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

CHIEF INFORMATION OFFICER

OCT 0 5 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

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

After the establishment of the Homeland Security Presidential Directive (HSPD) 12 mandate and the release of the federal credentialing standard, Federal Information Processing Standard (FIPS) 201, "*Personal Identity Verification (PIV) for Federal Employees and Contractors*"[1], there was a great deal of interest from parties external to the Federal government to develop high quality identity credentials for use by "non-PIV eligible" persons that interacted with federal information systems or accessed federal facilities regularly. These non-federal organizations desired identity credentials that are (a) technically interoperable with Federal public key-enabled information systems and (b) issued in a manner that allows Federal government relying parties to place trust in the identity asserted by the credentials. A credentialing standard was needed that was applicable to non-federal issuers of identity credentials and assisted credential holders in achieving interoperability with Federal government systems that have been public key enabled to perform authentication using PIV credentials and PKI certificates. The Federal PKI Policy Authority, in coordination with the Federal Identity, Credentialing and Access Management Subcommittee (ICAM SC), defined the requirements for the issuance of smart cards with PKI certificates (commonly known as PIV-Interoperable (PIV-I) credentials) that are designed to be interoperable with federal agency Personal Identity Verification (PIV) infrastructures. The credentialing requirements for non-federal identity credential issuers to produce federally interoperable credentials were incorporated in the latest version of the *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*[2], making it the credentialing standard for PIV-I credential providers. DoD participated actively in the revision of the FBCA certificate policy to ensure that documented requirements for PIV-I non-federal issuers met minimum DoD concerns regarding establishing trust relationships, trust paths, identity proofing, topology, issuer certification and auditing.

Identity credential providers are certified to issue PIV-Interoperable credentials following an approved cross-certification with the FBCA and mapping of the PIV-I

[1] Documents available at: http://www.idmanagement.gov/drilldown.cfm?action=library
[2] Document download available at: http://www.idmanagement.gov/fpkipa/

Points of contact are Tim Fong, timothy.fong@osd.mil, 703-604-5522 ext 109, or Keith Minard, keith.minard@osd.mil, 703-604-2770.

object identifier. Federal guidance for achieving PIV-I cross certification with the FBCA is available at the idmanagement.gov website.

PIV-I credential providers are issuers of public key infrastructure (PKI) based credentials. DoD policy authorizes DoD relying parties to accept for use all DoD-approved external PKI certificates. PIV-I providers are considered external PKIs. It is highly recommended that PIV-I providers apply to become "DoD-approved" to ensure interoperability of credentials with DoD. PIV-I credential issuers can initiate the DoD approval process by contacting the External Interoperability Working Group (EIWG) at: ExternalPKI.Interoperability@osd.mil.

In order to use PIV-I credentials to access DoD information systems or facilities, DoD mission partners or commercial vendors should procure qualified PIV-I credentials from credential providers that have been approved in accordance with the DoD External Interoperability Plan[3]. That plan outlines the steps to be accomplished to have a non-DoD issued PKI credential designated as "approved for use" within the Department of Defense. The authoritative list of DoD-approved PKIs and PIV-I credential issuers is at https://www.us.army.mil/suite/page/571419.

DoD Instruction 8520.02 authorizes DoD relying parties to accept for use all DoD-approved identity credentials for authentication and access to web portals, applications, and websites. At this time, PIV-I quality credentials shall NOT be used for authentication directly to DoD networks (e.g., Non-Secure Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet)). Relying party systems accepting PIV-I quality credentials as part of role-based access control procedures must ensure that the system threat assessment and risks inherent in PKI-based credential usage meet the requirements stated in DoD Instruction 8510.01.[4]

DoD 5200.08R, DoD Physical Security Program, is under revision to incorporate Directive Type Memorandum (DTM) 09-012. The revision will include policy addressing the use of DoD-approved PIV-I credentials for physical access control. Use

[3] Available at https://www.us.army.mil/suite/page/571419 and http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html

[4] DoD Issuances available at http://www.dtic.mil/whs/directives/

Points of contact are Tim Fong, timothy.fong@osd.mil, 703-604-5522 ext 109, or Keith Minard, keith.minard@osd.mil, 703-604-2770.

of PIV-I credentials for physical access must include the following: acceptance by the installation commander, a deployed and operational electronic physical access control system, all PIV-I credentials electronically authenticated and a basic name check conducted through the National Crime Information Center (NCIC).

DoD relying parties granting access to DoD information resources or installations/facilities based on presentation of a validated non-federally issued identity credential is strongly encouraged. Current budget constraints and strong leadership initiatives to reduce overhead should be seriously considered prior to incurring direct/indirect costs of issuing DoD credentials to PIV-I credential holders. DoD applications, installations and facilities should begin planning for and implementing the ability to authenticate and grant access based on the presentation of a valid PIV-I credential listed on the authoritative list mentioned above. PIV-I credentials will be an additional authorized form of identity to those already issued by the Department of Defense or Federal authorities. Technical support and guidance for enabling DoD websites and NIPRNET-based applications to accept the use of DoD-approved PKI credentials are available from the DoD Public Key Enabling team (pke_support@disa.mil) or at the DoD PKE web site: (https://www.us.army.mil/suite/grouppage/58452 )

Points of contact are Tim Fong, timothy.fong@osd.mil, 703-604-5522 ext 109, or Keith Minard, keith.minard@osd.mil, 703-604-2770.