IDENTITY ACCESS MANAGEMENT SYSTEM

HIGHLIGHTS FROM THE REQUEST FOR PROPOSAL

FROM DEPARTMENT OF INFORMATION TECHNOLOGY

RFP FROM DIT ON:
IDENTITY ACCESS MANAGEMENT SYSTEM

The purpose of this RFP and any resulting contract award is to solicit proposals for an Identity and Access Management Managed Service (IAM-MS) for the State of North Carolina government. The service will provide every State employee in North Carolina, as well as employees of local government, teachers, students, businesses, service providers and individuals who interact with State applications, an account with a single username and password that will enable authenticated access to on-premise and cloud-based resources. The IAM-MS will have three major components: a centralized data repository with all user identity information collected, a central directory service that provides a master authentication and authorization resource, and federation software that enables single sign-on (SSO) functionality for users.

The State is looking to the future and planning for the next generation of identity management. Long-term, the State is seeking to implement a distributed identity store with a token-based claim process and cryptographically-signed permissions. Further, the State seeks to authenticate citizens as they interact with services in a way that captures and validates micro-credentials.

For instance, a citizen who has passed the driver's test can hold a driver's license credential, a citizen who has been hired by the State can access wireless networks in certain State buildings, a citizen who holds a verifiable education degree and who has passed certain licensure exams can hold a teaching license, and so on.

The NC Department of Public Instruction (DPI) manages an IAM service supporting NC public schools. This service provides authentication and authorization services for all teachers, school staff/administration, and students. The service manages over two million active accounts supporting an average of 500,000 logins per weekday, peaking at a million logins per weekday. There are currently 27 unique target applications (service providers). In total, there are several thousand integrations, as target applications are integrated on a school district by district basis.

Key aspects of modernizing the Identity Access Management service include, but are not limited to the following:

- Replacing NCID authentication service (including self-service and onboarding workflow management);
- Automating Identity Management for those applications that have existing directories, consolidating directories where possible, and creating new directories as needed;
- Deploying application launcher/dashboards to State employees and agencies;
- Providing Multi-Factor Authentication (MFA);
- Providing Privileged Access Management (PAM)

- The most immediate priority of the NCID service modernization program is replacing the current DIT-managed NCID authentication service with a managed identity provider solution.
- A key element of an IAM service is the management and provisioning of identities within a directory. In some cases, there is a logical authoritative database/application from which identity data can be sourced. For instance, State employee data is managed in the State's Integrated HR/Payroll System and students' data is managed in the statewide student information system (SIS). Currently DPI's existing IAMS automates the management of student identities through an integration with an authoritative SIS integration that updates daily.

- The Department of Public Instruction will be the first agency to use the new automation solution, with other agencies to follow, including the source for State employee identity information.

- The State considers MFA to be part of a comprehensive IAM-MS. The State prefers to replace the existing MFA service with functionality provided within the proposed IAM-MS. The State requires multi-factor authentication to comply with current state and federal mandates and contractual obligations. The State's current MFA capability is built upon the Microsoft Azure MFA solution and provides MFA functionality for agencies' services and applications that integrate with NCID as a first factor authentication of user identity

- The current solution supports the following second factor methods:
- Phone calls
- SMS/text messages
- Mobile apps (Android; iOS; Windows)
- Hardware tokens (FOBS)
- Software tokens (Windows OS app)

- Currently DIT provides authentication for approximately 20,000 accounts, and is onboarding approximately 2,000 new users per week. It is estimated that the service will grow to approximately 100,000 users in the next twelve months.

- The proposed IAM service will scale from 500,000 to over 8,000,000 active accounts.
- The proposed IAM service will support an average of 200,000 logins per weekday with 350,000 peak logins, scaling to 2,000,000 logins per weekday, peaking at 3,000,000 logins per weekday.