and submit the HESAA Security Due Diligence Third-Party Information Security Questionnaire https://he7606.hesaa.org/Documents/RFPs/Fillable%20PDF%20NJ-Third-Party-Information-Security-Questionnaire.pdf with its Quote. If a Bidder does not submit the completed Questionnaire with the Quote, the Bidder must comply within seven (7) Business Days of the HESAA's request or HESAA may deem the Quote non-responsive.

This Questionnaire is designed to provide HESAA with an overview of the Bidder's security and privacy controls to ensure that the Bidder will (1) meet the Authority's objectives as outlined and documented in the Statewide Information Security Manual; and (2) comply with HESAA's security requirements as outlined in Section 6 – Data Security Requirements – Contractor Responsibility. HESAA reserves the right to remove a Bidder from consideration of Contract award if HESAA determines that the Bidder's Questionnaire failed to sufficiently convey that the Bidder's security and privacy controls meet HESAA's requirements.

HESAA has executed a Confidentiality/Non-Disclosure Agreement which is attached to the Questionnaire. The Bidder should countersign the Confidentiality/Non-Disclosure Agreement and include it with its submitted Questionnaire. If a Bidder does not submit the signed Confidentiality/Non-Disclosure Agreement with the Questionnaire, the Bidder must comply within seven (7) Business Days of HESAA's request or the HESAA may deem the Quote non-responsive. No amendments to Confidentiality/Non-Disclosure Agreement are permitted.

To the extent permissible under OPRA, the New Jersey common law right to know, and any other lawful document request or subpoena, the completed Questionnaire and supplemental documentation provided by the Bidder will be kept confidential and not shared with the public or other Bidders.

8.12 Privacy Policy

The Contractor is responsible for adhering to the Authority's privacy policy, as updated from time-to-time, and ensuring that any subcontractors to the prime Contractor also adhere to the policy. The Authority retains the right to seek any and all legal remedies in the event of a breach of the privacy policy by the prime Contractor or any subcontractor. HESAA's Privacy Policy can be found at: https://www.hesaa.org/Documents/PrivacyNotice.pdf.

8.13 Additional Work and/or Special Projects

The pricing response in this RFP is intended to be all-inclusive; the Authority anticipates that no additional work or special projects will be necessary. However, the Authority recognizes that changes in federal and state law and regulations over the course of the term of the contract may create additional work required from the Contractor. HESAA reserves the right to negotiate with the Contractor reasonable fees for services unanticipated or not existing at the time of contract award. Such services may include, but are not limited, to the initiation of an electronic payment system to be integrated into lockbox item processing, with associated posting and reporting functions. The Contractor shall work with other HESAA Contractors, if needed, to incorporate such products and functions. Should such a situation occur, HESAA personnel will be appointed at the appropriate time to act as project leader.

In the event of additional work and/or special projects, the Contractor must present a written proposal to perform the additional work to HESAA. The proposal should provide justification for the necessity of the additional work. The relationship between the additional work and the base contract work must be clearly established by the Contractor in its proposal.

The Contractor's written proposal must provide a detailed description of the work to be performed broken down by task and subtask. The proposal should also contain details on the level of effort, including hours, labor categories, etc., necessary to complete the additional work.

The written proposal must detail the cost necessary to complete the additional work in a manner consistent with the contract. The written price schedule must be based upon the hourly rates, unit costs, or other cost elements submitted by the Contractor in the Contractor's original proposal submitted in response to this RFP. Whenever possible, the price schedule should be a firm, fixed price to perform the required work. The firm fixed price should specifically reference and be tied directly to costs submitted by the Contractor in its original proposal. A payment schedule, tied to successful completion of tasks and subtasks, must be included.

No additional work and/or special project may commence without the Authority's written approval. In the event the Contractor proceeds with additional work and/or special projects without the Authority's written approval, it shall be at the Contractor's sole risk. HESAA shall be under no obligation to pay for work performed without HESAA's written approval.

8.14 Severability

In the event that any provision of this RFP or any agreement executed in accordance herewith shall be held invalid or unenforceable by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision.

9.0 SELECTION PROCESS

9.1 Small Business Preference

This RFP includes an evaluation preference for those Bidders who are registered as a Small Business Enterprise (SBE) with the Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit as of the date the proposal is received by HESAA.

In order to receive the preference, the Bidder must be registered as a qualified small business with the Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit, by the date the proposal is received by HESAA.

A Bidder should verify its Small, Minority, Veteran, and Women Owned Business Certification status on the "Maintain Terms and Categories" Tab within its profile in ***NJSTART***. In the event of an issue with a Bidder's Small, Minority, Veteran, and Women Owned Business Certification status, ***NJSTART*** provides a link to take corrective action.

If the Bidder has previously registered or been certified as a Small Business Enterprise, the Bidder should ensure it is currently registered and that its registration is active with the Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit, prior to submitting the proposal, to be eligible for award. The Bidder should ensure that it has completed the annual verification, if required.

Information, registration requirements and application are available at https://www.nj.gov/treasury/revenue/ucs.shtml.

9.2 Disabled Veterans' Business Preference

This RFP includes an evaluation preference for those Bidders who are registered as a Disabled Veterans' Business with the Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit as of the date the proposal is received by HESAA.

In order to receive the preference, the Bidder must be registered as a qualified Disabled Veterans' Business with the Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit by the date the proposal is received by HESAA.

A Bidder should verify its Small, Minority, Veteran, Women and Disabled Veterans' Business Certification status on the "Maintain Terms and Categories" Tab within its profile in ***NJSTART***. In

the event of an issue with a Bidder's Small, Minority, Veteran, Women and Disabled Veterans' Business Certification status, ***NJSTART*** provides a link to take corrective action.

If the Bidder has previously registered or been certified as a Disabled Veterans' Business, the Bidder should ensure it is currently registered and that its registration is active with the Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit, prior to submitting the proposal, to be eligible for award. The Bidder should ensure that it has completed the annual verification, if required.

Information, registration requirements and application are available at https://www.nj.gov/treasury/revenue/ucs.shtml.

9.3 Evaluation Criteria

The Authority will select a firm based on responses to the proposals. The Authority will evaluate the proposals received in response to this RFP to ensure the Bidder meets all the requirements of the RFP. All proposals deemed responsive will be ranked from lowest to highest according to the total Quote price located on the fee proposal.

9.4 Right to Waive

HESAA may waive minor irregularities or omissions in a proposal. HESAA reserves the right to waive a requirement provided that the requirement does not materially affect the procurement or the State's interests associated with the procurement.

9.5 Proposal Discrepancies

In evaluating proposals, discrepancies between words and figures will be resolved in favor of words. Discrepancies between unit prices and totals of unit prices will be resolved in favor of unit prices. Discrepancies in the multiplication of units of work and unit prices will be resolved in favor of the unit prices. Discrepancies between the indicated total of multiplied unit prices and units of work and the actual total will be resolved in favor of the actual total. Discrepancies between the indicated sum of any column of figures and the correct sum thereof will be resolved in favor of the correct sum of the column of figures.

After the Quotes are reviewed, one (1), some, or all of the Bidders may be asked to clarify inconsistent statement contained within the submitted Quote.

9.6 Best and Final Offer (BAFO)

HESAA may invite one (1) Bidder or multiple Bidders to submit a Best and Final Offer (BAFO). Said invitation will establish the time and place for submission of the BAFO. Any BAFO that does not result in more advantageous pricing to HESAA will not be considered, and HESAA will evaluate the Bidder's most advantageous previously submitted pricing.

HESAA may conduct more than one (1) round of BAFO in order to attain the best value for the Authority.

BAFOs will be conducted only in those circumstances where it is deemed by HESAA to be in the Authority's best interests and to maximize the Authority's ability to get the best value. Therefore, the Bidder is advised to submit its best technical and price Quote in response to this Bid Solicitation since HESAA may, after evaluation, make a Contract award based on the content of the initial submission

9.7 Board Approval

Appointment of a firm is subject to approval by the Authority's Board.

EXHIBIT A: Pricing Matrix				
A. Licensing Costs				
Item	**Unit Price**	**Quantity**	**Extended Price**	
UC License (per user/month)				
CC Agent License				
CC Supervisor License				
Devices (per unit)				
B. PSTN				
Item	**Rate**	**Usage Basis**	**Total**	
SIP Trunks / Call Paths				
Local Minutes				
Long-Distance Minutes				
Toll-Free / TFN				
Number Porting				
Burst Pricing				
C. AI Capabilities				
AI Function	**Unit**	**Included?**	**Unit Rate**	**Overage**
ASR (real-time)	per min	Y/N		
ASR (batch)	per min	Y/N		
Agent Assist	per user/mo			
Virtual Agent	per session/min			
Auto-QA	per seat or min			
D. Storage & Tuning				
Item	**Unit**	**Rate**		
Recording Storage (GB/month)				
Transcript/Analytics Storage				
Archival Storage				
KB / Prompt Ops / Tuning	Fixed price + hourly			
E. Professional & Managed Services				
Service	**Fixed Price**	**Hourly Rate**	**Notes**	
Implementation Services				
Managed Services (monthly)				
Training				
F. Financial Guardrails				
Guardrail	**Vendor Response**			
True-up/true-down mechanics				
Annual uplift cap (CPI-U or 3%, whichever lower)				
NTE Year 1				
NTE Renewal Years				