From: Joseph Burns <Joseph.Burns@csosa.gov>
To: "'draftfips201@nist.gov'" <draftfips201@nist.gov>
Cc: Andrew Thomas <andrew.thomas@csosa.gov ...snip... Timothy.Barnes@csosa.gov>
Subject: Comments on Public Draft FIPS 201

<<CommentTemplate 12-20-04.xls>>

Joseph Burns
Office of Security
Court Services and Offender Supervision Agency
633 Indiana Avenue N.W., Suite 824
Washington, D.C. 20004
Tele: (202) 220-5688
Fax: (202) 220-5726


CommentTemplate 12-20-04.xls

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
				FISP 201		
	CSOSA Office of Security	Carol Holloway	T	9 page v	delete the working with respest to contractors	Currently there is no mandate to investigate contractors unless they occupy a position that requires access to classified information
	CSOSA Office of Security	Carol Holloway	T	2.2.1 page 5	delete "as part of the federal vetting process..."	If this is going to apply to contractors they DO not go through a "FEDERAL VETTING PROCESS"
1	CSOSA Office of Security	Joseph Burns	E	2, 2.1, page 4	delete the word terrorist....we want to make identity credentials resistant to ALL exploitation not just terrorist explotation	"Issue Identity credentials that are resistant to identity fraud, tampering, counterfeiting, and explotation;"
2	CSOSA Office of Security	Joseph Burns	T	2, 2.2, page 4/5	Notes that not one invidual shall assuem more than one role in the process. Small agencies with small staff offices at times use one person to serve as the Registration Authority and the Issuing Authority.	Add the statement, "**Except in extenuating circumstances**, it should be noted...." Staff shortage should serve as an extenuating circumstance.
3	CSOSA Office of Security	Joseph Burns/ Carol Holloway	E	2.2.1, page 6	Position sensitivity level 4 (critical or special sensitive) should sumbit a Standard Form 86	Submit SF-86 or equivilant. You should implement the OPM position sensitivity of 1-6 to be consistent. In addition, the fact the the LBI is initiated should be sufficient since all preliminary checks are conducted.

D = Document,1 = FIPS201, 2 = SP800-73

T=Type of Comment, E = editorial, T = technical

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
4	CSOSA Office of Security	Joseph Burns	T/E	2.2.1, table 2-2, page 6	Recommend that everyone should have to present their source identification documents, undergo a NAC check with credit to include fingerprints. This should be enough to determine one's suitability be hired as a government employee and verify identity for issuance of credentials. Persons with a position sensitivity level 3 or 4 will have to wait MUCH longer than an employee hired the same day in a low position sentivity for their credential...even if both persons are employed in the same building.	Issue credentials based on the same uniform check. NAC with credit.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
5	CSOSA Office of Security	Joseph Burns/ Carol Holloway	T/E	2.2.1, table 2-2, page 6	The overall process to obtain a form of government I.D. as proposed is currently more prohibitive than being approved to be hired and obtaining an interim Secret security clearance upon entry on duty. It makes no sense to bring somebody on board, issue him or her an interim Secret clearance and then tell him or her they cannot come to work or have to be escorted because they don't have an I.D. yet. A Position Sensitivity Level 1 requires actual verification of submitted documents (i.e. driver's license and birth certificate), yet with levels 2, 3, and 4 the OPM check to be completed WILL NOT be verifying the source documents. This is inconsistent policy....levels 2, 3, and 4 should be required to at least match the level 1 standard. The use of OPM I-9 documents for authentication appears to be a valid means of identifying and authenticating someone's identity. However, for each Agency to independently verify the I-9 documents with the issuing agency could be time prohibitive. Additonally, many contracts expire before a background investigtation can be completed.	Issue credentials based on the same uniform check. NAC with credit. If these procedures are not modified, agencies could choose to bypass extra security processing by just hiring personnel at a lower level one.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
6	CSOSA Office of Security	Joseph Burns/ Carol Holloway	T/E	2.2.1, table 2-2, page 6	An employee may need a security clearance (critical sensitive position) and will have to fill out a form SF-86 for a clearance and further fill out a SF-85P for a level 2, 3, or 4 I.D. card. Additionally, the Agency may need to have 2 investigations completed on the employee. A NACI may need to be done for I.D. purposes and then an additional SSBI may need to be done for national security and personnel sensitivity reasons. An agency would want to issue the I.D. card as soon as possible and SSBI cases can take from 1 month to 1 year to complete while NACI's can be done quicker. Most likely the agency would absorb extra cost to get a NACI done and the I.D. card issued. This would pose undue hardship and extra adjudicative work for agency security offices. Again, inconsistent policy between existing personnel security and draft PIV.	Issue credentials based on the same uniform check. NAC with credit. If the Interim Security requirements are used to grant access to national security information, why are thye not good enough to have an federal identification card. It is inconsistent that a federal government agency can grant someone interim classified security clearnce but deny buidling access.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
7	CSOSA Office of Security	Joseph Burns/ Carol Holloway	E	2.2.3	Employees who are on board having to undergo visitor procedures will severely impact federal agencies effectiveness in the successful completion of their mission. This will also undermine agency morale.	Agencies should be allowed to issue a temporary access card that will allow full access to their facilities as they feel comfortable allowing an employee pending a final credential. Currently the government has the authority to waive certain checks if it is in the best interest of the govt./national security. Why should obtaining an access card be more strict then granting access to classified?
8	CSOSA Office of Security	Joseph Burns	E and question	3.2.1 page 11	Will agencies cooperating with other Agencies in using the PIV system to grant access to all people authorized be a mandatory or voluntary procedure? Many agencies may want to retain their own access control levels.	Has there been a query of other federal agencies to gauge their comfort level in granting access to federal employees from other agencies to their buildings.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
9	CSOSA Office of Security	Joseph Burns	E	3.3 page 12	The access control subsystem should be included as a part of the PIV System Front-End Subsystem. The front end subsystem indicated that the PIV card, card and biometric readers are part of the front end subsystem....these same items are ALSO part of any access control system. These two systems are integrated and cannot work without each other. The same goes as the PIV Card Issue and Management Subsystem	The physical access control system should be made part of the PIV System Front End Subsystem and PIV Card Issuance and Management Subsystem. The access control system is integrated into both PIV systems.
10	CSOSA Office of Security	Joseph Burns	E	3.3.2	The applicant registration data being stored in a registration repository will most likely require federal agencies to CHANGE their existing access control systems to accomadate this requirement. Adding PIN codes or biometrics to readers will also require a change to access control systems.	Cost concerns and disposition of existing legacy systems that may be relatively new systems.
11	CSOSA Office of Security	Joseph Burns	E	4.1.3.g	Not being able to punch a PIV card will leave the credential holder nothing to secure the card to their body or person. Currently many agencies use small punch holes to secure cards to neck chains or card holder clips	PIV cards may be punched with holes only if for display purposes only such actions will not affect the operation of the PIV card.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
	CSOSA Office of Security	Carol Holloway	E,G	4.1.4 page 19	Delete the mandatory (Employee Affliiation)	Currently the requirement is that the agency is listed. Why break it down further to what staff the employee is assigned?
	CSOSA Office of Security	Carol Holloway	E,G	4.1.4.2 page 20	Delete requirement for SSN and DOB.	If for some reason the card is in fact ever lost we are just giving criminals the opportunity to assume another identify because they will be provided will all of the vital information (ssn, dob, name etc.).
12	CSOSA Office of Security	Joseph Burns	E	4.4 page 30	The biometric data being stored to a card will most likely require federal agencies to CHANGE their existing access control systems to accomadate this requirement as these will also be required to be collected and stored into the access control system as part of card issuance.	Cost concerns and disposition of existing legacy systems that may be relatively new systems.
13	CSOSA Office of Security	Joseph Burns	E	4.4.5.1 page 35	The facial pixel requirements conforming with existing publications and needing to be located at specific pixel locations may have requirements that exceed the capabilities of existing legacy access control/credentialing systems.	Cost concerns and disposition of existing legacy systems that may be relatively new systems.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
14	CSOSA Office of Security	Joseph Burns	E	5.2.4.2	For re-issuance, an Agency should be able to use its discretion as to whether new personalization (image, fingerprints) is required. If a card is issued in December, lost in January and reissued a month later the image and fingerprints are still relatively new.	Agency discretion for re-issuance
	CSOSA Office of Security	Carol Holloway	E	5-1 page 41	We should use the 1-6 standard that OPM has in place for position senstivities	HSPD should be consistent with OPM federal requirements for background investigations.
	CSOSA Office of Security	Carol Holloway	E	5-2 page 42	Position Sensitivity levels should be consistent with OPM and so should the investigative standards	HSPD should be consistent with OPM federal requirements for background investigations.
	CSOSA Office of Security	Joseph Burns	E	A.2.5, page 63	"Implementing agencies shall rely upon regular audit reviews by trusted third parties." Agencies should be able to use their own independent third party sources such as OIG or Office of Professional Responsibility.	Agencies should be able to use their own independent third party audit sources.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
	CSOSA Office of Security	Carol Holloway	E, T	Appendix d, page 70 and 71	Delete current description of what is in the LBI, BI, NACI etc. because it implies that all is "PERSONAL COVERAGE".	Use OPM listing of what is in each investigation since they are the ones that set the standards and the do the investigations for the majority of the federal government.
				NIST SPEC PUB 80073		
	CSOSA Office of Security	Joseph Burns			NO COMMENTS	

D = Document,1 = FIPS201, 2 = SP800-73

T=Type of Comment, E = editorial, T = technical

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial,	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 = editorial, T = technical