SCHOOL EMPLOYEES RETIREMENT SYSTEM OF OHIO
300 E. BROAD ST., SUITE 100 • COLUMBUS, OHIO 43215-3746
614-222-5853 • Toll-Free 800-878-5853 • www.ohsers.org

Request for Proposal – Identity and Access Management
Questions Submitted to SERS

Question 1: ***To ensure we are providing a compliant and responsive bid, would you be willing to extend the due date for two business weeks?***

Answer: The due date cannot be extended.

Question 2: ***Can you provide the list for financial applications and core business applications? How many are there?***

Answer: Yes. We use Great Plains and a custom benefits processing platform (SMART). ADP is used for Payroll. A complete list will be shared with the winning bidder.

Question 3: ***How extensively are cloud services utilized, and are there specific platforms or providers? (MSFT Azure, AWS, Google, other) What is the environment?***

Answer: SaaS applications are used throughout the organization with Microsoft being the core of most standard business functions.

Question 4: ***What are the supported mobile devices? How many?***

Answer: Laptops and tablets. Less than 200.

Question 5: ***What are user identity store within scope i.e. Active directory, LDAP?***

Answer: Active Directory and associated identity platforms.

Question 6: ***What do the IAM systems encompass? i.e. IGA, Access Management, PAM***

Answer: Internal forms (wet ink signatures and electronic forms), Active Directory, databases and Microsoft 365.

Question 7: ***What is the vendor and is it cloud or on-premise for the IAM system?***

Answer: Compilation of systems and processes. No outside vendor.

Question 8: ***Is there any SIEM solution and what is the vendor?***

Answer: Our management SOC partner has a tool that we aggregate and forward logs to for analysis.

Question 9: ***What compliance regulation/s?***

Answer: HIPAA, NIST, PII regulations.

Question 10: ***What is the SERS budget for this project?***

Answer: The project is budgeted, but no details on the budget can be provided at this time.

Question 11: ***We noted that the contact person is the Chief Audit Officer. Should the consulting firm's work be completed in internal audit workpaper templates?***

Answer: This will not be necessary.

Question 12: ***What existing platforms are in place at SERS (e.g., Sailpoint, Saviynt, Fischer, Okta, etc.)?***

Answer: Internal forms (wet ink signatures and electronic forms), Active Directory, databases and Microsoft 365.

Question 13: ***Section III (Scope of Services) mentions alignment with relevant regulatory requirements. Has SERS already identified their applicable regulatory requirements related to this project scope?***

Answer: HIPAA, PII requirements, NIST.

Question 14: ***Does SERS have existing IAM architecture diagrams and process flows that the consulting firm will be able to leverage?*** **Is there an IDAM strategy in place for the organization?**

Answer: Documentation does exist. We can share specifics with the selected vendor.

Question 15: ***Does SERS have an expected number of hours for this project to be completed in?***

Answer: The timeline is included in the RFP. We have not identified the anticipated number of hours to complete the project.

Question 16: ***What is the IAM identity provider solution implemented for SERS and how does the NIST cybersecurity framework contribute to its implementation?***

Answer: Internal forms (wet ink signatures and electronic forms), Active Directory, databases and Microsoft 365.

Question 17: ***Is there any specific reason or business requirement for using NIST cyber security framework? Are there specific compliance requirements that the IDAM system must adhere to (e.g. GDPR, HIPAA)? Are there auditing requirements for NIST SP 800-53 regulatory compliance?***

Answer: We selected NIST as our framework after reviewing possible frameworks.

Question 18: ***Can you elaborate on your approach to assessing IT Operational infrastructure systems, mobile devices?***

Answer: IT performs a manual review of access quarterly.

Question 19: ***What is the total number of Employee and Contractor users?*** **What is the average number of users active on a daily basis? How many different types of accounts (regular, privileged, service)?**

Answer: Approximately 200.

Question 20: ***What serves as the primary source of truth for identity management within SERS (in what system are passwords stored)?***

Answer: Active directory.

Question 21: What is the current IAM (SSO) solution being used?

Answer: Active directory and Microsoft 365.

Question 22: How are user identities created, managed, and deactivated within the system? What is the degree of automation?

Answer: Access control forms are used to document the granting of access, modification of access rights and deactivation. Multiple approvals are required.

Question 23: Does SERS incorporate user provisioning and deprovisioning concepts? Does it rely on any external user database/directory services for storing user information?

Answer: Yes. Internal resources.

Question 24: Are two factor(2FA)/multi-factor authentication (MFA) or biometric authentication methods implemented? What solution is in place?

Answer: Two factor authentication methods are used.

Question 25: What measures are in place to assess and enhance the strength of user authentication controls?

Answer: The details of SERS security measures will be shared with the winning bidder.

Question 26: Is federated login journey implemented for users? Is your AD federated with other Identity providers (Idp) for SSO e.g. Okta, PingFederate etc.?

Answer: Yes. Microsoft Entra-ID (formerly Azure-AD).

Question 27: ***What are the existing password policies available in IAM Solution used by SERS?***

Answer: SERS policy will be shared with the winning bidder.

Question 28: ***Does the NIST framework extend support for and implementation of Single Sign-On (SSO) features within the SERS system? If yes, on which standard it is being implemented.***

Answer: No. We can discuss the details with the winning bidder.

Question 29: ***How does SERS manage excessive privileges, and what strategies or features within the NIST framework are implemented for this purpose?***

Answer: We will share details with the winning bidder.

Question 30: ***Does it have the provision to support OAuth/OIDC/SAML standard and use single user source or any external user source like Active Directory?***

Answer: SERS uses modern authentication and authorization strategies and tools.

Question 31: ***How do you plan to evaluate the strength and effectiveness of user authentication controls within SERS?***

Answer: We expect the vendor to complete an evaluation of our IAM processes and controls.

Question 32: ***How is Privileged Access Management (PAM) integrated within the SERS system as per the guidelines of the NIST framework?***

Answer: We will share with the winning bidder.

Question 33: ***What tools and systems are used for monitoring and logging IAM activities? How do you manage AD security, such as user accounts, passwords, permissions, group policies, and auditing?***

Answer: We will share with the winning bidder.

Question 34: ***Is Phishing, Smishing or any other Scams handled?***

Answer: Security incidents are investigated by Information Security. Security tools are used to minimize the impact.

Question 35: ***Are there mechanisms in place for real-time alerting in case of potential security incidents?***

Answer: Yes.

Question 36: ***How many applications are integrated?***

Answer: The details of SERS security measures will be shared with the winning bidder.

Question 37: ***What is the current IGA product being used?***

Answer: A combination of tools and processes.

Question 38: ***Do you have a centralized system for managing user access rights? If yes, what types of access control mechanisms are currently employed (e.g., role-based access control, attribute-based access control)?***

Answer: Yes.

Question 39: ***Is user Provisioning/De-provisioning (onboarding and offboarding) implemented?***

Answer: Yes.

Question 40: ***Which applications are using user Provisioning/De-provisioning (list of SaaS based applications)? What is the total Number of SAAS based applications / on Prem applications?***

Answer: Additional details will be shared with the winning bidder.

Question 41: ***Which regulatory requirements must the IAM Solution align with?***

Answer: HIPAA, NIST, PII regulations.

Question 42: ***Is there any documentation on how compliance is currently verified and maintained?***

Answer: An internal assessment of IAM is completed quarterly. Other assessments are periodically performed by the Internal Audit function, Information Security or in some cases a third party. Details can be shared with the winning bidder.

Question 43: ***What is the compliance standard being maintained currently by SERS?***

Answer: NIST is the SERS security standard.

Question 44: ***Are there plans for periodic compliance audits?***

Answer: An internal assessment of IAM is completed quarterly. Other assessments are periodically performed by the Internal Audit function, Information Security or in some cases a third party.

Question 45: ***Can you provide examples of previous assessments where you have evaluated password policies and practices for robust security?***

Answer: Additional details of previous assessments will be shared with the

winning bidder as needed.

Question 46: ***Can the work be completed fully remote?***

Answer: The majority of this work if not all can be completed remotely. Any on-site work would be limited. This will be discussed with the winning bidder.

Question 47: ***How much access to existing systems and environments will be available to the vendor?***

Answer: The required access to complete the project will be made available.

Question 48: ***Are there 3rd party suppliers who will need to be consulted or involved in the review?***

Answer: It is not anticipated at this time.

Question 49: ***Will SERS subject matter experts be available?***

Answer: SERS subject matter experts will be available as needed.

Question 50: ***Will there be a product owner assigned to this project?***

Answer: This review will be performed for the Chief Audit Officer with the Audit Committee and management receiving the final report.

Question 51: ***The "scope of review" is very much focused on security. Would there be appetite for a UX assessment which is as or nearly as important as security for a successful IAM solution?***

Answer: Not at this time. We have an IAM solution. We are looking for an assessment of the current state of our IAM policies and procedures.

Question 52: ***Have there been any previous security incidents or breaches related to IDAM?***

Answer: Any details related to security incidents will be shared with the winning bidder only as needed.

Question 53: ***How much up to date documentation is available on the current state of the existing IDAM solution? Including NFRs?***

Answer: Current documentation does exist and will be shared with the winning bidder as needed.

Question 54: ***How many domains and forests do you have to support your organization's structure and security boundaries?***

Answer: One.

Question 55: ***How is the logical structure of AD for your organization, such as domains, forests, organizational units (OUs), and groups?***

Answer: Details will be shared with the winning bidder.

Question 56: ***How do you secure your Active Directory environment, such as user accounts, passwords, permissions, group policies, and auditing?***

Answer: Details will be shared with the winning bidder.

Q***uestion 57:*** ***Number (and types) of systems and applications that interact with the IDAM system.***

Answer: Details will be shared with the winning bidder.

Question 58: ***What are the current SSO protocols supported within your current integrations e.g. SAML, OAuth, Open ID Connect etc.***

Answer: This technical information will be provided to the winning bidder as needed.

Question 59: ***What is the physical structure of AD for your network, such as sites, subnets, site links, and replication topology?***

Answer: This technical information will be provided to the winning bidder as needed.

Question 60: ***Provide details about the overall architecture of the IDAM system, including components such as identity providers, directories, authentication mechanisms, and access control mechanisms. Can you describe your current IDAM system? What are the primary challenges you face with your current IDAM system?***

Answer: The specifics of the overall architecture will be shared with the winning bidder as needed.

Question 61: ***What are your expectations for support and maintenance for the IDAM solution? Are you looking for a managed service or do you plan to manage the service in house?***

Answer: We are not looking for a IDAM solution. This RFP is for a review (audit) of our current policies and procedures.

Question 62: ***Is the current solution managed and maintained internally? Is the current model in line with objectives?***

Answer: Managed internally.

Question 63: ***How do you perform backup and restore operations for AD, such as system state backup, authoritative restore, and non-authoritative restore?***

Answer: We will share details as needed with the winning bidder.

Question 64: ***Do you use an Agile methodology supported by JIRA or Azure DevOps?***

Answer: Yes. Beginning to use Agile.

Question 65: ***What ticketing system do you use today? Do you have a preferred ticketing system for future use?***

Answer: Currently using a specific system. No plans to change our ticketing system. Any other details will be shared with the winning bidder as needed.

Question 66: ***What business and/or IT strategies/plans do the IDAM solution have to facilitate?***

Answer: SERS would like to maintain a secure system that complies with best practices that can support innovation and growth.

Question 67: ***Are there any features missing from the existing solution which prohibit these strategies/plans?***

Answer: No. The assessment should be designed to identify weaknesses in our approach to IAM.

Question 68: ***What governance and technical standards do you wish to have the assessment be made against?***

Answer: HIPAA, NIST, PII regulations.

Question 69: ***Has SERS undertaken an Information Security Risk Registry Exercise?***

Answer: SERS has a Risk Management Office that prioritizes organizational risks and maintains a risk register. SERS Internal Audit also

performs an annual risk assessment.

Question 70: ***Do you have a clear description of what worries your enterprise executive leadership has regarding IAM policies and practices?***

Answer: SERS has a Risk Management Office that prioritizes organizational risks. SERS Internal Audit also performs annual risk assessment. IAM is one of the many important functions that protect SERS assets and sensitive data. No specific worries beyond ensuring that SERS has strong controls and good policies and procedures.

Question 71: ***What requirements do regulatory agencies impose on you regarding IAM? How prescriptive are they (e.g., does a regulatory agency require specific conformance to all or some SP 800-53 controls)?***

Answer: HIPAA

Question 72: ***Can you provide more details about the structure of SERS, especially the distribution of IT professionals among the 34 mentioned?***

Answer: Details can be shared with the winning bidder.

Question 73: ***How many SERS IT staff members are involved with security, and how many specifically with IAM? Are any IAM functions or solutions currently outsourced to a vendor for engineering or maintenance?***

Answer: We will share details with the winning bidder.

Question 74: ***Could you elaborate on the specific authentication controls currently in place that you would like to assess?***

Answer: We will share details with the winning bidder.

Question 75: ***Are there any particular concerns or incidents related to user authentication that prompted this assessment?***

Answer: No. This is a normal part of SERS Internal Audit rotation through important processes. You will be performing this assessment/ review on behalf of and with some assistance from the Chief Audit Officer.

Question 76: What specific IAM systems are in use for monitoring and logging capabilities?

Answer: We will share details with the winning bidder.

Question 77: Are there any existing challenges or incidents related to the effectiveness of alerting mechanisms?

Answer: While there are challenges related to any process nothing at this time takes priority. We would expect that through the review process pain points and other challenges would be discussed with SERS staff.

Question 78: Are there any critical milestones or dependencies that could impact the project timeline?

Answer: Not at this time. The work should be completed according to the timeline outlined in the RFP.

Question 79: Could you elaborate on the specific information or insights you expect to gather from the questionnaire responses?

Answer: They are standards questions that appear in all SER RFP documents. Information about the firm, the firms qualifications, etc. assist SERS staff in evaluating RFP responses.

Question 80: Please clarify if the Assessment scope is to focus primarily on SERS employees and contingent workers (not to SERS benefit recipients, external business partners, etc.), and that the number of users is approximately 180. Is there a separate head count for contractors?

Answer: This is focused on SERS staff and contractors. There are 180 full-time employees and a much smaller number of contractors. Benefit recipients are not included.

Question 81: ***What high-priority issues, gaps or audit concerns are drivers for the assessment?***

Answer: No specifics gaps or audit concerns. SERS Internal Audit function is an independent office that performs audits and assessments of SERS business and IT activities.

Question 82: ***What, if any, technical solutions / products are currently used by SERS? Does "as-built" documentation exist for these solutions?***

Answer: We will share details with the winning bidder.

Question 83: ***What Identity Providers (IdPs) and authentication and authorization services (e.g. MFA) are in use by SERS, and how many instances?***

Answer: We will share details with the winning bidder.

Question 84: ***What is the scope of "Mobile Devices" as mentioned in SCOPE OF SERVICES, e.g. their use in authentication, endpoint management, etc.?***

Answer: SERS managed laptops and tablets.

Question 85: ***Will SERS provide remote access to a firms audit team members?***

Answer: Remote access will be provided as needed in order for the project to be completed.

Question 86: ***Are oral presentations required to be on-site or is video conferencing acceptable?***

Answer: Video conferencing should be acceptable.