Comments Received on NIST Draft Special Publication 800-152
(March 2015)

From: Dennis K. Branstad
Date: December 31, 2014

#	Type	Page #	Line #	Section	Comment (with suggestion)	
1	E	24	490	PA:3.2	"incorrect user input faults" should either be "incorrect user inputs" or "user input faults."	
2	E	25	514	PR:3.3	"(e.g.," is missing a ")" which must be inserted in the appropriate place.	
3	E	25	516-518		A goal of "designing, implementing, and operating" any system is to avoid complex and expensive litigation. Intellectual property rights, such as copyrights, trademarks, and patents should be respected as required by law. Therefore, it is best to ~~know~~ "identify" and resolve possible legal issues as soon as possible. [Insert quoted words and delete word as noted]	
4	E	28	584	Fig. 2	Problem with the "u" in Configuration on the bottom of the diagram;	
5	E	29	623		"supporting and adopting" should be changed to "adopting, supporting, and enforcing" to show that a policy first has to be adopted (when creating an FCKMS that is "built on" a particular CKMS), then implemented within the FCKMS so it can be supported and even enforced by the FCKMS.	
6	E	32	694		"accommodates" is different than either supports or enforces; suggest sticking with "supports"	
7	E	34	730	PR:4.9	"relationship between" should be "relationships among"	
8	E	34	736		"granting" should be "being granted"	
9	E	35	752		"its owner" should be "its subject or its owner"	
10	E	35	752		"related events" should be "specified events" (many events are related but these	

					relationships are not sensitive; they must be specified in order to be provided unlinkability)	
11	E	36	795	PR:4.15	"service" should be "transaction or service" to be like the discussion	
12	E	43	1003	PR:5.2	"A Federal CKMS **shall** train" should have a footnote that says, "A Federal CKMS consists of components and devices but also includes people authorized to perform specific roles. An FCKMS can therefore be personalized in sentences. For example, training could involve both training personnel and automated training services of the FCKMS itself."	
13	E	44	1013		"data integrity," should be "data integrity assurance,"	
14	E	45	1030	PR:6.1	**"shall** support all the key types and lengths specified in the CKMS design" may be not be always desired or acceptable (e.g., the CKMS may support some algorithm and key length that is neither needed nor allowed by the FCKMS Policy). Change to "…in the CKMS design and allowed/required in the FCKMS policy."	
15	E	45	1050		The footnote starting "Domain parameters " should start "Domain parameters in this context refer to specific cryptographic algorithms and NOT to Security Policy Domains …"	
16	E	49	1191	PA:6.9	**"shall** support all metadata elements that are specified in its CKMS design" perhaps should have appended "and that are required/allowed by the FCKMS Policy"	
17	E	79	2085		"could be detected" should be changed to "can be detected"	
18	E	90	2323		"principles" should be "procedures"	
19	E	91	2327		"consist of" should be "include"	
20	E	92	2351		"may be required" should be "should be performed" or "must be performed"?	
21	E	101	2547		"should" should be "must"	

NOTE: This is now a very useful and well written document. I like the format very much.
I really like that you tied this profile to other NIST documents by adding a reference column in the RAF tables.
I am very happy that you included a cleaner version of policy discussions in relevant sections.

From: Sam <samuel.wilke@att.net>
Date: Thursday, February 19, 2015

#	Type	Page #	Line #	Section	Comment (with rationale)	Suggested Change
1	G	58	1443	6.4.x	The term "may" is used multiple times regarding key management. The use of "should" (PA) and "could" (PF) are also used throughout this section. This has the potential to be misinterpreted or used to avoid implementation of controls.	Examine to determine clarity and intent of key management actions.
2	E	127	3131	Appendix A: References	Review references to ensure they are current. Rationale: 800-53 Rev. 3 is cited although 800-53 Rev. 4 is published. "NIST Special Publication 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009."	Update references to reflect current/applicable publications.

From: "Michael W. Harris" <fnb0@cdc.gov>
Date: Friday, February 6, 2015

CDC has no comments to provide on the *Draft Special Publication 800-152, A Profile for U.S. Federal Cryptographic Key Management Systems*.

Thank you for the opportunity to review and comment.