



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
INSTALLATION MANAGEMENT COMMAND  
HEADQUARTERS, UNITED STATES ARMY GARRISON  
PICATINNY ARSENAL, NEW JERSEY 07806-5000



IMNE-PIC-ZA

7 March 2011

MEMORANDUM FOR RECORD

SUBJECT: Mandate to Enforce CAC Only Login vs. CAC / Username and Password

1. Purpose: To detail the implications of enforcement of the AR 25-2 requirement stating all users to login via CAC vs. login via CAC or Username and Password
2. Scope: This applies to all tenant organizations and employees at Picatinny Arsenal.
3. Reference: Army Regulation 25-2, Information Assurance, 23 March 2010 sections:
  - (1) 4-5c(6): Validate that systems authenticate users through the use of the CAC as a two-factor authentication mechanism. The CAC has certificates on the integrated circuit chip (ICC), and will be used as the primary user identifier and access authenticator to systems.
  - (2) 4-5c(7): Validate system configurations to authenticate user access to all systems with a minimum of a USERID and an authenticator when the systems are incapable of CAC enablement until these are replaced.
  - (3) 4-12a: Implement two-factor authentication techniques as the access control mechanism in lieu of passwords. Use CAC as the primary access credential, or biometric or single-sign on access control devices when the IS does not support CAC.
4. Background: Formerly, Picatinny users were required to login via CAC, however, they were also allowed to temporarily login via their NAE domain username and password if they either had not received a CAC yet, or did not have their CAC that day. Effective 7 February 2011, the NEC will be strictly enforcing the Army's policy so as to require users to always login via their CAC. This will bring Picatinny Arsenal into alignment with cyber security practices Army wide.
5. Details: Any Picatinny employee who is unable to login to the NAE Domain via their CAC (e.g. does not have a CAC yet, forgot CAC at home that day, lost their CAC) will NO LONGER

IMNE-PIC-ZA

SUBJECT: Mandate to Enforce CAC Only Login vs. CAC / Username and Password

be allowed to login via their username and password. If the employee is unable to perform any of their normal duties, one of the following actions must be taken:

a. Remain at work and perform duties not requiring computer access as specified by their manager/supervisor

b. Return home, retrieve their CAC and return to work. The employee shall either:

(1) take leave (annual, comp time, LWOP) for the time away from the office

(2) shift their duty hours accordingly.

6. All choices related to this MUST be approved IN ADVANCE by the employee's manager/supervisor.

  
HERB KOEHLER  
LTC, LG  
Garrison Commander