X-Sieve: CMU Sieve 2.2
Subject: Comments on Public Draft FIPS 201
Date: Thu, 23 Dec 2004 14:44:41 -0500
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Comments on Public Draft FIPS 201
Thread-Index: AcTpJ9f6rYF0H6c6RVCfpjhKWmMb7g==
From: "Olivieri, Janine" <JOlivieri@intellicheck.com>
To: <DraftFips201@nist.gov>
X-SLUIDL: 67F79E45-F6A94D80-875A990D-D167117D
X-MailScanner:
X-MailScanner-From: jolivieri@intellicheck.com

<<CommentTemplateDraft2.xls>>

Janine Olivieri
Executive Administrator
Intelli-Check, Inc.
246 Crossways Park West
Woodbury, NY 11797
(516) 992-1900 phone
(516) 992-1918 fax
jolivieri@intellicheck.com
www.intellicheck.com


CommentTemplateDraft2.xls

Submitted by: Frank Mandelbaum, CEO, Intelli-Check, Inc.
Date: December 23, 2004

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	Intelli-Check, Inc.	Frank Mandelbaum, 516-992-1900, fmandelbaum@intellicheck.com	G	PIV1, FIPS 201, Section 2.2.1	Section acknowledges that "paper based source documents by themselves provide VERY weak ASSURANCE of identity." The high-tech revolution has created a major problem for those who rely on identification documents. In an age when scanners, computers and color printers are commonplace, fake IDs of the highest quality are easily obtainable from thousands of sites on the Internet. These fakes appear so real, even law enforcement agencies have difficulty distinguishing them from legally issued documents. These high tech devices can also be used to easily alter properly issued IDs. The process described in this section supplements document verification with background checks designed to improve ASSURANCE of identity. However, visual verification only of the identity source documents could allow people with false identities to pass the screening procedure. Electronic verification to mitigate the risk of fake IDs that applies tamper-detection logic to the barcode or magnetic stripe contained on a DL\ID or a smart chip such as contained on the CAC card or the MRZ on a passport of the person being screened would Currently available, COTS verification technology is capable of proving true identity and eliminating the inefficiencies and inaccuracies with manual data entry and export the captured data from the electronically readable encoding into a required form. It also is capable of electronically matching similar encoded fields from multiple identity source documents such as a driver license to a passport, a military ID to a passport or a driver license to a border crossing card etc. Additionally, this technology can electronically capture the data from the encoding on the identity source document and also link the image of the document being screened to an electronic file, thereby eliminating the need to maintain paper files which could become voluminous. Therefore, the requirement in the standard should be changed to eliminate visual inspection with electronic verification. This suggested change would comply with Section 3.1, 3.2.1 and 3.2.2 of the requirement that require the authentication and vetting of applicants.	Change: "**Two** of the documents shall be **electronically verified** valid State or Federal Government-issued picture IDs". Change: The PIV Requesting Official shall submit the PIV request and **electronically store the copies of** the identity source documents for Applicants in the PIV **file pertaining to the Applicant.** Change: **The PIV Authoring Official shall approve the request and forward it together with the electronically stored copies** of the identity source documents to the Registration Authority and PIV Issuing Authority. Change: The Registration Authority shall be responsible to maintain **electronic** copies of the identity source documents.

D = Document, 1 = FIPS2001, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical