Southeastern Pennsylvania Transportation Authority
1234 Market Street • Philadelphia, PA 19107-3780

June 17, 2026

Hello:

Enclosed please find attached Addendum No. Two (2) for SEPTA RFP No. 26-00036-ACAC, Actuarial Services.

Addendum No. 2 must be acknowledged by signing the Addendum Acknowledgement Form and submitting it with your Technical Proposal.

The due date for the submission of Proposals has been changed from **Wednesday, June 24, 2026 at 3:00 PM to Wednesday, July 1, 2026 at 3:00PM.**

This Addendum provides answers to some of the questions received. The responses to the remaining questions will be provided under a separate Addendum.

Any inquiries regarding this Addendum must be directed to Carolyn Cotton of the Procurement and Supply Chain Management Department at (215) 580-7599 or cCotton@SEPTA.org.

Thank you for your interest in SEPTA.

Sincerely,

Carolyn Cotton

Carolyn Cotton
Senior Contract Administrator
Procurement & Supply Chain Management

SEPTA's RFP No. 26-00036-ACAC Actuarial Services

This addendum to the Contract Documents is hereby part of the same and is incorporated in full as part of the Project. Proposer shall acknowledge Addendum No. 2 by completing the lines below, and returning this Addendum Acknowledgement Form with your Technical Proposal.

FIRM NAME (typed or printed) _____

AUTHORIZED SIGNATURE _____

TITLE _____

NAME (typed or printed) _____

DATE_____

This Addendum includes:

A. General

The due date for the submission of Proposals has been changed from **Wednesday, June 24, 2026 at 3:00 PM to Wednesday, July 1, 2026 at 3:00PM.**

This Addendum provides answers to some of the questions received. The responses to the remaining questions will be provided under a separate Addendum.

B. Questions and Answers (20)

Q1: Does the organization expect the pension portal solution to be hosted within the vendor's infrastructure, deployed into the organization's infrastructure, or supported through a hybrid deployment model? This impacts pricing, hosting, and scope of the project.
A1: Vendor's infrastructure.

Q2: What are the preferred cloud providers?
A2: AWS and Microsoft Entra/Azure.

Q3: Should the deployment be on premises or cloud?
A3: Cloud.

Q4: Should the infrastructure be hosted in a specific location?
A4: Contiguous US; multitenant environment is acceptable.

Q5: What are the disaster recovery and backup requirements?
A5: The vendor's standard, best-practices derived, and client-facing disaster recovery and backup procedures are acceptable. Please share these as part of your response to this RFP.

Q6: What are the SLA expectations?
A6: Vendor's standard, best practices-derived, and client-facing SLAs are acceptable. Please share these as part of your response to this RFP.

Q7: Who is responsible for monitoring the infrastructure (patching, upgrades, db management, security remediation, backups)?
A7: Refer to Q1 and Q1 - vendor and vendor's infrastructure services provider with clear communication to SEPTA on timings and detailed release notes.

Q8: Will the organization provide the following?:
- Q8a: Cloud Environments
- Q8b: Databases
- Q8c: Load balancers
- Q8d: Networking

A8a: N/A - SEPTA IT requirement is to use vendor's solution and hosting as indicated in questions Q1, Q2, Q3, and Q4.
A8b: N/A - SEPTA IT requirement is to use vendor's solution and hosting as indicated in questions Q1, Q2, Q3, and Q4.
A8c: N/A - SEPTA IT requirement is to use vendor's solution and hosting as indicated in questions Q1, Q2, Q3, and Q4.
A8d: N/A - SEPTA IT requirement is to use vendor's solution and hosting as indicated in questions Q1, Q2, Q3, and Q4.

Q9: What authentication is required (Multi-factor, SSO)?
A9: SSO through Microsoft 365 is strongly preferred.

Q10: Any penetrating testing required?
A10: None prior to execution of contract between SEPTA and vendor. Any desired penetration testing will be carefully coordinated between the vendor and SEPTA. Please complete the included security questionnaire.at the end of this document.

Q11: Are audit logs required?
A11: The vendor's hosted solution should have auditing capabilities enabled by default in addition to those provided by its infrastructure services provider, e.g., AWS or MS Entra. Any request from SEPTA to review these logs will be formally made to the vendor on a case-by-case basis.

Q12: Any specific encryption requirements?
A12: In-transit traffic must be encrypted with TLS, version 1.2 at minimum.

Q13a: What systems should the portal connect to?
A13a: SEPTA is willing and capable to establish interfaces from its existing systems of record for payroll and employee data. These will be position-delimited exports from our mainframe environment sent to the vendor via SFTP. The portal is not expected to send data back but reporting and export of data is required.

Q13b: HR, Payroll, Reporting Tools, Pension Systems?
A13b: Data from SEPTA to the portal is expected weekly. No periodic data feeds from the portal are expected at this time.

Q14: User expectations:
- Q14a: What are average users expected to be on the system at a given time?
- Q14b: What are the SLA response time expectations?
- Q14c: When are the peak calculation periods?

A14a: 2-4 Currently.
A14b: Please refer to Q6.
A14c: Periods are not defined. 8am to 4pm daily. Generally higher calc inquiries in September through October, and March through April.

Q15: UX Expectations:
- Q15a: Is multilingual support required?
- Q15b: Is mobile access required?

A15a: No.
A15b: No.

Q16: How many environments are required (Dev, QA, UAT, Prod)?
A16: Two (2) environments minimum - TEST / QA and PROD

Q17: Who manages deployments?
A17: The awarded vendor.

Q18: Are there any CI/CD requirements?
A18: Not at this time.

Q19: Are APIs already available to share data with other systems?
A19: No. SEPTA's source systems of record for employee data and payroll data are hosted on an on-premises mainframe. The mainframe uses SFTP to send or receive data.

Q20: How does SEPTA define success for this engagement?
A20: Success is measured by the awarded vendor meeting all aspects of the Scope of Work.

SEPTA VENDOR INFORMATION SECURITY QUESTIONS

Introduction

This questionnaire should be completed by any vendor that will provide technology services to SEPTA and submitted with all the other requirement materials when a vendor submits a bid to provide IT related functions.

SEPTA Project Name

SPONSORING DEPARTMENT:
PRIMARY CONTACT:
CONTACT PHONE:
CONTACT EMAIL:

Vendor Information

COMPANY NAME:
COMPANY URL:
PRIMARY CONTACT:
CONTACT TITLE:
CONTACT PHONE:
CONTACT EMAIL:

Network Diagram and BoM

Please provide network diagrams that includes all logical and physical components as well as a hardware and software bill of materials for all components and verify that they meet SEPTA's IT System Requirements.

Data Security

Where will my data physically reside?

Do you control the physical infrastructure or is the data hosted by a third-party cloud provider?

Can I specify the geographical location where the data are to be stored?

Who owns the data? Who owns metadata generated in the course of using the software?

Will any third parties have access to my data?

How is data protected in transit between the vendor and the client as well as between the vendor and the end-user? How is data protected at rest on servers and backup media? Are data transmissions to/from the application encrypted? Do you encrypt our data? Which data is encrypted? What kind of encryption is used?

What happens to data if the contract ends?

When data is deleted, is it permanently erased?

Who is responsible for the protection of my data? Which aspects of security are the responsibility of the provider, and what remains the responsibility of the customer?

Which jurisdiction(s) govern the service and our agreement, and how do you comply with regulations in those jurisdictions?

Security Management

What are you actively doing to prevent breaches?

How do you inform customers about security issues such a known security vulnerabilities?

Have you had any breaches or security issues in the past?

Are penetration tests performed by a qualified third party vendor? If so, how often are they performed and when was the last test performed?

Do you use IPS/IDS? Do you monitor failed logins? Do you use two-factor Authentication?

Are user actions in the application tracked?

Do you outsource any of your information security responsibilities? How do you ensure your third party vendors are secure?

Do you offer API access? How is access controlled?

Is the platform highly available, even under peak demand conditions? Will my data be available if a disaster impacts one of your data centers?

Have you implemented monitoring and alerting for your network?

Do you have a process for installing operating system and application updates and security patches on servers?

Are your systems configured to log security-relevant events, such as authentication, data access, etc.?

Do you regularly test your backups?

Security Policies

What policies and procedures do you use for your company and your data? What certifications do you hold

Do you have any security certifications? Are you PCI or HIPAA compliant? Do you have a SSAE16 (SOC 1/2/3), ISO27001/2 or another 3rd audit? If yes, what and when was the last one completed?

Can you provide the results of your most recent external security audit or penetration test?

Do you have a disaster recovery or business continuity plan?

Is there a formal information security program in place?

Is there a formal logical access review process? Do you adhere to the principles of least privilege?

Are employees and contractors required to attend security training?

Is there a formal incident management program in place?

Do you have a written policy that lists the physical security requirements for office facilities?

IT System Requirements

Servers

Virtualization

- All servers are deployed as virtual machines using VMware vSphere hypervisor.
- No hardware servers will be deployed.
- All server hardware is managed by SEPTA IT.

Operating Systems

- Windows servers must use Windows Server 2016 or later.
- Linux servers must use Ubuntu 20.04 LTS or later LTS release (only LTS releases are deployed).
- Server operating systems are managed by SEPTA IT.

CPU

- Up to 96 cores running at 2.4 Ghz can be provided per server.

Memory

- Up to 512 GB of RAM can be provided per server.

Storage

- The following physical storage types are available.
    - Spinning disk
    - SSD

Database

- Microsoft SQL Server 2014 or later is our preferred database platform.

Management

- All servers will be joined to SEPTA's domain.
- All Windows servers will have SEPTA's Group Policy Objects applied.
- Software updates for operating systems and COTS software will be automatically performed by SEPTA in accordance with SEPTA's update schedule.

Security

- All servers will have SEPTA's endpoint protection (EDR, antivirus, antimalware, etc.) software installed.
- All server admin work will only be performed using Privileged Access Workstations that are physically separate from normal workstations.

Remote Access

- Remote access, if necessary, will be supplied through SEPTA's privileged remote access system.
- No other forms of remote access will be allowed.

Network

- The TCP/UDP ports and application protocols used by the application must be identified.
- Estimated bandwidth usage and throughput requirements must be provided.

Encryption

- Traffic must be encrypted in transit with TLS.
    - TLS minimum version is 1.2.

Data access/interchange

- All interfaces with other SEPTA systems used to exchange data must be identified and described.
- All communications with other SEPTA systems must be encrypted.
- TCP/UDP ports and application protocols for these data transfers must be identified.

Clients

Operating Systems

- Clients must use a currently-supported release of Windows 10.
- Clients must run Windows 10 Enterprise.
- All clients must be imaged using SEPTA's standard imaging process.
- If vendor is supplying client hardware, it must include access to all drivers necessary to make SEPTA's standard Windows 10 Enterprise image work with the hardware provided.

Management

- All clients will be joined to SEPTA's domain.
- All clients will have SEPTA's Group Policy Objects applied.
- All clients will be managed by SEPTA's InTune environment.
- All client software will be distributed and installed by SEPTA's InTune environment.
- Software updates for operating systems and COTS software will be automatically performed by SEPTA in accordance with SEPTA's update schedule.

Security

- All clients will have SEPTA's endpoint protection (EDR, antivirus, antimalware, etc.) software installed.
- No local user accounts can be used on clients. All user accounts must be Active Directory domain accounts.

Application

- Web applications
  - Must support the current releases of Chrome, Firefox, and Edge.
  - Must not require browser plugins for the application to operate.
- Client applications
  - Must run on SEPTA's supported client operating systems (see above Client section).
  - Must not include any discontinued or end-of-support software.
- Mobile applications
  - Must run on the latest release of iOS or Android.

Cloud (SaaS, IaaS, PaaS, etc)

Authentication

- SSO using SAML or OID Connect with SEPTA's existing Microsoft Azure Active Directory is preferred.
- If an application does not authenticate using SEPTA's Microsoft Azure Active Directory, then it must provide a method for multi-factor authentication on all accounts.
- The person responsible for creating accounts in the cloud system must be a SEPTA staff member.
  - This person must be clearly identified in the project plan, SOW, or RFP.

Application

- Web applications
  - Must support the current releases of Chrome, Firefox, and Edge.
  - Must not require browser plugins for the application to operate.
- Client applications
  - Must run on SEPTA's supported client operating systems (see above Client section).
  - Must not include any discontinued or end-of-support software.
- Mobile applications
  - Must run on the latest release of iOS or Android.

Encryption

- Traffic must be encrypted in transit with TLS.
  - TLS minimum version is 1.2.

Hosting

- The location and service(s) used to host all systems involved in providing the application must be disclosed to SEPTA.

Network

- The TCP/UDP ports and application protocols used by the application must be identified.
- The domains and IP addresses used by the application must be provided.
- Estimated bandwidth usage and throughput requirements must be provided.

Data access/interchange

- All interfaces with other SEPTA systems used to exchange data must be identified and described.
- All communications with other SEPTA systems must be encrypted.
- TCP/UDP ports and application protocols for these data transfers must be identified.

SLA/Backup

- SLAs for the system must be clearly identified.
- SEPTA must be able to obtain a backup copy of all SEPTA data at its discretion.

Security

- The service provider must provide documentation about its security policies.
  - Documentation should include the following:
    - Cybersecurity frameworks or standards in use
    - Incident response and disaster recovery plans
    - Attestations of results or audit reports from regular security audits
- SOC 2 or similar certification must be provided for the locations hosting the system.