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

SUBJECT: Department of Defense Requirements for Accepting Non-Federally Issued Identity Credentials

References:
(a) Executive Office of the President (EOP) Office of Management and Budget Memorandum, October 06, 2011
(b) Executive Office of the President (EOP) Office of Management and Budget Memorandum (M-11-11), February 3, 2011
(c) DoD Instruction 8520.02, “Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO)”, May 24, 2011
(e) DoD Instruction 8520.03, “Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO),” May 13, 2011
(f) Directive-Type Memorandum (DTM) 09-012, “Under Secretary of Defense for Intelligence (USD(I)),” September 30, 2010
(g) White House, Office of the Press Secretary Homeland Security Presidential Directive/HSPD-12, August 27, 2004
(h) Executive Office of the President (EOP) Office of Management and Budget Memorandum (M-04-04), February 16, 2003

To leverage the convenience and cost advantages afforded by conducting transactions in cyberspace, DoD business partners and other members of the public have developed and issued
Non-Federally Issued (NFI) identity credentials to support authentication of their individual identities in online interactions with the Federal Government. The references above describe Federal Government guidance on acceptance and use of NFI identity credentials and specific DoD policies and practices on accepting credentials for logical access to DoD applications and websites. Per references (d) and (e), only Federally issued, high assurance credentials can be used for network access.

DoD Components will implement the following actions to support the use of NFI credentials in accessing specifically designated DoD applications and websites in accordance with reference (e).

1) Components will ensure that unclassified information systems will be enabled to accept NFI identity credentials for authorized users.

2) Components will ensure that information systems will support identity authentication using all credential strengths that meet or exceed the minimum level identified in accordance with reference c.

3) Components will accept a DoD approved very high assurance (reference h) credential from a user authorized system access rather than require the procurement of a DoD credential.

To ensure privacy, security and interoperability requirements are addressed; Components may only accept NFI identity credentials recognized through Department of Defense Chief Information Officer approval processes. The DoD-approved list of NFI identity credentials is at http://iase.disa.mil/.

An executive summary of the process for DoD adoption and use of NFI identity credentials is attached to this memorandum.

The point of contact for this memorandum is Mr. Paul D. Grant: Paul.Grant@osd.mil, 703-695-4808.

Teresa M. Takai

Attachment:
As stated
Executive Summary - Adoption and Use of Identity Credentials from Non-Federal Issuers

The DoD and Executive Branch will leverage identity credentials from Non-Federal Issuers (NFI) to authenticate CAC and PIV ineligible personnel to Federal information systems and services. The NFI identity credential initiative allows the Federal Government to:

- Reduce the need and costs to issue and maintain credentials for mission partners
- Protect partners by minimizing the collection and storage of personal information
- Benefit partners by minimizing the number of credentials they must protect and maintain
- Support the National Strategy for Trusted Identities in Cyberspace (NSTIC) ¹

Reference. The NFI identity credential requirement is documented in the October 06, 2011 OMB Memorandum, Requirements for Accepting Externally-Issued Identity Credentials, ² which requires Federal agencies to begin implementing the acceptance and use of NFI identity credentials for authentication to Federal websites and services by authorized individuals.

Identity Assurance Levels (IAL). There are four (4) IALs ranging from little to no confidence to high confidence and denoted as IAL-1 thru IAL-4. IAL are defined in OMB M 04-04³ with amplification available at www.idmanagement.gov.

Non-Federal Issuers (NFI). The Government maintains a list⁴ of NFI credential providers that have been evaluated and are deemed acceptable for authentication at specified IALs. The DoD augments this approval process creating a sub-set of approved NFI such that owners of DoD resources can only select from the DoD approved list⁵.

Determining Minimum IAL. Resource owners and their accreditors must determine the minimal IAL required for authentication to their asset using guidance associated with OMB M 04-04 and DoD Instruction 8520.03, Identity Authentication for Information Systems.⁶ The minimum IAL required is based on the potential impact resulting from an authentication error to the resource and the sensitivity of the resource. The more severe the impact requires higher confidence in the identity, i.e. higher IAL, before granting access. Note that the Federal Government recognizes IAL-1 credentials; however they are not approved for use in DoD.

Determining Acceptable NFI. Resource owners select NFI based on the minimal IAL required for their resource and the approved NFI offering credentials at, or above, that IAL. NFI vary in the IAL they offer and not all NFI offer credentials at every IAL. Relying parties can use the DoD list of approved TFP and NFI to select appropriate solutions that support resource requirements.

Implementation Guidance. Relying parties will have access to published guidance. Federal implementation guidance and general “how-to” best practices to be published on idmanagement.gov. Each individual TFP and/or NFI is expected to publish specific how-to guidance which will also be made available on this website.

Opt Up. Resource owners must allow users to “opt-up” the credential IAL they use to authenticate. “Opt-up” allows users to minimize the number of credentials they maintain and offers resource owners a tiered approach to information access based on its sensitivity and IAL of the credential; the higher the IAL, the more privileges and capabilities a resource can offer. Applications with lower credential requirements must allow users with higher credentials to use their stronger credentials for access and improved security, e.g. an IAL-4 holder should not be required to procure lower level credentials. Enabling for the minimum with the capability to “opt up” encourages the use of stronger credentials, increasing security and user convenience and supports the intent of the NSTIC.

¹ http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
² http://www.cio.gov/Documents/OMBReqforAcceptingExternally_IssuedIdCred10-6-2011.pdf
³ http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf
⁴ http://idmanagement.gov/
⁵ http://iasa.disa.mil/