X-Sieve: CMU Sieve 2.2
Date: Thu, 23 Dec 2004 14:19:09 -0500
From: Debb Blanchard <dblanchard@enspier.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)
X-Accept-Language: en-us, en
To: DraftFips201@nist.gov
CC: "Brindisi, Frank - OASAM" <brindisi.frank@DOL.GOV>,
Dan Backo <dbacko@enspier.com>,
"McCreless, Kenneth - ASAM" <McCreless.Kenneth@DOL.GOV>
Subject: Comments on Public Draft FIPS 201
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - zeta.sitelutions.com
X-AntiAbuse: Original Domain - nist.gov
X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]
X-AntiAbuse: Sender Address Domain - enspier.com
X-Source:
X-Source-Args:
X-Source-Dir:
X-MailScanner:
X-MailScanner-From: dblanchard@enspier.com

To Whom It May Concern:

Attached are the comments from Department of Labor with respect to the proposed FIPS 201.

Regards,
Debb Blanchard
Enspier DOL PM
office: 410-871-0836
email: dblanchard@enspier.com


CommentTemplate-2004-12-21.xls

Submitted by: ___Deborah Blanchard, Department of Labor (DOL)_____
Date: _12/23/2004

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	DOL	F. Brindisi	T	2.2, Page 4, last sentence	What are the minimum requirements and position sensitivity for people required to perform these roles, e.g., education, level of experience, etc.?	
2	DOL	F. Brindisi	T	2.2.1, Page 5, 2nd para., sentence 4	"...and photocopies of identity source documents.." - some states in which Regional and Field offices are located have deemed it illegal to make photocopies of a state-issued picture ID. What is the legality of the standard to require this with respect to state laws?	
3	DOL	F. Brindisi	T	2.2.1, Page 5, 2nd bullet	What are the requirements for the identified roles (Authorizing Official, Registration Authority, Issuing Authority) to "...maintain information...", e.g., date of birth, about the Applicant in a secure fashion IAW privacy concerns? See also comment #5	
4	DOL	F. Brindisi	T	2.2.1, Page 6, Table 2-2	Given the time frame to obtain a NACIC, is it the goal of the standard to have people who need this, obtain a lower level position while waiting for the NACIC? a. The requirement to wait for completion of the background check applicable to the position sensitivity level before the PIV is issued is not feasible as applied to logical access. A minimum acceptable background investigation should be established and allowed for issuance of the PIV, at least for an interim period until the background investigation required for the particular position sensitivity level is complete. b. Preferably, the standard should not be repeating or establishing the background investigations required for each position sensitivity level at all. The standard should only set the minimum investigation required for issuance of ALL PIV cards c. If the standard must state background investigation requirements for each position sensitivity level, the background investigation requirements should be stated as a minimums rather than as absolute requirements.	
5	DOL	F. Brindisi	T	2.2.1, Page 6, Table 2-1, Table 2-2	If the standard must state background investigation requirements for each position sensitivity level, (2-1) the necessary background investigation form is dependant on the type of investigation, not the position sensitivity level as indicated in the table; (2-2) the background investigation specified for each position sensitivity level should be expressed as a minimum rather than an absolute.	
6	DOL	F. Brindisi	T	2.2.1, Page 7, bullet list (all items)	At what level and how should the Registration Authority maintain this information? Refer to #3	"The Registration Authority shall be responsible to maintain the following in a secure manner in accordance with privacy requirements as noted <law?> and in section <???> of this standard:..."

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

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
7	DOL	F. Brindisi	T	2.2.2, Page 7,	What is the time frame allocated to a "most recent previous check"? What is the maximum time frame between background checks?	Suggest that the timeframe be mentioned for background checks.
8	DOL	F. Brindisi	T	2.2.3, Page 7	Refer to comment #4, if a person is slotted for a NACIC, is that person to be treated according to visitor procedures or shall that person be afforded a lesser position while the NACIC is being completed? a. The requirement to wait for completion of the background check applicable to the position sensitivity level before the PIV is issued is not feasible as applied to logical access. A minimum acceptable background investigation should be established and allowed for issuance of the PIV, at least for an interim period until the background investigation required for the particular position sensitivity level is complete. b. Preferably, the standard should not be repeating or establishing the background investigations required for each position sensitivity level at all. The standard should only set the minimum investigation required for issuance of ALL PIV cards c. If the standard must state background investigation requirements for each position sensitivity level, the background investigation requirements should be stated as a minimums rather than as absolute requirements.	
9	DOL	F. Brindisi	T	2.3, Page 7	At what level, e.g.m, sensitive, classified, etc., and how should the Issuing Authority maintain this information?	
10	DOL	F. Brindisi	T	4.1.3, Page 18	The card topology should allow for the card to be punched at the top left (front)/top right (back). The barcode generally does not need to run from edge to edge and should be oriented to the bottom of the card. The photo on the front can be adjusted accordingly.	
11	DOL	F. Brindisi	T	4.1.4.1.a, Page 19	WRT changing physical characteristics, e.g., facial hair, hair color, eyeglasses vs contact lenses/lasik, etc, is there a requirement to change the photograph with each change of physical representation?	
12	DOL	F. Brindisi	T	5.2.3.1, Page 43, 2nd sentence	To what does "these Cas" refer in this sentence?	
13	DOL	F. Brindisi	T	5.2.3.6, Page 46	Does this mean that all Cas operated and supported by an agency and that have cross-certified with the FBCA must now be signed by the root of the Common Policy CA?	
14	DOL	F. Brindisi	T	5.2.3.6, Page 46	WRT the agency that is operating their own CA that has cross-certified with the FBCA - is the agency now required to meet all the requirements of the Common Policy?	

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

Submitted by: ___Deborah Blanchard, Department of Labor (DOL)_____
Date: _12/23/2004

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
15	DOL	F. Brindisi	T	5.2.4.1, Page 46, last sentence	A role should perform this verificaiton	"The Requesting Official and Registration Authority shall verify that the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials."
16	DOL	F. Brindisi	T	5.2.4.2, Page 46, 1st paragraph, 2nd sentence	A role should perform this verificaiton	"The Requesting Official and Registration Authority shall verify that the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials."
17	DOL	F. Brindisi	E	5.2.4.2, Page 47, 1st sentence, 1st statement	should be a bullet and incorporated as part of the bulleted list	"...must be in place to ensure that: * The PIV card itself is revoked.... * The PIV Certificate Issuer....."
18	DOL	F. Brindisi	E	6.1, Page 49, 2nd Paragraph, last sentence	run on sentence; should be divided into 2 sentences	"For privacy reasons, contactless use of PINs and biometrics is not supported.. PINs and biometrics may be used with the PIV card using contact readers."

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