U.S. Department of Transportation
Office of the Chief Information Officer

Memorandum

Subject: **ACTION: ITIM 2022-006** U.S. Department of Transportation Implementation Guidance for Multi-Factor Authentication for Users of Information Systems and Applications

Number: ITIM-2022-006

From: Andrew R. Orndorff
Associate CIO /
Strategic Portfolio Management and
Chief Information Security Officer

ANDREW R
ORNDORFF

Digitally signed by
ANDREW R ORNDORFF
Date: 2022.07.08 16:32:44
-04'00'

To: Component IT Directors
Component Chief Information Officers
Component Chief Information Security Officers
Component Information System Security Managers

CC: Office of the Senior Procurement Executive

I. SCOPE

This Information Technology Implementation Memorandum (ITIM) applies to all Department of Transportation (DOT) Components[1] that expend funds to develop, operate, maintain, and/or enhance information technology (IT) systems and applications which support or further the mission of DOT.

The purpose of this memorandum is to provide requirements and strategies for the consistent and uniform implementation and enforcement of Multi-Factor Authentication (MFA) for user access to DOT networks, systems and applications in alignment with Federal Zero Trust requirements and principles. MFA for device and application-to-application authentication is outside the scope of this ITIM and will be addressed in subsequent guidance.

The Federal Aviation Administration (FAA) Chief Information Officer (CIO) has responsibility for overseeing and implementing the relevant Federal MFA and Zero Trust requirements within the FAA, and this action memo applies to the FAA only to the extent that such requirements and recommendations are consistent with the language contained in the FAA authorization statutes, FAA General Procurement Authority, and FAA Air Traffic Control Modernization Reviews (49 U.S.C. §§ 106, 40110, 40121).

II. INTRODUCTION

[1] Component has the meaning established in DOT Order 1351.A, IT Policy Management, and refers to all DOT Operating Administrations, the Office of the Secretary of Transportation, and the Office of the Inspector General.

The issuance of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, and Office of Budget Memorandum (OMB) memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (Federal Zero Trust Strategy)*, places renewed emphasis and attention on strengthening identity and authentication. It also requires that agencies eliminate weaker forms of identity and authentication, and transition to stronger, impersonation- and phishing-resistant multi-factor authentication as part of an overall plan for implementing zero trust within agency networks, systems, and applications.

A key tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, every attempt to establish access must be verified to secure the related network, system, application, and data. This verification must occur at the beginning of, and continuously throughout, access to a system or application, and may require reauthentication as a measure to mitigate risk, or limitation or denial of access in the event of undue risk. This strategy places significant emphasis on stronger enterprise-managed identity and access controls, including MFA. Secure, enterprise-managed identity functions improve agency control over networks, systems, applications, and data, and enhance protection of stakeholder information.

III. DEFINITIONS

- **Authentication:** The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.
- **Enterprise-facing:** Intended for use by agency staff, contractors and partners[2].
- **Enterprise-facing Identities:** Identities and accounts attributable to agency staff, contractors, and partners that require a strong form of phishing-resistant MFA, to include PIV, CAC, PIV-I, agency-approved FIDO2 credentials, and other agency-approved forms of strong MFA.
- **Enterprise-managed Identities:** Identities and accounts attributable to agency staff, contractors, and partners, and provisioned, stored, and managed in agency enterprise identity systems.
- **Multi-Factor Authentication:** An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know (e.g., PIN #), something you have (e.g., PIV Card), and something you are (e.g., biometric such as a fingerprint).
- **MFA Enabled:** Multi-Factor Authentication is available, but not enforced.
- **Phishing-Resistant MFA:** Phishing-resistant MFA cannot be compromised by even a sophisticated phishing attack. This means that the MFA solution cannot have anything that can be used as a credential by someone who stole it, including, but not limited to passwords, one-time passcodes (OTP), security questions, and push notifications.
- **Partner:** The term "partners" is meant to include users that are external to the agency, but whose use of agency systems requires a strong form of MFA. For example, this category could include Government contractors submitting financial information, or personnel in another agency accessing a shared system or service.
- **Public-facing:** Intended for use by the public, and/or non-federal agency stakeholders.

[2] OMB M-22-09, page 7

- **OpenID Connect[3]:** An identity layer built on top of the OAuth 2.0 protocol that allows client systems and applications to verify the identity of a user based on authentication performed by an authorization server, as well as obtain basic profile information about the user in an interoperable manager.
- **SAML:** Security Assertion Markup Language is an open standard used for authentication that supports the exchange of authentication information between entities, typically an identity provider and a service provider.

IV. REQUIREMENTS

The following requirements must be met for MFA compliance for networks, systems, applications or users:

1. All DOT networks, to include, but not limited to, sub-networks, component networks, virtual private networks (VPN), data and telephony circuits, Voice Over Internet Protocol (VOIP) networks, must enforce MFA for access.
2. All DOT systems, subsystems and applications must enforce MFA for access wherever credentials and authentication are required.
3. All DOT systems, subsystems and applications must enforce MFA for all users including privileged users, role-based users, external users (where credentials and authentication are required) and internal users. MFA must be enforced at the overall system and all system subcomponents/modules/interfaces to be considered compliant.
4. All users (e.g., employees, privileged account users, detailees, interns) accessing DOT's network and systems, must use DOT OCIO approved MFA compliant mechanisms (e.g., such as a PIV card, Temporary "T" Card, logical access card (LAC), or software-based MFA mechanisms such as Login.gov or MAX.gov).
5. All mobile devices accessing DOT networks, systems, and applications must enforce Phishing - Resistant MFA.
6. Networks and, systems, and applications systems that enable, but do not enforce, MFA are **not compliant**.
   a. MFA-enabled systems allow users to bypass MFA by using a single authentication factor, e. g., use of username/password and an answer to a secret questions together are all the same factor – something you know.
7. Temporary exceptions to MFA usage must be limited, kept to a minimum, and made only on a case-by-case basis (e.g., user forgot Personal Identity Verification (PIV) card at home or PIV card is damaged) and tracked regularly to prevent extensive time frames for excepted users.
   a. Systems that permit temporary exceptions must clearly state so in system security plans and operational documentation, along with the criteria used to grant temporary exceptions and the duration of the exception(s).
8. The MFA requirement is applicable for all system sensitivity levels.
9. Requests for approval of non-compliant MFA networks or systems must be submitted to the DOT CIO via e-mail to ITRiskmanagement@dot.gov.
10. Components should expect that users may be required to reauthenticate to systems and

[3] https://openid.net/connect/

applications at system and application boundaries or whenever there is an evaluation of risk as part of a mature implementation of zero trust architectural principles[4], even if previously authenticated to the DOT network or DOT single-sign-on (SSO) or enterprise identity systems.

11. Components are responsible for ensuring continuous enforcement and use of MFA by their personnel, contractors, partners, and stakeholders for all personnel, networks, systems, applications, and devices within their purview.

V. REQUIRED ACTIONS

1. DOT OCIO requires all networks to be MFA compliant by **December 31, 2022**, and systems to be MFA compliant by **December 31, 2023**.
2. Within 30 days of the date of signature of this ITIM, Components must:
    1. Evaluate their systems to determine compliance with the requirements for enforcement of MFA for user authentication:
        - i. A system is **fully** compliant if:
            1. Enterprise-facing identities are Enterprise-managed and authenticated with both unprivileged and privileged access requiring mandatory use of a PIV or PIV-I card, CAC, or DOT-approved Phishing-Resistant MFA for access. Enterprise-facing interfaces of the system or application must also employ one or more appropriate, approved MFA solutions from the Standard.
            2. Partner Enterprise-facing identities require mandatory use of a PIV or PIV-I card, CAC credential, or DOT-approved Phishing-Resistant MFA for authentication and unprivileged and privileged access to Enterprise-facing interfaces of the system or application, employing an appropriate, approved MFA solution from the Standard.
            3. Public-facing access and authentication require mandatory use of an appropriate, approved MFA solution from the Standard.
        - ii. All other systems and applications not meeting the requirements of Sections V.2.1.i are **not** compliant and require a full corrective action plan and remediation.
            1. If a system employs Microsoft ADFS or the MyAccess enterprise service and meets the other requirements of Section V.2.1.i(1), above, the corrective actions and compliance plan should reflect either adoption of the replacement/modernized service(s), or migration to one or more of the other approved MFA solutions from the Standard.
    2. Provide a Component-wide MFA compliance plan that details a schedule per system with proposed solution(s) for bringing each system into full MFA compliance leveraging solutions from the Standard. Plans must be submitted in electronic form via e-mail, using the template provided, to CyberPMO@dot.gov.
3. Components must engage DOT OCIO immediately if the Component identifies a system that cannot be fully compliant by end of calendar year 2023.

[4] OMB M-22-09, page 9

VI. REFERENCES

a) DOT Order 1351.39A, *Information Technology Management*, August 3, 2017; https://www.transportation.gov/sites/dot.gov/files/docs/dotorders/DOT1351.39A_Information%20Technology%20%28IT%29%20Management%20Policy_3-Aug-17.pdf

b) DOT Order 1351.37, *Departmental Cybersecurity Policy*, July 7, 2011; https://usdot.sharepoint.com/sites/CIOITPolicy/Shared%20Documents/DOT%20Order%201351.37,%20Departmental%20Cybersecurity%20Policy.pdf?CT=1656612644938&OR=ItemsView

c) Office of Management and Budget (OMB) Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019; https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

d) Executive Order 14028, *Improving the Nation's Cybersecurity;* May 12, 2021; https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

e) Office of Management and Budget Memorandum 22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022; https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

f) *Digital Government Strategy - Building A 21st Century Platform To Better Serve The American People*., May 23, 2012; https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

VII. EFFECTIVE DATE

This ITIM is effective as of the date of signature and remains in effect until canceled,amended, or replaced by updated guidance or instruction.

VIII. CONTACT

For questions regarding this memorandum, please contact the OCIO Office of Strategic Portfolio Management at ITRiskmanagement@dot.gov.

U.S. Department of Transportation (DOT)
STANDARD

Approved Multi-Factor Authentication (MFA) Solutions

Version	Date	Description	Approver
1.0	2022/06/30	Initial Release	Andrew R. Orndorff

APPROVED:

ANDREW R ORNDORFF

Digitally signed by ANDREW R ORNDORFF
Date: 2022.07.08
16:33:24 -04'00'

Andrew R. Orndorff

Associate CIO/SPM and CISO

INTRODUCTION

This standard provides guidance on acceptable MFA solutions that may be deployed for immediate use within DOT's information technology environment. As additional solutions are evaluated and determined to meet DOT's functional and technical requirements, this standard will be updated.

DOT's current MFA solution portfolio/architecture consists of:

Solution[i]	Supports	Best for Use Cases
Microsoft Active Directory (AD) / Microsoft Active Directory Federation Services[ii] (ADFS)	SAML OpenID Connect	DOT federal, contractor, and other badged personnel accessing agency networks, systems, and applications Customers of the DOT Common Operating Environment (COE) operated by DOT OCIO
Microsoft Azure AD, Azure AD SSO, and Azure B2B	SAML OpenID Connect	DOT federal, contractor, and other badged personnel accessing agency networks, systems, and applications Customers of the DOT Common Operating Environment (COE) operated by DOT OCIO
GSA Login.gov	SAML OpenID Connect	Non-DOT, public/external stakeholders – e.g., citizens, State, Local, Tribal and Territorial (SLTT) entities, private-sector/industry

Solution[i]	Supports	Best for Use Cases
SailPoint and CyberArk[iii] with integration of personnel security	IAM and PAM/Password Vault Credential and privilege management	DOT Systems for CRED, PRIV, TRUST and BEHAVE DOT federal, contractor, and other badged personnel accessing agency networks, systems, and applications Customers of the DOT Common Operating Environment (COE) operated by DOT OCIO
MAX Portal/Services	SAML	Partners accessing DOT systems and applications Government-to-Government authentication Interagency and Government Federation use cases
DOT MyAccess[iv]	SAML OpenID Connect	DOT federal, contractor, and other badged personnel accessing agency systems, and applications

ACRONYMS

Acronym	Definition
AD	Active Directory (Azure or Microsoft)
ADFS	Active Directory Federation Services
CIO	Chief Information Officer
COE	Common Operating Environment
DOT	Department of Transportation
IAM	Identity Access Management
IT	Information Technology
LAC	Logical Access Cards (issued for select Use Cases to enforce MFA)
MFA	Multi-Factor Authentication
OCIO	Office of the CIO
OTP	One Time Password
PAM	Privilege Access Management
PIV	Personal Identity Verification
SAML	Security Assertion Markup Language
SLTT	State, Local, Tribal and Territorial governments
SMS	Short Message Service
SSO	Single Sign-On

[i] Any proposed solution not in the Standard must be coordinated with and approved by the DOT OCIO. Proposed solutions should be submitted via e-mail to ITSpendApproval@dot.gov and CC CyberPMO@dot.gov.

[ii] Microsoft ADFS is a retiring/deprecated service for which Microsoft recommends Azure AD as a modern replacement.

[iii] SailPoint and CyberArk are in development as enterprise capabilities available in FY2023.

[iv] DOT MyAccess is a current DOT enterprise solution undergoing modernization and it is expected to be fully compliant with Federal MFA requirements. Systems already using MyAccess need not transition to another solution unless system business or mission requirements warrant a different solution. Systems not already using MyAccess may choose to do so.