United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

April 20, 2021

Memorandum

To: Bureau and Office Associate Chief Information Officers

From: Deborah (June) Hartley
Chief Information Officer (Acting)
Office of the Chief Information Officer

DEBORAH HARTLEY Digitally signed by DEBORAH HARTLEY
Date: 2021.04.20 14:51:48 -06'00'

Subject: Alternative Multi-Factor Authentication Service

Purpose:
This memorandum rescinds the Office of the Chief Information Officer (OCIO) memorandum titled "Implementation of Alternative Multi-Factor Authentication Service", dated April 27, 2020, and provides updated guidance regarding Microsoft (MS) Authenticator. MS Authenticator is the replacement tool for the enterprise-wide Alternative Multi-Factor Authentication (AMFA) service.

This memorandum augments OCIO Directive 2016-006, "Strong Authentication Exception Policy", dated November 7, 2016. Effective immediately, all remote access exceptions must use the AMFA service rather than using username and password.

Background:
In April 2020, the OCIO implemented the initial operating capability for the AMFA service, using Symantec Validation and Identity Protection (SVIP). The SVIP toolset was a temporary solution and is now being replaced with MS Authenticator.

Effective Date:
This policy is effective immediately. All existing SVIP Users should be transitioned to MS Authenticator prior to April 30, 2021, after which the SVIP service will be turned off.

Authority:
OMB Memorandum M-19-17: Enabling Mission Delivery through Improved Identity, Credential and Access Management

Scope:
This memorandum authorizes the use of MS Authenticator as the AMFA risk-managed service for U.S. Department of the Interior (DOI) users that require network access but cannot obtain a DOI Access Card due to lack of USAccess station availability or who are having other technical difficulties with their existing DOI Access Card.

Policy:
The AMFA service provides a risk-managed, proven alternative for accessing DOI systems when personnel do not have, cannot get, or cannot use their DOI Access Card. Without this alternative, users would be denied access since the use of UserID and Password is no longer allowed as an

alternative authentication method. The loss of access presents unacceptable mission and productivity risk. The OCIO reviewed a variety of alternatives and determined that the AMFA method is the best alternative for ensuring that DOI systems remain cyber-secure under current operating conditions. The DOI Access Card provides the highest level of security for accessing DOI systems and remains the required method for accessing our systems when available. Users must restore or obtain a replacement DOI Access Card as soon as possible.

The MS Authenticator tool has a mobile client platform only and is not available for installation on DOI government-furnished laptops. Therefore, the mobile client is authorized for installation use for the purposes of AMFA token generation on both government-furnished mobile devices, and personally owned mobile devices, if needed. The risk of allowing use of personally owned mobile devices to be used for generating the AMFA token is deemed low and does not introduce any new risks to the environment. Using MS Authenticator on a personally owned device for the purpose of AMFA, does not in any way imply authorization or authorize the user to attempt to synchronize or download their government email and calendar directly to their personally owned mobile device. Use of the MaaS360 Secure Container remains the only authorized solution for synchronizing government email and calendar on a personally owned mobile device.

Roles/Responsibilities:

1. DOI Users:
    a. Monitoring the expiration status of both the DOI Access Card itself, and the associated digital certificates.
    b. Exercising due diligence to take appropriate action to obtain or correct any DOI Access Card issues.
2. Bureau and Office IT Service Desk Managers:
    a. Disseminating the attached configuration guidance and user login instructions.
    b. Managing and monitoring the associated bureau-managed security group which allows access to the Pulse Secure remote access system using AMFA.
    c. Coordinating with bureau Identity, Credentialing, Access and Management leads to implement an internal review and approval process.
    d. Submitting requests to the BisonConnect Support Team for Azure One Time Passwords, when needed.
3. OCIO Enterprise Services Division:
    a. Distributing technician configuration guidance and user instructions (Attachments 1 and 2) to all ACIOs and IT service desk managers for immediate implementation within their respective bureaus and offices.
    b. Processing Azure One Time Password requests on a timely basis.

Please contact Martha Eichenbaum at martha_eichenbaum@ios.doi.gov with any questions regarding this memorandum.

Attachments:

1. MS Authenticator and Pulse Secure Configuration (for Technicians)
2. MS Authenticator VPN User Login Instructions

cc: Assistant Secretary – Policy, Management and Budget
OCIO Core Leadership Team
Bureau and Office IT Service Desk Managers