Submitted by: Steve Price-Francis, LaserCard Corporation
Date: Dec 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	LaserCard Corporation	Steve Price-Francis Vice President Business Development	T	p. 17; para 4.1.2.a.	OVD's and OVI do not provide tamper resistance but rather counterfeit resistance and visual authentication support. However, both are relatively easy to simulate and will likely pass visual inspection. The first point of attack by criminals is to produce "look-alike" cards which can be used to breach security in situations where visual inspection is the norm.	The visual authentication aids and counterfeit resistance measures should be much stronger, involving the specification of a proven and widely used feature that can deliver a hierarchy of security levels. A method of achieving this is described in the attachment: "Optical Memory - The proven component of the US Government's Identity Card programs"
2			T	p.17; para 4.1.2.b.	Tamper resistance is a key component of a secure ID card program. Without sufficient attention to this point, alteration of the information on the card will be relatively easy and imposters will use authentic cards which have been compromised by this method.	Tamper resistance should be provided by a proven, unalterable visual and digital storage technology. See attached: "Optical Memory - The proven component of the US Government's Identity Card programs"
3			T	p.18; para 4.1.3.1.	OVD's are not tamper resistant features but rather counterfeit resistant and supports to visual authentication.	See proposed change #1 above.
4			T	p.19; para 4.1.4.1; p.35; para 4.4.5; p.49; para 6.1.1	The facial image zone is unnecessarily limited and will work against the need for ease of visual ID verification.	Redesign the card with visual inspection in mind.
5			T	as above	One of the most secure visual and data storage technologies for ID cards is optical memory. To exclude it from the specification is unnecessarilty limiting agencies' scope and options.	Optical memory should be specified as an option and should be accommodated in accordance with applicable ISO standards: ISO/IEC 11693 and ISO/IEC 11694 Parts 1 - 4 and draft Parts 5 & 6.
6			T	p. 31; para 4.4.2	It is correct that the greatest level of interoperability of biometrics is via transportability of images. A typical storage requirement for a JPEG facial image is 15K; two WSQ compressed forensic quality fingerprint images will occupy 25-30K each, for a total of 65-75K. Therefore, it is counterproductive to specify a memory form which is acknowledged as limited in its capacity and requires trade-offs (ref. p.35; para 4.4.5.5). Such an approach unnecessarily limits agencies' choices and scope, for example, to expand to other forms of biometric in the future, and risks compromising security if inappropriate trade-offs are made.	Optical memory is the only widely used, tried and tested, high capacity, secure storage technology able to amply accommodate this requirement. See attached: "Optical Memory - The proven component of the US Government's Identity Card programs"
7			T	Section 5 PIV Issuance and management	PKI and associated certificate registration and revocation is a very costly and complex initiative. GAO reports indicate that, for example, the Department of Defense originally budgeted $73m to implement PKI for 4.3m Common Access Cards. That expenditure is expected to reached $1bn or more (or approximately $230 per cardholder).	Optical memory does not need to be supported by a PKI and, therefore, should be considered for applications where such an enormous investment is not justified.
8			T	as above	PKI carries the requirement for on-line, real-time, communications. Such systems are vulnerable to system overload and down time which can cripple a mission critical application.	Optical memory can operate securely off-line obviating the problems of system overload, failure or malicious attack on a network system. (see attached: "Optical Memory - The proven component of the US Government's Identity Card programs")

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical