CASE STUDY

EASY DYNAMICS℠

FROM PATCHWORK APPROACH TO UNIFIED ACCESS

Modernizing App Authentication with MFA SSO & Zero Trust

Introduction

Federal mandates such as Executive Order 14028, *Improving the Nation's Cybersecurity;* OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management;* and OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* have clearly signaled the need for transformation. The adoption of GSA's FICAM architecture, Zero Trust architecture, phishing-resistant multi-factor authentication (MFA), and cloud-native platforms are no longer optional – they are foundational pillars for securing federal information systems. In 2022, these pillars were far out of reach for one Cabinet Level Agency (CLA).

Prior to Easy Dynamics' CLA contract award in August 2022, two other vendors had their contracts terminated due to failure to meet their obligations. The agency awarded Easy Dynamics a 5-year contract to design, build, implement, and operate an efficient, secure, and modern cloud-based identity, credential, and access management (ICAM) system to serve its employees, contractors, partners, and public users while meeting regulatory and policy requirements.

A project of this size and complexity required a multi-team Agile delivery model. Easy Dynamics established a Tier 3 ICAM Program Management Office (PMO) comprised of technologists, business analysts, communications experts, and security and policy analysts to provide strategic oversight across the organization, driving initiatives pertaining to the identity pillar that comply with strategic goals, federal guidelines, and Executive Branch Directives. With a focus on process automation, transparency, and resource optimization, the team facilitates collaboration and alignment between senior leadership, programs, and stakeholders. These core services include establishing policies and processes; facilitating training and information sharing; performing governance; and implementing, operating, and overseeing the agency's full ICAM ecosystem with cross-functional authority and enterprise-level integration.

Where to Begin?

While Microsoft's cloud-based identity and access management platform Entra ID (formerly Azure Active Directory) was deployed at CLA, it was limited to authenticating users to Microsoft 365 applications. CyberArk's privileged access management software was also deployed, but processes associated with administering privileged user accounts and access were at an ad hoc maturity level. CLA's systems and applications were a mix of custom and commercial off-the-shelf (COTS), with only a handful leveraging single sign-on (SSO) with MFA. The agency was contracted with GSA's USAccess program for PIV card issuance. Aside from these elements, CLA's ICAM program was bare bones when Easy Dynamics began its work, making it necessary to modernize and build it from the ground up. Given the agency's experience with prior contractors, the project was already delayed, and stakeholder engagement was low due to a lack

of faith in the longevity of ICAM projects. Speed, efficiency, and quality of our service delivery were key drivers.

One obstacle we faced was that the agency had only provided a single production environment, with no non-production environments available for enterprise ICAM. To enable the implementation of modern Agile DevSecOps practices, we provisioned our own development and testing environments, which were subsequently migrated into the enterprise ICAM authorization boundary.

Starting Point: Deploy SailPoint's IdentityIQ

A top priority for CLA was deploying IdentityIQ (IIQ), SailPoint's identity governance and administration solution. It was such a high priority that we were given just 30 days to provision and securely integrate the solution in preparation for an Authorization to Operate (ATO). That meant fully automating, wherever possible. To achieve this, we deployed a new SailPoint instance, standing up the infrastructure and deploying the latest version using GitHub for source control, and Terraform, an open-source infrastructure-as code (IaC) tool, to provision, manage, and version cloud infrastructure safely and efficiently. Automation included:

+ *Azure SQL instance and database with latest release of IIQ 8.3*
+ *KeyVault for managing secrets*
+ *VM image hardening (STIG) and patching procedures*
+ *Deploying infrastructure to support a static website for documents*
+ *Deploying infrastructure to support SailPoint IIQ*
+ *Deploying diagnostic settings to centralize logging into an operational and security log analytics workspace*

SailPoint IIQ was deployed to integrate HR systems with identity lifecycle orchestration of CLA's employees and contractors. At the 30-day mark, we successfully demonstrated automated provisioning of SailPoint with the security controls necessary to go into production, achieving a FISMA moderate ATO months after closing PO&AMs. It is worth noting that deploying to production within 30 days was a tremendous achievement by the Easy Dynamics team and made a spectacular first impression on the agency.

App Integrations and Technical SME Advisory & Support Services

To better protect CLA's IT resources, and to comply with FISMA and Executive Branch mandates, we tapped the agency's existing Entra ID licenses and utilized that platform's authentication services to integrate legacy applications typically accessed with weak authentication (i.e., via a username and password) to SSO requiring MFA. Initially, PIV cards and OTP tokens were supported; in 2024, we added additional phishing-resistant authentication via FIDO2 security keys and Windows Hello for Business, a requirement of OMB M-22-09.

As is typical with most large federal agencies, CLA had a combination of modern and legacy applications – along with a mix of COTS and custom applications – residing in different technology stacks, with server-side and client-side using different authentication protocols. While the infrastructure presented challenges, Easy Dynamics' extensive experience in federal ICAM enabled efficient delivery.

Application integration at scale requires a combination of technical subject matter expertise, effective communications for organizational change management, and policies that support the strategy. Through a series of meetings with CLA stakeholders, ISOs, and ISSOs, we gained an understanding of the agency's systems, applications, data, and end users. We provided technical subject matter expertise to ensure a smooth migration and minimize the impact to end users and the agency's mission.

While some stakeholders or their staff could perform the authentication and authorization coding required to integrate

their mission applications with Entra ID, many could not. To accelerate the process, Easy Dynamics developed reference implementations of the authentication plugins required, along with detailed instructions on how to configure the plugins for CLA's application teams. We also deployed technical resources to assist the mission program's team with app development and configuration, ensuring smooth integration with the agency's new ICAM service. This was a win-win for everyone.

Login.gov Integration

GSA's Login.gov is used for identity proofing external users, including partners and the general public, and supports OpenID Connect and SAML protocols. Because Login.gov does not provide tools for integration, our team tailored Entra ID's B2C starter pack to support the service.

At the time, Login.gov was not compliant at identity proofing at NIST Identity Assurance Level (IAL) 2, requiring our team to onboard external users at IAL1. However, Login.gov had its own set of profiles for each Authentication Assurance Level (AAL) and IAL, making it necessary to adapt its profiles to support external users. We used GitHub as a source repository and developed the IaC, which included unique policy-as-code for every IAL/AAL combination we might receive from Login.gov. Our integration of Login.gov with Entra ID also leveraged automation to support step-up authentication, requiring an initial one-time passcode when an authentication request was flagged as risky.

Migrating applications to SSO requires more than just technical experience and resources – it also requires a well-executed change management process, which Easy Dynamics also spearheaded for the agency to great success.

Conclusion

Modernizing CLA's ICAM ecosystem required a technically rigorous, standards-aligned implementation that addressed legacy fragmentation, security gaps, and scalability challenges. Easy Dynamics successfully stood up an enterprise-grade identity infrastructure by deploying SailPoint IIQ with full lifecycle automation in just 30 days – an extraordinary timeframe in the federal space.

Our team operationalized Entra ID beyond its limited Microsoft 365 scope, enabling enterprise-wide SSO and phishing-resistant MFA through PIV, FIDO2 security keys, and Windows Hello for Business in alignment with OMB M-22-09 and Zero Trust principles. We also executed complex application integrations across diverse stacks and protocols; our Login.gov integration for external users further extended the identity perimeter, while accommodating NIST's IAL and AAL profiles via Entra B2C custom policy-as-code deployments.

Through technical agility, automation, and direct engagement with CLA's system owners and developers, Easy Dynamics successfully delivered a secure, scalable, and extensible ICAM solution.

CONTACT US

Greg Gordon
Chief Delivery Officer
ggordon@easydynamics.com

JJ Harkema
VP Solutions & Partnerships
jharkema@easydynamics.com