December 22, 2004

TO: National Institute of Standards and Technology

FROM: Michael Butler, Deputy Director of Smart Card Programs and Operations for Defense Manpower Data Center

SUBJECT: Public Draft of Federal Information Processing Standard 201 (FIPS 201)

The Department of Defense (DoD) fully supports the intent of HSPD-12 to mandate a secure and interoperable identity credential with rules and standards for issuance, identity assurance, and requirements for electronic authentication. However, DoD takes strong exception to the following sections of the proposed implementing standard, Federal Information Processing Standard (FIPS) 201. DoD is supporting the current IAB position that was submitted to NIST on 21 December 2004.

- **PRESCRIBED IDENTITY VETTING/CREDENTIALING PROCESS REQUIRES MAJOR RE-ENGINEERING OF A SYSTEM THAT ALREADY MEETS THE INTENT OF HSPD-12:** The proposed standard is excellent in formalizing and separating roles and responsibilities for identity vetting and credential issuance. However, the standard prescribes a business process model based upon physical access badging versus the credential model adopted by DoD. The standard appears to prescribe a business process rather than specify functional requirements. As a result, major DoD systems will require re-engineering to meet the standard and achieve certification. This re-engineering will not improve the existing system or its security. DoD recommends the standard define functional requirements of the identity vetting/credentialing process rather than prescribe a specific business process.

- **PRESCRIBED USE OF BIOMETRICS IS OUT OF SYNCH WITH TECHNOLOGY AND STANDARDS THAT HAVE UNKNOWN SECURITY:** The standard requires two fingerprint images and one digital photo on the chip for facial recognition. This will consume approximately 20 -25K of the available 48K space on the 64K card. This space requirement will not fit on the next generation Common Access Card (CAC) scheduled for production in 2005. Storing template minutia rather than biometric images significantly reduces space requirements down to approximately 10K of space. There are unanswered questions regarding the security of using IMAGES rather than template minutia. This is of particular concern since each person has a finite number of biometrics available, should one be compromised. Recommend the biometric requirements on the card be changed from images to template minutia. This should be implemented at such time as (1) interoperability specifications for biometric template minutia become mature and compliant products are available from multiple vendors, and (2) card capacity increases from 48K to 64K. Additionally, security requirements to protect biometrics from compromise should be assessed and prescribed in the standard.

- **REQUIREMENT FOR COMPLETED BACKGROUND CHECK IMPROVES SECURITY, AND REDUCES RISK, BUT CURRENT INFRASTRUCTURE CANNOT SUPPORT. THIS REQUIREMENT COULD INCREASE THE TIME TO HIRE NEW EMPLOYEES/CONTRACTORS BY FOUR TO TWELVE MONTHS:** The standard requires completion of a background check, or National Agency Check (NAC), prior to issuance of a federal credential. Based on what is at stake, this requirement would clearly improve our security and reduce risk. Credentialing someone and granting access on the basis of this credential without a background check poses a security risk. All military members, civilians, and contractors, in sensitive positions, requiring security clearances already meet this requirement in DoD (approximately 75% +). However, the infrastructure to conduct the NACs, as proposed, does not exist or efficiently operate today. Frequently, there is a 4-12 month delay for completion of the background check that forces new employees to be treated as visitors. This is much too long. DoD recommends this requirement be implemented when the infrastructure is in place to complete background checks within a reasonable timeframe, such as 30 days. Concurrently, alternate processes that may meet the requirement to issue a credential should be considered.

- **PROPOSED TECHNICAL STANDARDS ARE UNTESTED WITH NO REFERENCE IMPLEMENTATION AND NO COMPLIANT PRODUCTS AVAILABLE:** The proposed standard is new and has never been implemented. Currently, DoD and other Federal Agency systems support the existing National Institute of Standards and Technology Report (NISTR) 6887 and the Federal Government Smart Card Interoperability Specification (GSC-IS). The draft FIPS 201 is a significant departure from the NISTR 6887 interoperability framework. Smart card systems within DoD, Department of Homeland Security (DHS), Department of Interior (DOI), National Aeronautics and Space Administration (NASA), and Department of Veterans Affairs (VA) use NISTR 6887 as the basis for interoperability. These programs have evidenced success by receiving numerous industry awards and recognition. NIST created the FIPS 201 technical standard without leveraging the benefits of the current NISTR 6887. The departure from the existing NISTR 6887 interoperability framework will require significant changes to the existing infrastructure, re-tooling of software, re-certification of applications, and additional changes that result in costly re-investments in technology. There are too many unknowns in the new standard. Therefore, DoD recommends the existing NIST interoperability standards be prescribed as the baseline for FIPS 201and that the ambiguities in the existing standards be tightened. In addition, a phase-in for the new standard should be added to the FIPS 201 after the new technical standard has been fully vetted, a reference implementation developed, required changes made, testing conducted, and backwards compatibility accommodated.

- **PROPOSED FIPS 201 PLACES CONFIGURATION MANAGEMENT CHANGES OUTSIDE THE CONTROL OF THE FEDERAL GOVERNMENT AND IN THE HANDS OF AN INTERNATIONAL BODY THAT REMOVES FEDERAL GOVERNMENT CREDENTIAL MANAGERS FROM THE PROCESS:** NIST has proposed that configuration management of the FIPS 201 will be the responsibility of the International Standards Organization (ISO) instead of the Federal configuration

committee that has operated under the Interagency Advisory Board (IAB) for the past two years. Allowing change management to occur outside the Federal sector (outside the United States) will increase the risk that additional change, beyond the control of federal credential managers, will take place. DoD recommends the IAB process remain in effect and that NIST be formally tasked to support and advise the IAB. In addition, new capabilities recommended for standards changes must be endorsed by the IAB.

- **WITHOUT ELECTRONIC AUTHENTICATION OF CREDENTIALS, FIPS 201 REQUIREMENTS DO NOT PROVIDE IMPROVED SECURITY:** HSPD-12 encourages electronic authentication; however, the proposed FIPS 201 standard allows a manual/visual processes for checking credentials and states that electronic authentication is outside the scope of the standard. A manual/visual process is very dependent upon the human being involved. Without a more prescriptive timeline and direction towards using electronic authentication, there is the risk that a significant amount of work will be done with very little return on investment or security. DoD recognizes that electronic authentication may be outside the scope of the proposed standard. As such, DoD strongly recommends that the Office of Management and Budget (OMB) publish policy prescribing an aggressive implementation of electronic authentication at physical access points over the next five years and requires Agencies to provide their implementation plans to OMB. If a decision is made to not perform electronic authentication, then the criteria used to make that decision should be provided. Strong credentials, identity proofing and vetting, and revocation are critical; however, without electronic authentication it is impossible to be assured that physical access points will be able to identify fraudulent or revoked credentials.

- **PROHIBITED USE OF COLOR CODE/STRIPE TO PHYSICALLY DELINEATE NON-US CITIZEN (OR FOREIGN) CARDHOLDERS RISKS FORCE PROTECTION AND THREAT DEFENSE CAPABILITIES:** The proposed standard prohibits the use of color coding and designs on Federal credentials. Since the CAC uses RED or GREEN stripes to define Foreign Nationals and Contractors, a redesign of the CAC will be required. The CAC does identify roles by text on the card. The point of major concern is that elimination of the red stripe, which identifies foreign national personnel, is inconsistent with General Accounting Office (GAO) Report findings. The results of GAO reports specifically suggest aggressive measures to minimize risks associated with not clearly identifying foreign national personnel within virtual and physical communities of Federal Government. The requirements of the proposed draft standard are inconsistent with GAO findings and place significant risk on the ability to visually identify foreign nationals, maintain good force protection, and defense-in-depth techniques. Recommend that a common approach to this business process be coordinated among existing users to determine impact.