



UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

APR 16 2020

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF  
DEFENSE  
SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
CHIEF OF THE NATIONAL GUARD BUREAU  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR OF COST ASSESSMENT AND PROGRAM  
EVALUATION  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR OF OPERATIONAL TEST AND EVALUATION  
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF  
DEFENSE  
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE  
AFFAIRS  
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC  
AFFAIRS  
DIRECTOR OF NET ASSESSMENT  
DIRECTORS OF DEFENSE AGENCIES  
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Exception to Policy Allowing the Temporary Acceptance of Expired Department of  
Defense Credentials during the COVID-19 National Emergency

References: (a) DoD Manual 5200.08, Volume 3, "Physical Security Program: Access to DoD  
Installations," January 2, 2019  
(b) Under Secretary of Defense for Personnel and Readiness Memorandum,  
"Policy Guidance for Identification Card Operations for COVID-19,"  
April 7, 2020

In response to the threat of the SARS-CoV-2 coronavirus and the COVID-19 disease it  
causes, the Under Secretary of Defense for Personnel and Readiness and the Military  
Departments are taking actions to reduce visits to Department of Defense (DoD) identification  
(ID) card offices for basic actions such as renewal of expiring credentials. This memorandum  
allows for the temporary acceptance of certain DoD-issued credentials presented for physical  
access after the date printed on the card ("expired cards"), when they have been electronically  
extended in the appropriate DoD databases, subject to certain conditions identified below.

### **Installation Access**

DoD Manual 5200.08, Volume 3, paragraph 3.2.a(1) prohibits the acceptance of expired  
credentials for installation access within the United States, including the continental United  
States, Alaska, Hawaii, Puerto Rico, and Guam. Effective on the date of this memorandum until

September 30, 2020, the Secretaries of the Military Departments and the Director, Defense Logistics Agency may accept a DoD Common Access Card (CAC) or Uniformed Services ID card (USID), such as those issued to dependents or retirees, for installation access after the expiration date printed on the credential.

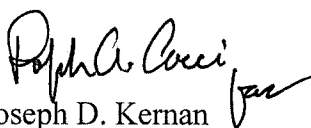
The printed expiration date on a qualifying USID or CAC must be January 1, 2020 or later for USIDs and April 16, 2020 or later for CACs, and the credential must be successfully verified using an electronic physical access control system (ePACS) that verifies continued DoD affiliation against an authoritative DoD source. An expired USID or CAC that fails to electronically verify shall not be accepted, but shall not be confiscated unless believed to be counterfeit. Expired credentials of any other type shall not be accepted for installation access. Individuals with such expired USIDs and CACs remain subject to continuous vetting through the Identity Matching Engine for Security and Analysis, and therefore, meet the “current fitness” requirement of Reference (a).

### **Facility and Building Access**

Effective on the date of this memorandum until September 30, 2020, Heads of DoD Components may accept expired CACs for access to facilities and buildings, on and off DoD installations. The printed expiration date must be April 16, 2020 or later and the cardholder’s continued DoD affiliation must be verified. Expired credentials of any other type shall not be accepted for facility or building access.

The use of an ePACS that verifies CACs and their electronically-extended expiration dates against the Defense Enrollment Eligibility Reporting System (DEERS), or that properly verifies a digital certificate stored on the CAC, is an acceptable method of affiliation verification. The use of an ePACS that verifies CACs and their electronically-extended expiration dates against a locally-managed database is an acceptable method of affiliation verification only when measures are in place to verify continued affiliation either prior to extending the expiration dates in that database or on a regular and recurring basis. ePACS that rely exclusively on the expiration date contained within the Cardholder Unique Identifier (CHUID) stored on the CAC will be unable to accept expired CACs, as this date cannot be extended. At facilities and buildings that have an ePACS that does not verify continued DoD affiliation against an authoritative source, or that do not have an ePACS, DoD Components must implement appropriate steps to verify continued DoD affiliation.

The Director for Defense Intelligence (Counterintelligence, Law Enforcement, & Security) may grant extensions to this memorandum, if necessary, while the national emergency concerning the novel coronavirus remains in effect. The point of contact for this issue is Mr. Josh Freedman at (703) 692-3724 or [joshua.a.freedman.civ@mail.mil](mailto:joshua.a.freedman.civ@mail.mil).

  
Joseph D. Kernan