Ohio's Big Bang: Launching Single Sign-on for the Department of Education

Category: Cybersecurity

State: Ohio

Contact: Katrina Flory, Department of Administrative Services, State of Ohio; Katrina.flory@das.ohio.gov

Project Initiation and End Dates: March 8 – May 13, 2019

Executive Summary

The InnovateOhio Platform, Department of Education, and Department of Administrative Services partnered with a private vendor to bring every application used by the Department of Education – 43 in total – onto Ohio's digital identity platform, which includes user lifecycle management, identity proofing, strong authentication, coarse-grain authorization, fraud analytics, and threat monitoring.

Ohio's digital identity provides an end-to-end solution that fosters a simpler, more trustworthy, and secure experience between the State and its constituents by:

- Developing a single proofed identity for citizens (teachers, parents, and students) and internal users (State employees) that enables access to all required state resources with the assurance that the individual is who they say they are.

✓ Onboarded **43 applications** to the State identity platform in a single integration completed in 3 **months**

✓ Moved from "home-grown" in-app security to a **NIST 800-53 compliant**, enterprise-supported identity product

✓ Successfully on-boarded **25K new users** in the first month

✓ Available to **700K teachers, students, parents, and administrators**

- Automating privacy and security laws and policies compliance, including NIST, HIPAA, IRS 1075, accessibility standards per section 508 of the Rehabilitation Act, and the State of Ohio's standards for data retention

- Hosting in the cloud on a highly available and highly resilient redundant infrastructure

- Offering three levels of assurance, as well as multi-factor authentication with the level and frequency of identity authentication chosen by the individual content owners

Delivering a set of identity services for consumption by all agencies, boards, and commissions that will simplify, decrease cost, and enable delivery of a better experience for the end user.

Concept

After Ohio's digital identity program had been stood up, onboarding key user groups became the next priority. Onboarding the Ohio Department of Education (ODE), with over 700,000 potential users, represented a significant step forward as our program moved out of the pilot phase and into full production. In addition, by bringing ODE users onto the State platform, offered increased security and privacy protections for one of the state's most active digital user groups.

Ohio's Digital Identity Guiding Principles & Capabilities
Ohioans expect their information to be secure and private. Ohio's digital identity program provides an enterprise solution that equips agencies to safeguard customer data and maintain compliance standards. Digital identity goes beyond security by also meeting customers' expectations for personalization, self-service account maintenance, and single sign-on access across state systems. The state formalized these concepts into two guiding principles:

- ✓ Security and privacy come first; securing data and information entrusted to the State is of foremost importance.

- ✓ Provide self-service and choice for customers to manage their own interactions.

The timeline on this project was short and sweet – less than 3 months, for development and implementation – to accommodate an end-of-the-fiscal-year deadline for teacher licensing renewal. Additionally, within the first month of go-live, 25,000 new users successfully registered an OH|ID account.

Significance

The state's digital identity program provides state agencies and organizations with capabilities that ensure that state resources and information are accessible to every Ohioan and simplifies interactions with state systems while keeping information secure and private.

Significance cont.

Single Sign-On
Sign in once to get to everything

2-Factor Authentication (2FA)
Secure assets with second factor

Multi-Factor Authentication
Increased identity security when needed

Privileged Access Management
Greater controls for sensitive accounts

ADA-Compliant
Built-in accessibility compliance

Real-Time Analytics
Monitoring and analysis

Self-Service Portal
For integrations and users

Identity Proofing
NIST-compliant proofing

Access Logging
Full logging and history

Access Management
Control Access by roles and groups

Just-In-Time Provisioning
Add users where and when needed

User Management
Manage all users

Each user's identity is centrally maintained within a controller infrastructure managed by leading practices across a host of NIST, federal, state, and accessibility regulations and standards so agencies can focus resources on services to their constituents. This solution provides the following capabilities and key security and privacy benefits:

- ✓ Provides Single Sign-On (SSO) to internal and external applications
- ✓ Automates provisioning and de-provisioning of users in near real-time
- ✓ Expands automated user provisioning and consolidation via industry standard endpoint adapters
- ✓ Mitigates security risks associated with human intervention through self-service password reset
- ✓ Provides Multi-factor Authentication (MFA)
- ✓ Provides validation of citizen identities using Experian Identity Proofing
- ✓ Closely integrates with State SIEM for real-time threat monitoring
- ✓ FedRAMP moderate certified infrastructure
- ✓ Deploys ID as a common security platform that follows State and Federal guidelines like 800-53 and 800-63-2
- ✓ Complies with NIST FIPS 140-2 and State's ITS-SEC-01 for data encryption and cryptography
- ✓ Adheres to user accessibility standards in Section 508 of the Rehabilitation Act
- ✓ Complies with IST 800-88 standard for data destruction

Significance cont.

These capabilities are scalable and delivered through a self-service enablement approach, meaning agencies can quickly onboard applications, portals, websites and intranets. Capabilities such as single sign-on and built-in ADA compliance mean all Ohioans can access the critical information and services they need from anywhere and on any device. The platform's adherence to NIST, federal and state security and privacy standards means citizen interactions with on-boarded applications and portals are always supported with the latest security standards, eliminating the need for individual agencies to monitor and maintain compliance on their own.

Impact

Through the Identity and Access Management (IDAM) initiative, ODE leveraged the digital identity program's core OH|ID Workforce & Citizen services and the Identity Platform-as-a-Service to provide their internal and external users (administrators, teachers, students, and parents) with a more secure, private, intuitive, and interactive experience. This included:

- Self-service password reset functionality available to all ODE state/county users

- Automated access provisioning for 43 applications

- Integration of account creation between the state's HCM system and digital identity platform's ISIM Console

As a result, ODE now has single sign-on access for every one of its business applications. Users are also able to take advantage of self-service password resets through OH|ID and myOhio (workforce), reducing the burden on the Cleveland Sight Center, ODE's remote call center and help desk.

Summary

This project to onboard all 43 apps as a single integration to single sign-on through myOhio and OH|ID within 3 months pushed ODE, IOP, and DAS to create a better, more secure experience for citizen and workforce users.

Ohio | Department of Administrative Services

IOP | Innovate Ohio Platform

Previously, the Department of Education's single sign-on relied on homegrown security at the application level. With this onboarding, all their apps were able to leverage the full suite of the InnovateOhio Platform's robust security and privacy capabilities and to a NIST 800-53 secure environment.

Along with that, ODE was able to modernize its user experience in familiar way – by replacing links to sites with applications tiles, creating a visual appeal that mirrors a tablet or smartphone.

The Department of Education's successful launch and adoption of single sign-on through OH|ID demonstrates the effectiveness of the program's scalable platforms and repeatable processes for both identity and user experience, enabling efficient agency on-boarding and lowering barriers to and cost of adoption. As agencies and programs onboard to this enterprise platform, they avoid ongoing and redundant costs associated with security, privacy, and ADA solutions that would otherwise be maintained at the agency and program level while also allowing quicker reaction to policy or cyber events since changes can be rolled out globally.