United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

August 26, 2022

Memorandum

To: Heads of Bureaus and Offices
Associate Chief Information Officers

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

DEBORAH HARTLEY Digitally signed by DEBORAH HARTLEY
Date: 2022.08.26 15:46:58 -06'00'

Subject: Implementation of Multi-Factor Authentication using Phishing-Resistant Credentials Directive

Purpose

This policy directive requires the Department of the Interior (Department, DOI) bureaus and offices to complete the full implementation of phishing-resistant multi-factor authentication (MFA) by the end of Fiscal Year (FY) 2024.

Background

In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, initiating a government-wide effort to migrate the Federal Government to a zero trust architecture. The Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, dated January 26, 2022, reinforced the transition to a zero trust approach while placing a significant emphasis on stronger enterprise identity and access controls, including phishing-resistant MFA. In response to OMB M-22-09, the Department issued Office of the Chief Information Officer (OCIO) Memorandum, *DOI Zero Trust Strategy Implementation Plan* dated March 28, 2022, which directs bureaus and offices to ensure existing applications are enabled to use the Department's approved phishing-resistant MFA services.

The majority of DOI's systems and applications use DOI's enterprise solution to enforce MFA; however, there are several information systems where MFA has not been implemented due to budgetary, technical, and operational constraints. While the Department recognizes these challenges, it can no longer accept the risk of relying on password-based authentication for these systems and applications.

Policy

Bureaus and offices must enforce MFA through the Department's approved phishing-resistant MFA services for all information systems. Bureaus and offices must complete system modernization or replacement of information systems to ensure compatibility with one of the Department's approved MFA services by the end of FY 2024. If bureaus and offices are unable

to meet the FY 2024 deadline, then they must create a Plan of Actions and Milestones (POA&M) that details MFA implementation plans, milestones, and costs. If a POA&M is required, the POA&M must be closed by the end of FY 2025.

Scope

This directive applies to the development, operation, and maintenance of all Departmental information systems, whether externally hosted, or managed by DOI, regardless of funding source. Information systems whose funding is appropriated or collected from partner agencies, states, local government, or grants, are within scope of this directive.

Roles and Responsibilities

A. Bureau and Office Associate Chief Information Officers (ACIOs)
   - The ACIOs must coordinate with their Bureau and Office Directors to:
     - Support the Department's future zero trust and MFA goals;
     - Identify information systems that require modernization or replacement to ensure compatibility with the Department's services; and
     - Gain support for modernization or replacement of information systems where required to support MFA.

   - The ACIOs must coordinate with their information technology (IT) staff to:
     - Plan the integration of existing mission/business systems with an approved MFA logon solution;
     - Require MFA for all new or future systems and applications;
     - Leverage login.gov for web services where public logon is required; and
     - Support the future technical solution(s) associated with MFA by allowing for bureau or office participation in various zero trust architecture strategy and technical working groups.

B. The Office of the Chief Information Officer (OCIO) shall:
   - Sponsor strategy teams and working groups to provide the foundational policies and procedures, and a clear and consistent direction for the enterprise implementation of MFA;
   - Identify any gaps that may prevent the Department from achieving 100% adoption of phishing resistant MFA by the end of FY 2025;
   - Evolve the MFA strategy as the Department migrates to cloud technologies; and
   - Ensure that future MFA technologies are unobtrusive and enable mission stakeholders to simply and securely access DOI information and information.

Effective Date

This policy directive is effective immediately until further notice.

Authorities and References

A. Federal Information Technology Acquisition Reform Act (FITARA) of 2014

B. Executive Order 14028, Improving the Nation's Cybersecurity and the Federal Information Security Modernization Act (FISMA) of 2014

C. Office of Management and Budget (OMB) Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles"

Points of Contact

Please direct questions regarding this policy directive to Jay McMaster, Acting DOI Chief Information Security Officer, at Jay_McMaster@fws.gov.

cc: Bureau and Office Deputy Directors
Cyber Security Leadership Team
Portfolio Management Leadership Team