Subject: Comments on Public Draft FIPS 201
From: "Tsacoumis, Perry" <perry.tsacoumis@ngc.com>
To: <DraftFips201@nist.gov>

On behalf of Northrop Grumman Information Technology / Defense Enterprise Solutions, and also on behalf of the Federation for Identity and Cross-Credentialing Systems (FiXS), I am pleased to submit the following comments for your review and consideration.

Please see attached file.

<<Comments.xls>>

Should you have any comments, questions, and/or concerns regarding the comments contained herein, and/or my particular role in representation, please do not hesitate to contact me at your earliest convenience.

there's no limit to what a project can accomplish so long as nobody cares who gets the credit

Perry Tsacoumis
Contributing Architect & Technical Co-Chair, Project Manager DCCIS
Lead, FiXs Architecture Team
(Defense Cross Credentialing Identification System /
Federation of Identity and Cross Credentialing Systems)
Northrop Grumman-Information Technology (<http://www.northropgrummanit.com/>>)
7575 Colshire Drive (Mailstop C 6 W 2)
McLean, VA 22102
Phone: 703-556-1507
Toll-Free: 1-800-457-2122
Fax: 703-556-1755


Comments.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
1	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		2.2	"…one individual shall not assume more than one role in this process" – How do the PIV Officials and Authorities obtain a PIV card, if they cannot assume the role of "Applicant"?	Need to describe how the PIV Officials & Authorities initially get a PIV card
2	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		2.2	Missing Role of "System Auditor". This role is first identified in A.2.5	Need to add role "PIV System Auditor" (See A.2.5 – "The PIV System Auditor may not hold any other operational role in the system")
3	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		2.2.1	Form I-9	please consider more stringent guidelines, as being proposed by DCCIS/FiXS governance Council (Form I-9 Plus)
4	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		2.2.1	How many times can an Applicant apply for a PIV, before he/she is permanently denied?	Need to define ELSE clauses in the Policy, for error conditions, situations which can/may/will occur
5	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			What if the Requesting Official denies the application?	
6	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			What if the Authorizing Official denies the application?	
7	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			What if the Registration Authority denies the application?	
8	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			What if the Issuing Authority denies the application?	
9	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			What is there is an un-successful background check? What happens to the applicant?	
10	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			What if there isn't enough life history to conduct a background check?	
11	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		2.2.1	What are the "expected", "required", "mandatory" time frames for the entire process? Each of the sub-processes?	
12	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		2.2.2	When a govt emp transfers from one agency/dept/org to another, are there any allowances for transferring records? Or does the entire process have to be re-iterated in every single case?	
13	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		3.2		Applicant has well-defined rights under Privacy Act see http://www.usdoj.gov/04foia/privstat.htm
14	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		3.3.3	"logical resource"	need to add "the network" itself as part of this domain. Current definition seems to imply that anybody can access the network.
15	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		Figure 3-2		Consider adding "Audit Trail" to diagram
16	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		4.1.4	DoD CAC Program includes "Cadency" (Jr, Sr, III, IV, etc) in Zone 2 – Name	Consider including Cadency to Zone 2 – Name.
17	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		4.1.4	is "Position Sensitivity Level" stored anywhere on the card? Physical (front/back) or on the chip?	
18	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		4.1.6	"PIV Card must be activated to perform privileged operations".	Consider defining the scope, risks & liabilities of the term "privileged operations".
19	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		4.4	What is the process if a duplicate fingerprint is found during the 1-to-many matching? What happens? Who gets notified? Who is responsible for taking action? What are the time constraints?	
20	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		4.4.4	Using TWO fingerprints for card authentication	Are you really sure that you want to compare TWO (BOTH) fingerprints during the PIV Card authentication process?
21	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		4.4.5.7	Background color is inconsitent	Para 4.1.4.1 (Figure 4-1) says a "light blue background"

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, T-Technical)	Section, Annex, etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
22	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)		Section 5	Renewal - What is the process for notifying a person of the need to renew their PIV Card? What if the person does not renew their PIV card w/in that time frame?	
23	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			Re-issuance -- What is the responsibility of the cardholder, in terms of notification? Need to record the reason for re-issuance (expired, compromised, lost or stolen, change in emp status, etc).	
24	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)			Revocation --	Consider a separately numbered paragraph on this very important subject.
25	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)				Consider the following as a requirement: "No Unauthorized persons shall be granted access to any Federal physical or logical resource, using a PIV card"
26	NGIT / DES & FIXS Governance Council	Perry Tsacoumis (perry.tsacoumis@ngc.com)				Consider the following as a requirement: "No illegal or unauthorized PIV cards shall be used for the purpose of requesting access to a US Federal physical or logical resource"
27				GENERAL		Need to add Privacy Act compliance requirements (for ex: where's the Audit Trail of access transactions?) see http://www.usdoj.gov/04foia/privstat.htm; Esp note the following: [c] accting of certain disclosures; [c] access to records; [e] agency rpts; [f] agency rules
28				GENERAL		Need to include references to appropriate Security Requirements (for ex: for DoD, need to refer to DITSCAP (DIACAP, once released), and/or NISPOM).

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