

Strong Authentication Exceptions for Unprivileged Employees, Contractors and Associates

Long Term Exceptions - The Associate Chief Information Officer (ACIO) may grant a long term exception to unprivileged network users who work outside the continental United States, Alaska or Hawaii (for example, in a foreign country, on an offshore oil platform or research vessel) and whose existing Department of the Interior's Access Card (DOI Access Card) or certificates have expired. The length of the strong authentication exception is equal to the time period the employee is working outside the United States, or until the user can return to the United States to receive and activate a new card, whichever is less. Bureaus must take reasonable actions to ensure these users' DOI Access Card will not expire before the next anticipated return or travel to the United States for replacement. This includes issuing a new DOI Access Card or updating certificates prior to departing the United States.

Short Term Exceptions - A short term exception may only be granted for one of the scenarios listed in the table below. The exception shall be removed on or before the maximum allowed duration, and strong authentication re-enforced as soon as the issue is resolved. If an unprivileged user requests additional time, the ACIO may request the DOI Access Card's Sponsor to review the user's record to ensure all steps to correct the DOI Access Card issues have been completed. Requests to extend Short term Exceptions beyond the designated Maximum Duration should be reviewed and granted by the ACIO, to ensure no more than two consecutive exceptions have been allowed.

Category	Scenarios	Maximum Duration
No Card	New hire waiting for card to be delivered.	7 calendar days
No Card	Card left at home - user not on travel.	24 hours
No Card	Card left at home - user on travel.	7 calendar days
No Card	Card lost or stolen - Reprint required.	7 calendar days
Card Not Working	Card locked/blocked – Personal Identification Number (PIN) reset required and Activation station not readily available (if an activation station is readily available, only a 24 hour exception is authorized)	7 calendar days
Card Not Working	Defective or malfunctioning card - Reprint required.	7 calendar days
Card Not Working	Certificates expired and card terminated.	7 calendar days
Card Not Working	PIV logon not working for helpdesk personnel using remote network authentication (e.g. Remote Desktop Connections)	24 hours
Card Not Working	Credential status was updated from Suspended to Active – Certificate Revocation List (CRL) has not yet been updated to reflect certificate status.	48 hours
Equipment Not Working	Full-time telework user unable to use their Government Furnished Equipment (GFE) computer and require a replacement system be shipped to them.	7 calendar days
Equipment Not Working	Defective or malfunctioning card reader.	7 calendar days