Received Comment on SP 800-131C

Steve Ratcliff, ICSA Labs.....2
Mike Grimm, Microsoft.....3
Ashit Vora, Cisco.....5
Stephanie Eckgren, Infogard.....6
Jon Geater, Thales Security 7

From: Ratcliffe, Steve <sratcliffe@icsalabs.com>
Date: February 28, 2011

Page 7
Remove the two "[" from:
Laboratories to the CAVP or CMVP. An example of an implementation that conforms to only part of [FIPS 186-3 might be an implementation that p[erforms key generation but does not perform key pair generation.

From: Mike Grimm mgrimm@exchange.microsoft.com
Date: March 31, 2011

Section	Page #	Draft Text	Comment
2.1	6	Table on Page 6	· Please provide a table number to enable references. · It is unclear to the reader why these three columns are formatted in this way and not, for example, in separate tables. It may be useful to add a column for security strength, to make this clearer. · We would also suggest adding a note to the DSA entry for L=1024, N=160 pointing out that it is subject to the SP 800-131A transition.
3	7	"An example of an implementation that conforms to only part of [FIPS 186-3 might be an implementation that p[erforms key generation but does not perform key pair generation."	Multiple typographical errors: · The title of this section "Validation Transition Plan" has the final n in blue; the rest of the document is in black. · Please add a closing "]" character after "186-3" · Please remove the "[" character from the word "performs".
3	7-9	"The testing of new implementations of disallowed key lengths for digital signature generation may be performed by the CST laboratories independently from CAVP validation testing using test tools previously provided for validation testing. The test results should not be submitted to the CAVP for validation."	· When CAVP no longer performs validation testing for disallowed algorithms, can the corresponding validation testing tools be made available to the general public? Since many vendors may still implement disallowed algorithms for interoperability with legacy devices, making the testing tools publicly available provides the developer with the ability to check their implementation without the additional expense of hiring a cryptographic testing laboratory. · How would such testing (of disallowed key lengths) be documented in the Security Policy? · Will similar provisions apply to testing of FIPS 186-3 implementations for disallowed key lengths after 1/1/2014?
Appendix A	10	"Note: As appropriate, the CMVP will only	It isn't clear whether the vendor may modify the Security Policy. Please clarify whether the

		modify the module validation entry information; the Security Policy provided with each module validation will not be modified.”	vendor may provide a modified Security Policy since CMVP will not be editing these documents.

From: Ashit Vora <asvora@cisco.com>
Date: February 25, 2011

1. SP 800-131C: This document does not indicate a definitive transition date of FIPS 186-2 to FIPS 186-3. Based on Peer-2-Peer session at RSA conference, the transition date discussed was December 31, 2013. This needs to be clearly stated
2. General comment: Similar to above comment, 131A does not specific any transition date to FIPS 186-3. The general understanding was that as long as the key strength requirements are met, using FIPS 186-2 is acceptable. We would appreciate it if this is maintained as well.

From: Stephanie Eckgren <seckgren@infogard.com>
Date: March 24, 2011

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
1	General	Most, if not all, of the statements in SP 800-131C have already been made clear by SP 800-131A and SP 800-131B. SP 800-131C only adds confusion at this time.	Discontinue SP 800-131C. Instead, add a short section to SP 800-131B explaining that both FIPS 186-2 and FIPS 186-3 are accepted as long as they meet the rules of SP 800-131A. FIPS 186-2 will naturally be phased out. (This new section could also include the RNG statement in SP 800-131B, Section 3.2, Paragraph 3).	When SP 800-131A Section 3 was modified to include FIPS 186-2, most, if not all, questions were answered. It is clear that you will accept FIPS 186-2 AND FIPS 186-3 algorithms if they meet the requirements of SP 800-131A. It is clear that you will accept FIPS 186-2 AND FIPS 186-3 as laid out in SP 800-131B.
2	General	The clarifications made about "domain parameter generation", "domain parameter validation", "key pair generation", and "public key validation" were good. But they could be simplified into one paragraph and added to SP 800-131A.	Add a couple of sentences to SP 800-131 A Section 3 clarifying that: - The requirements for "Digital Signature Generation" also apply to "Domain Parameter Generation" and "Key Pair Generation". - The requirements for "Digital Signature Verification" also apply to "Domain Parameter Validation" and "Public Key Validation".	The clarifications made are important but they could be made more concise and in a more appropriate place (i.e., SP 800-131A Section 3).

From: Jon Geater <Jon.Geater@thales-esecurity.com>
Date: March 31, 2011

1. *"New implementations refer to cryptographic modules that are either new modules or the revalidation of modules where less than 30% of security-relevant mechanisms have changed"*

Surely this is the wrong sense? Should this not be "…more than 30%"?

2. *"It is the user's responsibility to determine that the algorithms and key sizes utilized in their system are in compliance"*

Thank you for this explicit clarification.