Phishing-Resistant Multi-Factor Authentication (MFA) Success Story: USDA's Fast IDentity Online (FIDO) Implementation

Publication: November 2024

Cybersecurity and Infrastructure Security Agency and
United States Department of Agriculture

Table of Contents

Executive Summary

The U.S. Department of Agriculture's (USDA's) over 130,000 employees have unique technical needs to do their work. Unlike most of the federal government, USDA cannot exclusively rely on personal identity verification (PIV) cards to authenticate, or prove, who employees are to access government systems. This is because the USDA has seasonal employees who cannot receive the same PIV credentials as full-time government employees due to security and administrative concerns. Further, some USDA employees work in lab environments that require decontamination procedures that the standard identification card cannot survive. These circumstances pushed USDA to develop a technical solution that provides the same protections as a PIV but withstands decontamination. Like a PIV, the solution needed to provide phishing-resistant authentication, allowing users to authenticate without the threat of malicious actors tricking them into supplying login credentials. Additionally, the ability to provide multi-factor authentication (MFA)[1] was a key requirement of the solution's success.

USDA turned to Fast IDentity Online (FIDO) capabilities, which its centralized technology architecture already supported, to address the challenge of finding an authentication solution to counter credential phishing threats. FIDO is a set of authentication protocols that uses cryptographic keys on user devices to offer a secure, phishing-resistant way to authenticate user identities—all without passwords. To date, this technology has allowed approximately 40,000 registered users, some of whom historically required PIV exemptions, to access USDA's network without introducing the risks associated with usernames and passwords.

This report details how USDA successfully implemented phishing-resistant authentication in situations where in the past only authentication methods vulnerable to phishing were feasible. Due to the adoption of a centralized model to manage Identity, Credential, and Access Management (ICAM), the ability to make incremental improvements, and knowledge of the use cases in need of address, USDA succeeded in implementing MFA. USDA encourages all organizations facing phishing-resistant authentication enforcement challenges, where PIV or other certificate-based authentication is not an option, review USDA's use of FIDO for guidance.

USDA'S MFA Use Cases

USDA had use cases for FIDO in two scenarios where staff did not have PIV cards. The first use case involved employees, such as seasonal workers, who were ineligible for a PIV card per the Office of Management and Budget's guidelines. Additionally, other workers did not have PIV cards because the process to issue the cards for eligible employees takes months.

Previously, USDA addressed this challenge by providing a waiver to issue employees a user ID and password. However, with the emergence of more sophisticated credential phishing campaigns, this became an unacceptable risk for USDA. Ultimately, USDA needed a phishing-resistant alternative to

[1] MFA is a security control that requires a user to present a combination of two or more different authenticators (i.e., something you know such as a PIN, something you have such as a PIV card or passkey, or something you are such as your fingerprint).

PIV card usage as many employees needed to access USDA's environment without a physical card at some point during their employment.

Why Are USDA'S MFA Use Cases Important?

USDA needed to implement a modern, phishing-resistant form of MFA that would work with their unique use cases to protect against the growing threat of phishing for credentials. Their decision to adopt FIDO highlights the importance of organizations moving away from using password authentication and, instead, adopting secure MFA technologies.

Not all MFA technologies provide equal protection. Forms of MFA vulnerable to common MFA bypass attacks include authenticator codes, short message service (SMS) codes, and push notifications. A malicious cyber actor can circumvent the MFA protections offered by one-time passwords (OTP) or SMS codes by tricking users into providing their codes. Another MFA bypass attack, known as push bombing (or push fatigue), involves a malicious cyber actor overwhelming users with push notification requests until they approve access. Fortunately for all organizations, FIDO adoption eliminates these forms of MFA bypass attacks. Authentication technologies that do not involve FIDO or public key infrastructure (PKI)—a security framework based on public key cryptography—to support confidentiality and integrity will only continue to put organizations at risk by allowing malicious cyber actors initial access to their networks via credential phishing attacks.

Solution

Notably, USDA was ahead of the curve in launching its own phishing resistance initiative before the U.S. government's publication of *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09[2], which included requirements for the federal government to implement phishing-resistant MFA.

To provide its initiative scope, USDA's ICAM Division first reviewed its password exemptions and waivers. Then, they identified specific, organizational use cases that posed the largest challenges. While the agency championed the use of PIV for many years, it needed a complementary alternative

[2] The Office of Management and Budget's Memorandum for the Heads Of Executive Departments and Agencies.

for users who were, for various reasons, unable to use a PIV card. USDA determined that a multifaceted solution was required to support desktop login, virtual private network (VPN) access, single sign-on (SSO) application access, and Microsoft Office access and authorization. By looking at employee IT usage, USDA further determined that enabling enforcement of phishing resistance for those four IT services addressed most of the user requirements.

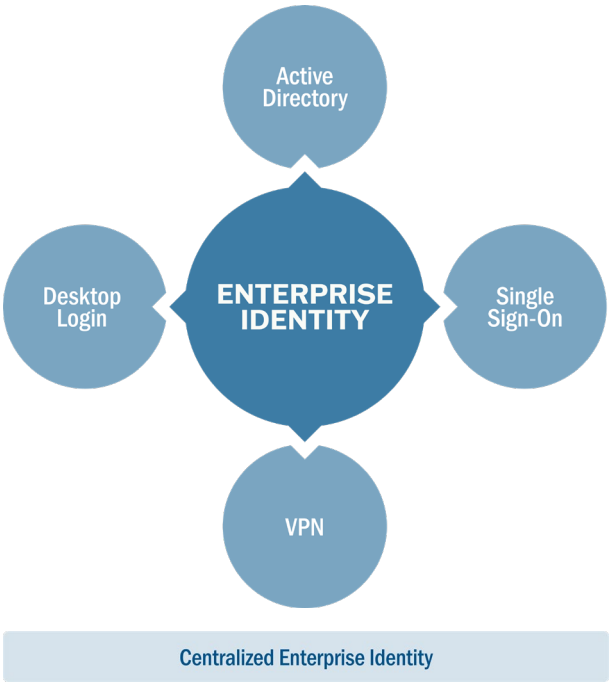
USDA had already implemented centralized authentication using an SSO platform to make enterprise updates more agile. It was also adopting hybrid cloud identity solutions, including Microsoft Entra ID, as it transitioned to software-as-a-service (SaaS) collaboration services. Having a centralized authentication and a hybrid cloud identity solution prepared USDA to adopt a FIDO authentication solution that was already available in Microsoft Entra ID.

In addition to understanding the importance of centralization and hybrid cloud identity solutions, USDA tracked identity industry trends to help inform them in their adoption of technical solutions. USDA's ICAM policy and engineering teams were aware of the growing threat of credential theft and the commercial capabilities phishing resistance afforded. Consequently, USDA was well-positioned to change their existing enterprise ICAM services to enforce phishing-resistant authentication for a large portion of their IT systems.

USDA was also active in the ICAM community and maintained relationships with industry vendors. This helped the agency stay informed of threats, mitigations, and best practices. One of the best practices USDA learned was how to use inherent phishing-resistant authentication in their Azure Active Directory (now Microsoft Entra ID) platform. USDA decided to make continuous and incremental changes to their enterprise services through pilots, accepting the cost of this decision in favor of agility and responsiveness.

USDA piloted two device-bound FIDO options that added phishing resistance to Windows authentication. The first was Microsoft's Windows Hello for Business (WHfB) solution, which leverages the device's Trusted Platform Module for hardware protection. The second was Federal Information Processing Standard 140 (FIPS-140) validated security keys. Both options offered phishing resistance with hardware binding that complemented PIV authentication. This enabled USDA to scale these capabilities to enforce phishing-resistant authentication for their four main enterprise services:

- Windows desktop logon
- Microsoft M365
- VPN
- Single Sign-On (SSO)



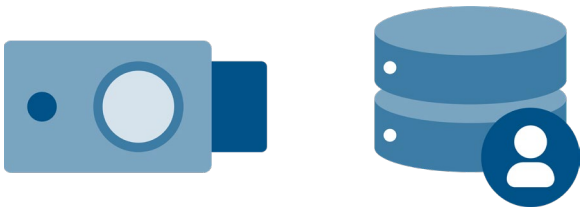
USDA's centralized architecture was instrumental in allowing them to quickly implement change. By enabling FIDO authentication in their SSO system, USDA protected over 600 applications from even the more advanced types of MFA bypass techniques.

By enabling FIDO authentication in their SSO system, USDA protected over 600 applications from even the more advanced types of MFA bypass techniques.

By focusing on FIDO and SSO, USDA advanced their ability to address future use cases. For example, workers in biocontainment facilities needed access to systems within the facility, but a PIV would not survive the physical decontamination required when leaving the facility. Because USDA supported FIDO, they piloted FIDO security keys that would support the mission and survive decontamination.

Providing credential lifecycle management for a non-PIV, non-PKI authenticator such as FIDO required a more holistic lifecycle management capability. USDA adopted its centralized human resources (HR) application as the source of truth for identity. The HR system provided:

- Authoritative identity lifecycle data on employees, including employees without PIV cards; and
- Allowed an automated mechanism for provisioning and deprovisioning:
  - WHfB credentials or security keys for those users, as well as their access to resources through accounts or groups.



FIDO + SSO

When internal users visited USDA's enterprise WebSSO solution (USDA eAuthentication), the login screen presented them with a new "USDA Work Account" option that redirected users to Microsoft Entra ID to authenticate. USDA used OpenID Connect to federate WebSSO with Microsoft Entra ID, which allowed USDA users to authenticate using their Microsoft account and access applications supported by WebSSO.

By integrating Microsoft Entra ID with the centralized WebSSO platform already serving more than 600 internal applications, USDA was able to incrementally deploy a FIDO capability and support both PKI and FIDO for the applications and services relevant to most users.

Each step was a logical progression that safely moved USDA towards phishing-resistant MFA for its entire user population.

Each step was a logical progression that safely moved USDA towards phishing-resistant MFA for its entire user population.

USDA's centralization will only continue to support its Zero Trust roadmap in the future by enhancing its access control capabilities. USDA will implement context-based access control included with the Microsoft Entra ID platform to centrally integrate risk signals and events[3] to make more granular access decisions and use them for monitoring by their security operations center.

Recommendations

Organizations need to understand the threat landscape's "new normal." Malicious cyber actors are continuously trying to trick unsuspecting users into providing their names, passwords, and 6-digit MFA codes. Ideally, organizations will focus their efforts on implementing solutions that defeat credential phishing attacks, like FIDO or PKI. USDA's technical solution to address gaps in phishing-resistant MFA is useful for any organization looking to overcome its ICAM-related implementation obstacles. These use cases also highlight fundamental programmatic strategies that increase the efficiency of large-scale evolutions, such as those required by Zero Trust Architecture. The organizational environment can either provide a supporting framework for evolution and innovation or cause inefficiencies related to unnecessary or arbitrary obstacles. The below subsections provide specific recommendations based on USDA's implementation of FIDO and lessons learned.

Embrace Centralization

USDA adopted a centralization principle across their enterprise by consolidating IT support, security operations, and IT infrastructure (including their ICAM systems) under their USDA Headquarters CIO's office. By centralizing their ICAM systems through an SSO platform and hybrid cloud identity solution, USDA provided better security and user management across the enterprise. This centralization was key to USDA's ability to rapidly deploy FIDO capabilities, closing gaps in phishing-resistant MFA use. Moreover, the tight collaboration between IT support, IT operations, and cybersecurity experts helped USDA mitigate common challenges (such as conflicting changes, implementation delays, and integration challenges) in large-scale deployments, as well as risks associated with consolidation.

Make Incremental Improvements

USDA has an organizational philosophy of "always be piloting." In an enterprise as diverse and complex as USDA, it is essential to continuously learn about new solutions to meet requirements.

[3] The outputs from cybersecurity sensors and tools.

Because of USDA's diverse operational requirements, it is unlikely to find one solution for everyone. Pilot programs that support incremental change, instead of making sweeping changes, mitigate risk by adding lessons learned during the piloting process.

Always be piloting.

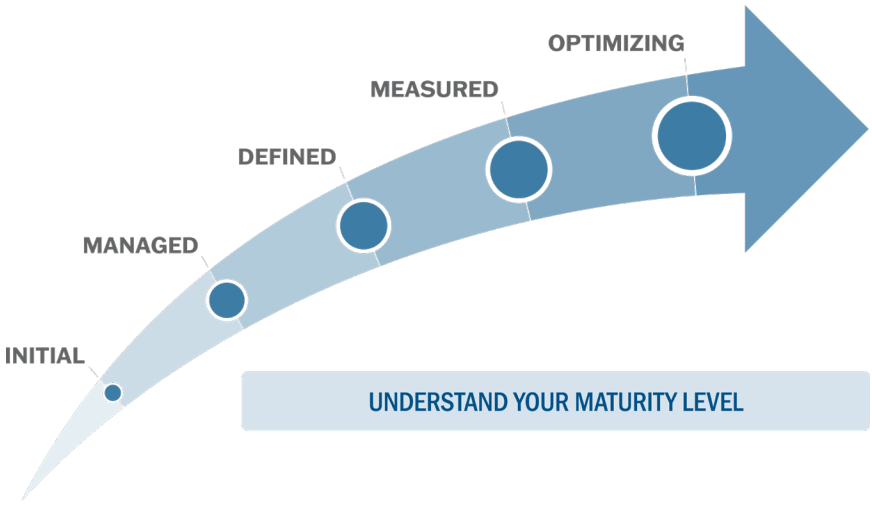
Considerations for incremental piloting include careful selection criteria, such as:

- Choosing groups performing non-critical functions;
- Possessing a stable and standard IT environment;
- Using groups where potential implementation issues would only impact a smaller population; or
- Choosing a technically mature group that has experience quickly mitigating implementation issues.

Organizations can use lessons learned from these piloting efforts in other pilot programs until they develop a proven implementation plan.

Understand Your Maturity Level

Change management is challenging enough, but controlling change in an inconsistent operational environment will likely lead to pain points. Organizations striving to implement large-scale change should first work to ensure, at a minimum, they document relevant processes and consistently implement them. USDA had a well-defined baseline for its enterprise and has since invested in continuous improvement, helping leaders understand and manage risk.



Understand Your Environment and Use Cases

USDA leveraged its existing SSO platform to enable FIDO authentication methods that provided two phishing-resistant authentication solutions for users without PIV cards. By focusing on FIDO and SSO, USDA was able to address its phishing-resistant MFA requirements for most of their users. While the technical solutions may vary, organizations should be able to adapt the methodology USDA used in determining its operational requirements to nearly any environment.

Organizations should prioritize implementing phishing-resistant MFA across their enterprise. For many organizations, there may be barriers to achieving this due to specific employee or technology use cases. Despite similar challenges, USDA was able to use FIDO to provide phishing-resistant authentication when PIV cards were not an option. Embracing centralization and continuous, incremental improvement was critical in USDA's success. Any organization looking for ways to resolve MFA implementation challenges will benefit from USDA's experience and lessons learned.

Organizations should prioritize implementing phishing-resistant MFA across their enterprise.

Resources

[1] CISA Blog: Phishing: What's in a Name?

[2] CISA Blog: Phishing Resistant MFA is Key to Peace of Mind

[3] CISA's Implementing Phishing-Resistant MFA

[4] CISA's Zero Trust Maturity Model

[5] FIDO Alliance

[6] Catching the Big Fish: Analyzing a Large-Scale Phishing-As-A-Service Operation

[7] Windows Hello for Business (WHfB) Playbook