DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301–6000

CHIEF INFORMATION OFFICER

OCT 05 2010

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

SUBJECT: Department of Defense Acceptance and Use of Personal Identity Verification -Interoperable (PIV-I) Credentials

The Federal CIO Council issued guidance to assist non-federal issuers of identity cards in achieving interoperability with Federal government PIV systems. In May 2010 the credentialing standards for PIV-I non-Federal credential providers were formalized and included in the *X.509 Certificate Policy For The Federal Bridge Certification Authority*. The policy's documented requirements for PIV-I non-federal issuers meets minimum DoD concerns regarding establishing trust relationships, trust paths, identity proofing, topology, issuer certification and auditing.

The Department is aggressively moving to accept qualified PIV-I credentials for access to physical and logical resources. A PIV-I credential, when electronically validated and where accepted by the relying party (DoD installation commander or information system owner), provides a fraud resistant, federally interoperable identity solution for populations of DoD mission partners and commercial vendors that interact with the Department of Defense on a recurring basis. Generally, use of PIV-I credentials, wherever possible, reduces overhead costs of issuing additional credentials, while still ensuring appropriate security, risk management, and identity proofing and vetting. The

process for qualifying PIV-I credentials for use in the Department of Defense is outlined in the attachment to this memorandum.

DoD relying parties granting access to DoD information resources or facilities must continue to be in compliance with applicable federal laws, regulations and current DoD physical security or information security and information assurance policies. Acceptance of PIV-I credentials is expected to be contingent on a risk management approach and comply with identification and authentication requirements, where applicable.

In those cases where DoD relying parties, installation commanders, and facility coordinators determine that granting access is appropriate and that appropriate vetting requirements are met, they should begin accepting DoD-approved PIV-I credentials for authentication and access. There are two exceptions. The first is authentication directly to DoD networks (e.g., NIPR, SIPR) as opposed to authenticating to web portals, applications, and websites. The second exception is physical access control systems where electronic identification systems are not in place. In either of these cases, a PIV-I credential cannot be used.

This memo should be given the widest dissemination throughout the Department and to the public. My points of contact are Mr. Tim Fong, timothy.fong@osd.mil, 703-604-5522 ext 109, or Mr. Keith Minard, keith.minard@osd.mil, 703-604-2770.

David M. Wennergren
DoD Deputy Chief Information Officer

Attachments:
As stated