DEPARTMENT OF DEFENSE
HUMAN RESOURCES ACTIVITY
DEFENSE MANPOWER DATA CENTER
1600 WILSON BOULEVARD SUITE 400
ARLINGTON VA 22209-2593

February 5, 2008

MEMORANDUM FOR DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER (CIO)
DEPARTMENT OF THE ARMY CIO
DEPARTMENT OF THE NAVY CIO
DEPARTMENT OF THE AIR FORCE CIO
DIRECTOR, JOINT STAFF FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEM (J6)
COMMANDER, JOINT TASK FORCE GLOBAL NETWORK OPERATIONS (JTF GNO)
OFFICE OF THE SECRETARY OF DEFENSE CIO
DEFENSE AGENCIES CIOs

Subject: Obsolescing Legacy Common Access Card (CAC) Interfaces—Technical Notification

References: (a) HSPD-12, Common Identification Standard for Federal Employees and Contractors, 27 August 2004
(b) ASD (Homeland Defense) memorandum, Coordinating and Monitoring the Technical and Implementation Activities for Homeland Security Presidential Directive 12, 24 September 2004.
(c) Under Secretary of Defense (Personnel and Readiness) memorandum, Department of Defense (DoD) HSPD 12 Implementation Plan, 27 June 2005
(d) Under Secretary of Defense (Personnel and Readiness) memorandum, Department of Defense (DoD) Updated HSPD 12 Implementation Plan, 12 September 2006

As outlined in reference (a), the President directed that all Federal Agencies migrate to a single identification standard for physical access to federal government facilities and logical access to federal information systems. The National Institute for Standards and Technology published Federal Information Processing Standards Publication 201-1 (FIPS) 201-1, outlining the federal standard for Personal Identity Verification (PIV) of federal employees and contractors. On behalf of the chair of DoD Identity Management and Protection Senior Coordinating Group (IPMSCG), Defense Manpower Data Center (DMDC) has worked with the DoD's identity management proponents to outline a plan for the migration of the existing DoD Common Access Card (CAC) to fully comply with HSPD-12, FIPS 201-1, and all associated NIST special publications; reference (b)

designates HSPD-12 implementation responsibility while references (c) and (d) provide the Department's Implementation Plans to the Office of Management and Budget (OMB).

The current CAC supports the following set of interfaces:

- Government Smart Card Interoperability Specification (GSC IS) 1.0 (August 2000)
- Original CAC interface (October 2000)
- GSC IS 2.0 (Fall 2001)
- GSC IS 2.1/National Institute of Standards Technical Regulation 6887 (July 2003)
- FIPS 201-1 (March 2006)
- NIST Special Publication 800-73-1 (April 2006)
- NIST Special Publication 800-78-1 (August 2007)

As with many information technologies and standards, technology evolves such that support for older capabilities and interfaces cannot continue forever. The CAC as a technology appliance is no different. Space constraints make it such that the CAC must evolve and legacy capabilities must be obsolesced, when appropriate. This memorandum is intended to serve as a technical notification on a major change in the CAC configuration. Beginning on 31 July 2008, all newly issued CACs are expected to be configured to support only the following interfaces:

- GSC IS 2.1/National Institute of Standards Technical Regulation 6887 (July 2003)
- FIPS 201-1 (March 2006)
- NIST Special Publication 800-73-1 (April 2006)
- NIST Special Publication 800-78-1 (August 2007)

Most current commercial CAC middleware products support at a minimum NISTR 6887. The Department's largest middleware providers began this support with ActivIdentity's Activclient version 5.4 and Saflink's Netsign version 5.5. The Military Services and DoD Components' middleware experts have told us that most of their UNCLASSIFED workstations have implemented product versions that are at or beyond the minimum. To operate correctly, organizations are strongly encouraged to provide the necessary oversight to make sure all applicable middleware upgrades take place by the end of July 2008. I solicit your support and attention to ensure there are no disruptions in service. My team has briefed members of your identity management teams on this strategy and they concurred. We are prepared to assist as much as possible in this transition. If there are any questions or comments, please contact my middleware subject

matter experts Ms. Felicia Johnson (703-696-3911, felicia.johnson@osd.pentagon.mil) or Jonathan Baldwin (703-696-0232, jonathan.baldwin.ctr@osd.pentagon.mil).

Mary M. Snavely-Dixon
Director