X-Sieve: CMU Sieve 2.2
Importance: Normal
From: David_Belchick@ios.doi.gov
To: DraftFIPS201@nist.gov
Date: Thu, 23 Dec 2004 12:40:25 -0500
X-MIMETrack: Serialize by Notes Server on IOSDCAMAIL02/OS/DOI(Release 6.5.2|June 01, 2004) at
12/23/2004 12:40:25 PM,
Serialize complete at 12/23/2004 12:40:25 PM,
Itemize by Notes Server on IOSDCAMAIL02/OS/DOI(Release 6.5.2|June 01, 2004) at
12/23/2004 12:40:25 PM,
Serialize by Router on IOSSMTP1/OS/DOI(Release 6.0.3|September 26, 2003) at
12/23/2004 12:44:24 PM
Subject: Comments for FIPS [Virus checked]
X-MailScanner:
X-MailScanner-From: david_belchick@ios.doi.gov

Please call me with any questions.

David Belchick
202-208-4262


FIPS201.xls

Submitted by: _____

Date: _____

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
	DOI	David_Belchick@ios.doi.gov	G		Currently, Biometrics are not a mature technology that can support interoperability. The Government has only completed laboratory testing. The Standards work needs to be completed, and an accompanying Business Case developed that increases Security and Provides functionality.	DOI would recommend keeping Biometrics in the Policy Guidance in the FIPS document and moving all technical and implementation guidance out into an accompanying handbook. Incorporating the New Biometrics work will be much easier in a Handbook versus the FIPS publication.
1	DOI	Russell_Davis@blm.gov	T	Table 5-2, page 42	The DOI would like to allow customers to receive ICCs from sources such as State Driver License issuers. As such, they would not have a position 1 - 4.	Allow a new level 0 for customers dealing with a Federal agency that are not employed by a Federal agency and would not have completed a NAC.
2	DOI	Russell_Davis@blm.gov	T	Section 5.2.3.4, Page 45, second paragraph	Certificates cannot be distributed via LDAP because the FASC-N is contained within the subject alt name. As certificate management systems do not mediate certificates, this is a potential show stopper.	Make the FASC-N non-sensitive and allow LDAP distribution of certificates containing this value.
3	DOI	Russell_Davis@blm.gov	G	Section 5.2.4.1, Page 46, second paragraph	Having users get new photographs for each renewal is not labor cost effective.	Allow photographs to be reused for up to five years.
	DOI	Russell_Davis@blm.gov	G	Table 5-3, Page 45	There are different key sizes listed with expiration dates. For example, the PIV Authentication key is good at 1024-bits until 12/31/2010 yet the Key Management Key is good at 1024-bits only until 12/31/2007. Other areas of the document have a similar problem (including with the hash algorithm). This leaves the reader with the impression that their is no science behind the decision process.	Reference a document that explains the rational used in selecting various dates for algorithm upgrade.
	DOI	Russell_Davis@blm.gov	T	Section 5.2.3.2, page 43	This section requires the Common Policy Certificate Policy (CP). In the Common Policy CP, Section 3.1.1, there are a number of naming issued that need to be resolved. The cn=nickname lastname does not necessarily represent a meaningful name. Second, contractors have the following format cn=firstname initial. lastname (affiliate) yet there is no standardization as to what the affiliate is. Third, there is no policy that describes how two people with the same name will be resolved. Forth, there are people that do not have a middle name, how will these be addressed? This CP impacts the entire Federal government yet it is predominantly the work of the Certificate Policy Working Group (CPWG). There needs to be open vetting, consistent with all other NIST efforts, applied to this working group.	Do not use nicknames; specify how multiple users with the same name will be resolved; specify the distinguished name for people with no middle names; specify the affiliate extension; when the CPWG is standardizing policies that impact the Federal government, these products need to be vetted in an open forum.

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

Submitted by: ______________________

Date: ____________

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

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