



UNDER SECRETARY OF DEFENSE

5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

APR 29 2008

INTELLIGENCE

Incorporating Change 2, September 7, 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 08-004, "Policy Guidance for DoD Access Control"

References: (a) DoD 5200.08-R, "Physical Security Program," April 9, 2007
(b) Homeland Security Presidential Directive (HSPD)-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
(c) Federal Information Processing Standard (FIPS) 201, March 2006

Purpose. This DTM clarifies guidance for physical access equipment. This DTM is effective immediately; it shall be incorporated into DoD 5200.08-R. This DTM shall expire effective February 28, 2013.

DoD 5200.08-R implements the requirements of Reference (b) for physical access. In complying with HSPD-12, the Department of Defense will develop a robust interoperable system that raises security standards.

HSPD-12 requires establishment of a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees) to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Reference c is the approved Government-wide standard. DoD 5200.08-R allows for legacy access control systems to be used during the HSPD-12 transition. These systems require

interfacing hardware using commercial off-the-shelf solutions to complete the access control system. We are engaging the physical security community and industry to assess the availability of access control capabilities that are FIPS 201 compliant.

Upon completion of this assessment, we will provide further guidance. Changes will be incorporated in DoD 5200.08-R during periodic updates. Any questions or concerns regarding access control policy may be requested from my office. My point of contact is Donna Rivera at donna.rivera@osd.mil or (703) 604-1172.

Applicability. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively as the “DoD Components”).

Responsibilities

- The Under Secretary of Defense for Intelligence shall identify capabilities, requirements, and baseline standards for a comprehensive suite of hardware and software solutions to provide Components the necessary tools to verify and authenticate the identities and manage physical access authorizations or denials for personnel entering their facilities.
- The Heads of the DoD Components shall apply the following interim guidance when replacing electronic access control equipment until final guidance is issued: when purchasing upgrades to existing access control systems or when replacing current systems, the upgraded system must meet FIPS 201 (including ISO 14443 contactless technology and ability to perform automated personal identity verification); include an emergency power source; and have the ability to provide rapid electronic authentication to Federal and DoD authoritative databases, including DoD personnel registered in the Defense Enrollment and Eligibility Reporting System.


Procedures.

Change the first sentence of paragraph C1.3.4 of DoD 5200.08-R to read “Standardize personal identification and authentication to DoD installations and facilities, including interoperability with other Federal entities, utilizing the DoD PIV credential (Common Access Card (CAC)) as the universal authority of individual authenticity, consistent with applicable law.”

Change the fourth sentence of paragraph C3.3.1 of DoD 5200.08-R to read “Consistent with applicable law, the CAC shall be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces.

Change DoD 5200.08-R to delete paragraph C3.3.2. in its entirety on page 17 and delete the first sentence of paragraph C3.3.3. on page 18 “Upon full implementation of the CAC, the standard DoD PIV access control credential and the DBIDS credential, eliminate all other non-FIPS 201 compliant badges and associated equipment used for physical access (see Reference (r)).”

Releasability. UNLIMITED. This DTM is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.



James R. Clapper, Jr.