United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

NOV 0 7 2016

OCIO Directive 2016 - 006

To: Associate Chief Information Officers

From: Sylvia Burns
Chief Information Officer

Subject: Strong Authentication Exception Policy

Purpose

The purpose of this Directive is to establish a limited set of Personal Identity Verification (PIV)/2-Factor exceptions that bureaus and offices can use when it is not possible to meet the requirement for PIV/2-Factor authentication outlined in the *Email Message from CIO Sylvia Burns; Date: June 15, 2015; Subject: Enhancing and Strengthening DOI's Cybersecurity Posture*. This Directive will ensure exceptions to PIV/2-Factor authentication (hereafter referred to as Strong Authentication) are granted and managed consistently across the Department of the Interior ("Department" and "DOI" are used interchangeably throughout this document) and minimize the risks associated with extended use of user identification (userid) and password for access.

Background

On March 31, 2011, the Assistant Secretary for Policy, Management and Budget memorandum required use of Strong Authentication as the common means of authenticating to facilities, networks and information systems within the Department of the Interior. At the end of 2014, the White House and Office of Management and Budget (OMB) issued *Cross Agency Priority Cybersecurity Goals for Strong Authentication*, which expedited the rollout and enforcement of Strong Authentication throughout the Department. DOI met and surpassed OMB's Strong Authentication goals during the 2015 CyberSprint, when Office of the Chief Information Officer (OCIO) issued the June 15, 2015 memorandum to immediately expedite enforcement of PIV/2-Factor authentication by taking these actions:

- Enforce PIV/2-Factor authentication for remote access (expressly rescind all two-factor authentication waivers and exceptions previously granted)
- Enforce PIV/2-Factor authentication for users at the machine level using Active Directory (AD) Group Policy
- Enforce use of PIV/2-Factor authentication for all regular and ***privileged*** users

Policy

Bureaus are required to enforce Strong Authentication as outlined in the June 15, 2015 memorandum. This directive establishes approved Strong Authentication exceptions, defined in Attachment "A", that address all expected scenarios when Strong Authentication is not possible. Risks associated with userid and password authentication must be minimized by limiting the time for the exception to the minimum time needed to fix the problem, and by enforcing strong authentication as soon as the issues have been resolved.

Private sector employees and contractors, non-DOI personnel, and other members of the public who require access to DOI training computers will be allowed to authenticate only to local accounts, specifically configured as a training account. Strong authentication is not required for this case, provided the computers being used are isolated, either physically or logically, from DOI network resources (e.g. using an Internet only Virtual Local Area Network (VLAN)).

Exceptions

Strong Authentication Exceptions are ***not*** allowed for privileged account holders, shared accounts, or for any form of remote access through Virtual Private Network (VPN), or unrestricted Virtual Desktop Infrastructure (VDI) access:

- Privileged Account Holders - A privileged user who cannot use their DOI Access Card will temporarily have their privileged access suspended until the issue is resolved. Strong Authentication exceptions for Privileged Account holders can be approved by the ACIO for emergency or extenuating circumstances only.

- Remote Access - All remote access users must use Strong Authentication for authentication, per *Email Message from CIO Sylvia Burns; Date: June 15, 2015; Subject: Enhancing and Strengthening DOI's Cybersecurity Posture.*

- Shared Accounts - All Shared account holders who cannot use their DOI Access Card will temporarily have their access suspended until the issue is resolved. Note: Shared accounts shall use certificate mapping with all users of the accounts having their certificate mapped to the account.

Responsibilities

This policy supersedes all bureau and office strong authentication exception policies. Bureaus and offices are required to update their current Strong Authentication exception policies to comply with this policy; this includes termination of all existing strong authentication exceptions not addressed by this policy.

Bureaus and offices must be able to create reports showing how many exceptions have been granted for each exception type listed in the Short-term Exception Table in Attachment "A".

Effective Date

This Directive is effective immediately and maintained in effect until further notice.

Points of Contact

Questions regarding this Directive should be directed to the bureau Logical Access Working Group (LAWG) member. If questions are still unresolved, the LAWG member should contact Judy Snoich at (703) 648-5623 or judith_snoich@ios.doi.gov.

cc: Associate Chief Information Security Officers
Bureau Logical Access Working Group members

Attachment (A): Strong authentication exceptions for unprivileged Employees, Contractors and Associates
(B): Email Message from CIO Sylvia Burns; Dated June 15, 2015; Subject: Enhancing and Strengthening DOI's Cybersecurity Posture