SUCCESS STORY

EASY DYNAMICS℠

OUR COMPREHENSIVE APPROACH TO MFA ADOPTION YIELDS RESULTS

Easy Dynamics' strategy for expanding MFA adoption was key to helping a cabinet-level agency successfully meet its federal compliance targets.

Background

The Federal Information Security Modernization Act (FISMA) of 2014 mandates that federal agencies report their cybersecurity posture to ensure the security of information systems. The act mandates regular reporting to the Office of Management and Budget (OMB) and the Department of Homeland Security on cybersecurity performance metrics, including quarterly submissions by CIOs to demonstrate compliance with OMB policies and guidance. These quarterly submissions include 22 separate metrics regarding the level of adoption of multi-factor authentication (MFA) among the agency's portfolio of systems, including whether MFA implementations are phishing-resistant or not and whether the use of different forms of MFA are required or optional for different user communities, including federal enterprise identities and general public identities.

Phishing-resistant MFA is critical for securing online accounts and systems because it addresses the vulnerabilities that make traditional authentication methods, such as single-factor authentication (username/password) or non-phishing-resistant MFA (one-time-passcode via text/email), susceptible against phishing attacks. Per OMB M-22-09, phishing-resistant MFA is required for federal enterprise identity users (agency staff, contractors, and mission partners) and it must be available as an option for general public identity users.

While Personal Identity Verification (PIV) smart cards are required as the *primary* authentication method for federal civilian enterprise identities, they are not always available for use. General public users do not have access to PIV smart cards, and there are many circumstances in which they may be unavailable for federal enterprise users: they may expire, be lost, or become temporarily unavailable; a PIV card reader may stop working; or the user's device may not have a PIV card reader at all (e.g., a mobile device or tablet). To ensure the availability of phishing-resistant MFA in all these cases, we deployed multiple FIDO2 and Web Authentication-based authenticators to serve as alternate phishing-resistant MFA methods.

The Challenges

Historically, the data used for quarterly FISMA submissions was derived from information stored in the department's Governance Risk and Compliance (GRC) tool for each system, which presented several challenges:

Imprecise Data Capture.

Due to a lack of specific data fields to capture each metric, a significant number of responses had to be estimated.

Poor Data Quality.

We encountered data quality issues in the GRC tool, including missing data for some systems and incorrectly entered data for others.

Lack of Clarity.

System owners responsible for supplying information to the GRC tool didn't understand the questions asked for each metric, or know which categories to use for their system's authentication methods.

Our Solution

Easy Dynamics worked with the GRC tool support team to add custom fields that capture responses for each metric for every system. We provided several training sessions to educate system owners about the different types of authentication methods and practices, providing common examples and illustrating which categories they fell into for various metrics. Our team then published user help guides to explain each metric question in detail, with instructions for how to determine answers for their systems.

We also automated validation logic to quickly and accurately identify data errors. For example:

- *If the answer to question #3 is X, then the answer to question #7 can't be Y.*
- *If the system is integrated with the Enterprise ICAM system and utilizes Single Sign-On for authentication, then these questions should have these answers.*

We integrated these data fields directly from the GRC tool to the FISMA quarterly reporting tool to reduce time and errors associated with manual reporting. Our team proactively reaches out to system owners before each quarterly reporting period, reminding them to update these fields and correct any errors discovered in the validation logic.

The Measurable Benefits

- **Increased confidence** in accurate reporting; **drastically reduced reporting time** from 100s of man-hours to mere minutes using automation; and added traceability to **support audits**
- **Integrated 180+ applications and services** within the first two years to leverage Enterprise ICAM's **phishing-resistant MFA** services under a single management control plane via SSO
- **Improved MFA adoption and compliance** of the agency's system portfolio, from 55% at the end of FY23 Q1 to greater than 92% at the end of FY24 Q2 – **exceeding the 90% target** established by the White House Office of the National Cyber Director in FY23 Q3

CONTACT US

Greg Gordon
Chief Delivery Officer
ggordon@easydynamics.com

JJ Harkema
VP Solutions & Partnerships
jharkema@easydynamics.com

FEDERAL EXPERIENCE

- Department of Agriculture
- Department of Homeland Security
- Defense Information Systems Agency
- Defense Logistics Agency
- Naval Special Warfare Command
- Federal Law Enforcement Training Center
- National Institute of Standards and Technology
- Cybersecurity and Infrastructure Security Agency
- Internal Revenue Service
- General Services Administration
- Department of the Treasury
- Health & Human Services
- Social Security Administration
- Department of Education

CORE CYBERSECURITY CAPABILITIES

- ICAM
- Cloud Modernization
- Risk Management
- Automation & Resiliency