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

CHIEF INFORMATION OFFICER

May 5, 2005

Ms. Michele Courtney
General Services Administration
Office of Identity Policy and Practices Division (MEI)
1800 F Street, NW
Room 2014
Washington, DC, 20405

Dear Ms. Courtney:

The Department of Defense (DoD) is pleased to present the attached comments in response to the tasks for comments on the Homeland Security Presidential Directive (HSPD) 12 Implementation Plan Reporting Template and the Draft Department and Agency Implementation Guidance. DoD concurs with the Implementation Plan Reporting Template and the Guidance pending inclusion of the comments provided in the attached supporting documentation.

Please forward any additional question or comments you may have to Mr. Michael Butler, michael.butler@osd.pentagon.mil or (703) 696-7395. Thank you for the opportunity to provide DoD's comments.

Sincerely,

Priscilla Guthrie
DoD, Deputy Chief Information Officer

Enclosure:
Comments Matrix

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
1	DoD	Michael Butler	E	Sec 1, pg. 3	The Acronym for the Department of Defense is used incorrectly.	Change to DoD.
2	DoD	Michael Butler	E	Sec 1, pg. 3	The paragraph contains the text, "...who require long-term access to Federally controlled facilities…", but does not clearly define long term".	Federal facilities and installations are routinely visited by personnel on an inconsistent schedule (e.g. repair pesonnel providing service under a maintenance agreement, personnel who provide routine, scheduled support, vendors and delivery personnel). In these cases the period in which the visits are conducted spans years, but is not on a daily basis. "Long Term" needs to be clearly defined, establishing the eligibility threshold for those individuals who require only part time acccess.
3	DoD	Michael Butler	E	Sec 2, Part B, pg. 4	The table indicates that by October 27, 2006, covered departments and agencies must comply with FIPS 201, Part 2, but does not state whether compliance must be initial operating capability, or full operating capability.	Modify the text to include the phrase "at initial operating capability." Implementation of full operational capability is physically and fiscally impractical for the department. Full implementation is not likely to occur until sometime in 2010, and this reality must be acknowledged.
4	DoD	Michael Butler	E	Sec 3, Part 1, B, pg. 5	The text states, "Adopt and accredit a registration process consistent with the identity proofing and registration requirements in section 2.2 of the Standard. This registration process applies for all new identity credentials issued." It must be noted that this requirement will have an immediate impact on recruiting for the military services, and could cause delays in the commissioning and/or enlistment process. This is potentially crucial in today's difficult recruiting market. "For existing employees and contractors, develop a plan and begin completing the required identity proofing requirements for all current employee and contractors who do not have an investigation (i.e., “completed National Agency Check with Written Inquires or other Office of Personnel Management or National Security community investigation”) on record." This is not consistent with the standard that calls for a completed NAC/NACI before the issuance of a credential.	Sufficient flexibility should be included in the text to allow continued accessions processing of military recruits, while the NAC or NAC-I proceeds. These personnel are under stringent observation in a very controlled environment during the accessions process, and during initial training (recruit training, officer candidate school, etc.). Should adverse information be developed by the NAC or NAC-I, these personnel can be immediately processed for discharge. The background investigation process is backloged. The Department will not be able to meet these timelines. Implementing the required identity proofing requirements for all current employees and contractors who do not have a completed National Agency Check with Written Inquiries will further delay investigations. Therefore, those employees who truly need high level clearances will wait even longer and the Department will experience unacceptable delays. If the Federal government imposes this requirement, we must either allow current employees and contractors to hold credentials once an accredited registration process has begun, allowing new employees and contractors to receive credentials after being entered into an accredited registration process, or provide a huge increase in resources for the completion of the investigation process.
5	DoD	Michael Butler	E	Sec 3, pg. 5	FIPS-201: Page 6, section 2.2 states "At a minimum, the [NAC] shall be completed before credential issuance." Page 39, section 5.3.1 "An employee or contractor may be issued PIV Card and Logical Credentials while a [NACI or equiv] … is pending." "…successfully completed … within 6 months of… issuance… or the PIV card and PIV Authentication Certificate shall be revoked."	The HSPD-12 Implementation Plan Template, Section III, 3) should be rephrased to accurately reflect Section 5.3.1 of FIPS-201 (e.g. "NACI is complete NLT 6 months after PIV and Authentication Certificate issuance or they are both revoked").
6	DoD	Michael Butler	E	Sec 3, pg. 5	FIPS 201 does not specify a method for doing logical access but only specifies the authentication for eligibility to have logical access. Part 2: PIV 2 #17 requires a agency to authenticate for logical access.	Recommend re-phrasing #17 to measure Agency to the Standard “Capable of Authenticating Part 2 Credentials for Logical Access”.

7	DoD	Michael Butler	T	Sec 3, Part 2, A, pg. 6	Dod is implementing Common Access Card Certificate Logon in the Active Directory environment that will meet the logical access requirement. However, to do so, the user's account/name in AD has to be bound to the user's certificate's Electronic Data Interchange Personal Identifier (EDIPI) number. This may cause a problem with cross agency authentication. If a Fed from outside DoD uses a PIV Card with certificates issued from their Department's Certificate Authority, there is a possibility that the EDIPI number will duplicate a user's EDIPI number in the DoD. Need to determine if mechanisms are being put in place to guarantee there are no EDIPI duplications across the varying Federal PKIs.	There may be an interoperablity issue related to the uniqueness of EDIPI numbers across Federal Agencies with separate PKIs. For this reason, it would be more likely to have a plan for a interoperable cert. validation rather than have implementation of the solution.
8	DoD	Michael Butler	T	Sec 3, Part 2, A, pg. 6	The implementation of CAC Logon and certificate validation across the Department will take longer than the timelines allow.	There are only two ways to achieve the standard: extend the implementation time allowed, or increase the funding to shorten the schedule. The directive impedes the ability of the DoD to carry out an existing program for strong, secure identity management. Regardless of the "goodness" of the standard, the DoD is engaged in a Global War on Terrorism and our resources are stretched thin. Our budget constraints are such that we cannot achieve fielding in under two years
9	DoD	Michael Butler	E	Sec 4, C, pg. 7	After meeting the specifications of HSPD-12, little room remains for the DoD requirements (e.g. Geneva Conventions, treaties, status of forces agreements).	Include escalation process within the guidance document for determining the priority of items that use the card's limited space.