Comments Received on NIST SP 800-140Br1 Initial Public Draft and CMVP Responses

Comment period closed July 12, 2022 – Second public draft published October 17, 2022

Included below are all the comments received in response to the Initial Public Draft of NIST SP 800-140Br1, posted May 12, 2022. The comments have been organized by issue/section. There is an initial set of general comments followed by a set of comments related to specific sections of the document.

General Comments

Category	Comment	Source	CMVP Response
Web Cryptik Input	Various sections list input method as "Web Cryptik", but it is unclear how Web Cryptik is populated, used, and safeguards Vendor proprietary data:	Cisco	In addition to the direct entry of the table information through Web Cryptik, we are providing a json schema which can be used to develop the json separately and upload into Web Cryptik. In addition, we are providing a structured document definition and template for non-table SP sections instead of using Web Cryptik for rich-text entry. The information for the SP tables will be inserted into this template document, from which the final SP will be generated. This will be available to the vendors and labs prior to finalizing. The CAVP Filtered json endpoints will also be available to labs/vendors so that they could do the selection process within
	Does the Test Lab input Vendor information into Web Cryptik?	Cisco	
	Have you considered Vendor input the SP data instead of the lab? Manual input of SP data by the lab into Web Cryptik is too much work for the lab.	Graham Costa (Thales) at presentation	
	Web Cryptik is cumbersome. Have you considered a JSON entry input to import data?	Renauldt (atsec) at presentation	
	For the SP structure, please consider making an outline document as a template available on the CMVP portal to be used as a base for all labs & vendors. SP structure file is then exported into Web Cryptik. The SP is a living document. Web Cryptik is not efficient. The lab must focus on Content and not Data Entry.	Yi (atsec) at presentation	
	Using Web Cryptik to enter the required information is cumbersome and time consuming. The text boxes are sometimes too small to fit the text written with. Possible modification suggested would be to 1) update the web-cryptik to allow for importing of field content. 2) allow for text boxes to expand to fit text contained within.	atsec	
	when entering repetitive information (e.g. CAVP certificates), entering the information manually for anything more than 10 entries becomes time consuming. Possible modification suggested would be to 1) update the web-cryptik to allow for importing of field content.	atsec	
	Section 6.3 requires Web Cryptik being the data input method. This prevents the collaboration between a vendor and a lab in composing the SP. The current Web Cryptik interface is very limited for data entry and it significantly hinders the lab's productivity. SP 800-140B can define the format and required content of an SP, but it shall not to mandate using which tool to write an SP.	atsec	

Category	Comment	Source	CMVP Response
	It is strongly recommended to have an import/export function provided by the Web Cryptik where a template WORD SP can be exported from the Web Cryptik, allowing the SP to be completed jointly by the vendor and the lab, then the completed SP can be imported into the Web Cryptik.		the json and submit the filtered CAVP certificate json files.
	How can vendors and labs work together to input data into Web Cryptik? What is currently slated as the lab's sole responsibility to access Web Cryptik may seem like a daunting data entry type task, especially when it comes to SSPs, SFIs, and Approved algorithms. We estimate this task could take over a week for one of our more complex product. Does the CMVP plan to provide a provision for vendors to contribute to the inputs of this tool? Thales believes it would solve several issues beyond the 'data entry' task set up for the lab. To name a few, future re use of the exported files could be advantageous for labs with similar products. Vendors with this exported tool data could also take their SSP/SFI/Algorithm 'data' to other labs, rather than their lists of 'data' belonging to a single lab.	Thales	
Complexity of defining and inputting information	My general concern with the proposal is the effort and complexity of inputting the information through a webUI but I can see ultimately how you could create records for keys, services and crypto and then go through some kind of process to define relationships but it's super non-trivial and even as a vendor think this would likely be something that would take us weeks if not months to do and check. All to say I don't see this as viable if it's the lab that is responsible for entering the information. I am pro automating aspects of the SP to avoid mistakes but do think that the implementation is going to be the crux as to whether this brings any benefits and/or whether you simply switch from a world of human errors at the point of writing SP, to human errors at the point of data-entry through web-cryptic.	Graham Costa (Thales) separate email	
Data Validation	General Comment: We assume that there will be some automated checking build into Web Cryptik. To avoid possible unexpected data import exceptions, we propose this document define the set of rules that will be used to validate the inter-dependencies between the various tables. e.g. We shouldn't be able to define a SFI if it's not mapped to at least one service. We shouldn't be able to define an approved algorithm unless it's mapped to at least one SFI. We shouldn't be able to define an SSP if not mapped to SFI etc.	Thales	
Data Definition/ Validation	General Comment: There are many situations where a complete set of enumerations for certain entries could but aren't defined by this document. We strongly suggest that	Thales	Yes, these will be included, where possible, and

Category	Comment	Source	CMVP Response
	before publication, this document define standard sets of entries for table entries with only a finite known set of options, e.g. 'Type' in Pre-Operational Self-Tests (B.2.10.1) there is no reason why the list of allowed test types can't be enumerated now and will help with standardization and implementation of tools to support the updated SP formats.		become part of the json schema.
Section 6.3	Minor (editorial) - Typo in section 6.3, fix 'PFD' to 'PDF'.	Thales	Updated
	Minor (editorial) - it may be clearer to have the three options 'Web Cryptic', 'CAVP Algorithm-Mode-Property Selection' and 'Vendor Documents Uploads' as bullets. At the moment, they look a little off as the format is similar to the sections in the document and where it initially read when we reviewed like these should be separate sub-sections (i.e. 6.3.1, 6.3.2 and 6.3.3) that had been mis-numbered/Internal Comments to S&C Team	Thales	Updated with change in format.
Optional vs required	In SP functions – Can you give options as to what's explicit and what's optional?	Renauldt (atsec) at presentation	Added designations for optional document sections and table columns.
Misc	Is this information used to generate both the Security Policy (SP) and Test Report? How are these documents different? If they are not different, it is unclear how this would improve the CMVP review process.	Cisco	Yes, they are different. There is an initiative currently underway in the NCCoE CMVP Automation project to identify the TEs that can be satisfied with information identified here. Once that process has completed, Web Cryptik can be updated to automatically fill in the corresponding TEs.
Trial Period	Have you considered a trial / pilot period to test efficiencies?	Graham Costa (Thales) at presentation	Yes – we will have a trial period.
Flexibility of Info	Will there be flexibility where a statement language is used instead of a table (e.g. vendor affirmed OE)	Walker Riley (atsec) at presentation	There will be the option to include statements in addition to the structured

Category	Comment	Source	CMVP Response
			table information, but not in place of it.
	Will there be table flexibility? Presently there are 5 tables. (Primarily related to SSP tables)	Sweepneela (atsec) at presentation	No – to achieve the results, all of the structured information for the modules will need to follow the same structure. Some columns could be empty/NA. The presentation of the information in the SP would be able to only include applicable columns. It could also combine and/or separate structured information suitable to differences in the modules.
Grandfathered	Will the previous module submissions be grandfathered?	Mark Boire (??) at presentation	Yes.
Purpose of the Security Policy	What is the Security Policy's function, purpose, reason for existence? Who is reading it? Our concern is that the Security Policy is moving farther away from its original intended purpose of providing Users with FIPS understandable information as it relates to operational use. It seem that the SP is being used more and more solely for the CMVP reviewer. There is so much convoluted information in it, making it difficult to read, understand or use. Users need to know how to place the module into its FIPS mode of operation. Protocols supported. Algorithms available. Beyond that the document starts to overwhelm the user with information that is beyond their cryptographic knowledge. Things like Security Levels, cryptographic boundary, module interfaces, redundancy in algorithms, entropy and Roles mean nothing to the User trying to place a module into FIPS mode of operation. All of this may seem nice in an academic world but in the real User world "precise specification of the security rules under which a cryptographic module shall operate" can become convoluted with too much information yet not enough true operational information.	Cisco	This comment would appropriately be discussed separately. This update only organizes previously defined requirements for the SP.

Category	Comment	Source	CMVP Response
Proprietary Data Protection	How is Web Cryptik protecting Vendor data and what safeguards are in place to ensure no proprietary information is entered in Web Cryptik.	Cisco	We believe the proprietary data concern is answered in first item above by providing the entire SP prior to finalization.
	What is the review process to ensure that Vendor proprietary data is provided to CMVP but not published in the non-proprietary SP?	Cisco	
	How do you delineate vendor proprietary and non-proprietary information?	Chris (Oracle) at presentation	
	For many years, vendors have owned creating a security policy document and can control the type of information that gets disclosed publicly. With SP 800-140Br1, the content for the security policy is being driven by the information that is provided by vendors and given to Labs as evidence and that information gets entered into web cryptic. We understand that the CMVP wish to automate the security policy creation to make it consistent with vendor validation reports. We also want to be clear that vendor information is required in order to create a validation test report and in general, vendors do not have a problem disclosing information needed to substantiate that a cryptographic module meets the requirements of FIPS 140-3. What vendors are concerned about is detailed information about a cryptographic module that if made public could compromise the security of a cryptographic module. We believe that if a security policy document will be generated from proprietary information from a vendor, that vendors must have a say in the approval of the final publication of the document. Currently the guidance offers no recourse to vendors to have a say in what information gets published and this concerns us. We are more than happy to work with the CMVP to help disclose information needed for a FIPS 140-3 certification but not at the risk of compromising the security of the cryptographic module. Thank you.	Oracle	
Example SP	NIST SP 800-140Brev1 adds several new tables and concepts. Please provide an example SP for hardware, software, and firmware with these new elements	Cisco	Two examples have been developed and will be provided.
N/A Sections	Please confirm, if a section is “Not Applicable” to a Vendor, is the section included and “Not Applicable” stated?	Cisco	We have marked the SP sections – which are optional and could be removed and which will need to exist and be identified as N/A.

Category	Comment	Source	CMVP Response
Definition of "techniques"	The term "techniques" is used throughout the document (and ISO) but never defined and not used consistently. For example: SSP Storage - Specify the SSP storage technique(s). [AnnexB:] Annex B does not detail techniques; however, it does provide EPROM as an example. EPROM is a type of memory, not a technique, way of carrying out a particular task, especially the execution or performance. Please clarify the definition of "technique" and provide an example of what is required.	Cisco	Changed Annex B text.
Duplication of Requirement Information	Based on our reading, the purpose of sections 6.1 – 6.3 is to identify additions/changes to the ISOs SP standards. These sections reference documents such as SP800-140:VE02.20.04 and the FIPS 140-3 Implementation Guidance (IG). Why is the text from these documents being inserted here? The IG is frequently updated. When an IG is updated a new version of the Special Publication will be required. References to the other documents are helpful, but it is redundant to have the text in two places and difficult to maintain.	Cisco	Agreed. We have removed the IG requirements and will separately work to create a document that contains the collected SP requirements and is updated appropriately.
	Section 6.2 includes many specific IGs and their current text. IGs are subject to change more frequently than the SP 800-140B. It's better to include a statement that IGs should reference to the latest publication whiles the included text are taken from a particular edition published on YYYY-MM-DD (To Be Specified by the SP 800-140B authors).	atsec	
	Sections B.2.2, B.2.3, B.2.4, B.2.5, B.2.7, B.2.9 and B.2.10. Whilst we recognize the value of gathering all security policy related requirements in a single document, we are concerned that SP800-140B will get stale quickly and where the IG are likely to be updated more often than SP800-140B. As a suggestion, we'd propose adding a statement to section 6.1. to ensure that the source documents are kept as the authoritive source of requirements with SP800-140B only bringing them together for convenience. Example statement "Where source documents cited as the origin of requirements included in this section are updated, the source documents should be taken as authoritive over copies of requirements in SP800-140Br1."	Thales	

Section-Specific Comments

Category	Comment	Source	CMVP Response
Section 6.3 (Line 655):	Update "sub-section and upload it as a PFD file" to "sub-section and upload it as a PDF file"	Cisco	Updated
B.2.2.6, B.2.2.7, B. 2.6.2 - Operating Environments Tables	Please clarify why two tables are needed. These tables contain the same information. As stated above, when information is listed more than once, there is greater risk for error.	Cisco	The tables in this section were updated. Given that the information is json and can be easily repeated, we have left the optional columns in the tables.
	I'm in the process of reviewing a security policy and have noticed something that I think would be helpful to tidy up: OE requirements. In the current version of 140B, there are OE requirements in both B.2.2 and B.2.6. I spend a lot of time scrolling between these two areas. There's also some duplication – listing the OS and tested platforms being the example that prompted this suggestion.	Lightship - Brent	
	PAA/Acceleration is not relevant to all module and merely bloats the table with unnecessary information (i.e. "None") allow the PAA/Acceleration column to be optional for modules that do not implement PAA.	atsec	
	"Distinguishing Features" is also not relevant to all module and merely bloats the table with unnecessary information (i.e. "None") allow the "Distinguishing Features" column to be optional.	atsec	
	Should these not also include the hardware platform or at minimum CPU alongside the OS?	Thales	
B.2.2.8, B.2.2.9 - Boundary Definitions	19790:2012 and with it 140-3, does not define 'Physical Boundary' as being a defined term independent from 'Cryptographic Boundary'. As such, IF NIST wants the Security Policy to list a 'physical boundary' as being independent from the 'cryptographic boundary' it will separately need to define what the 'physical boundary' is to be defined as.	Thales	Agreed. Instead of 'Physical Boundary' we have incorporated the 140-3 concept of TOEPP.
	in a very similar sent to the comment above - it's not clear what the 'Physical Perimeter' is as term not defined in 19790 and where at the moment, the requirement statement is identical between section B.2.2.8 and B.2.2.9 Our feel here is that it's likely that section B.2.2.9 Physical Perimeter is not needed.	Thales	Agreed. We removed the "Physical Perimeter" section.

Category	Comment	Source	CMVP Response
B.2.2.13 - CAVP Cert Filter Selection	The current way algorithm certificates are formatted by 'implementation suites' is challenging for what Thales envisions SP800-140B evolving into. In the event that an entire 'implementation suite' is not utilized by a particular module (i.e. specific algorithms/modes are disabled in FW), will Web Cryptik be able to selectively identify these algorithm parameters and modes which are specifically supported by the module?	Thales	We believe that the 140-3 requirement to distinguish modules that implement different cryptography answers this question/issue. It is a correct assumption that the current design of the module's information doesn't provide for different implementation suites.
B.2.2.14 – VA Algos B.2.2.15 – Non Approved Algos	"algorithm properties" will need to be typed by the user, but there is no clear information what the content should be. 1) make the "algorithm properties" selectable like is done for "Algorithm" so that the content in this field is consistent and not left up to the SP author to define. 2) provide a definitive list of properties that can be entered for each vendor affirmed algorithm.	atsec	For the vendor affirmed table, we will be providing specific information required for the few algorithms that can currently be vendor affirmed. At present, information for the most frequent (CKG) has been added.
	It states that "A module can (and often does) have more than one implementation for a given Security Function type". The "can" in this statement seems to imply this table could be optional. It seems that this table is intended to supplement the "services" tables. allow SFI Table to be optional if there is nothing new to add from the "Services" tables.	atsec	The table is not optional. What we've seen in Services listings can be very broad and encompass many different SFs and makes it difficult to decipher.
	It states "For many modules, there would likely be one SFI for a SF type". Does this mean that there should be one table per SF type? Make explicit statement that one row from SFI table is required for each SFI type.	atsec	Which SFs are present is dependent on what is offered by the module. This would be tied to the services. Every service

<table>
<tr><th>Category</th><th>Comment</th><th>Source</th><th>CMVP Response</th></tr>
<tr><td></td><td></td><td></td><td>should include at least one SFI. Every SFI should be represented by at least one service. Every algorithm should be incorporated into the SFI table.</td></tr>
<tr><td></td><td>SFI table, it is not clear what is the difference between SF properties and algorithm properties and what information is required in the type column. Also it seems the required information will already be covered with B.2.2.19, line #901

Either provide example table with few SFIs. or simplify the table as below by combining with B.2.2.19

<table><tr><th>Algorithm/SFI Name</th><th>Standard</th><th>Key/strength</th><th>Mode</th><th>CAVP Cert #</th></tr><tr><td>RSA Signature generation</td><td>FIPS 186-4</td><td>2048 bits/112 bits</td><td>PKCS</td><td>#AXXX</td></tr></table></td><td>atsec</td><td>Algorithm properties are taken directly from the CAVP testing information.

SFI properties are entered separately by the lab/vendor. We will build, over time, specific SFI properties that correspond to particular SFs. To begin, the bit-strength caveats for KTS and KAS-SSC SFs are SFI properties.

The information in B.2.2.19 is a specific place in the SP to address many SP requirements called out in the IGs. Some of these would be covered by information already presented in the SFI table and would not need to be duplicated in this section.</td></tr>
<tr><td>B.2.2.19 - Algorithm Specific Information</td><td>We're concerned this information will be confusing to the end-user of the Security Policy when taken out of context of the tables of approved and allowed algorithms. If possible, ideally the relevant statements should be woven into the bigger tables as relevant.</td><td>Thales</td><td>See above</td></tr>
</table>

Category	Comment	Source	CMVP Response
	- isn't vendor affirmation to SHA3 listed in this section duplicating an entry that would be added to B.2.2.14, 'Vendor Affirmed Algorithms'.	Thales	In this case, yes. See above.
B.2.2.20 - Key Agreement Information	- this sections feels like it will duplicate information already likely to be in Approved Algorithm Section and/or will be captured between the approved algorithm section mapped to the Security Function Implementation section. Whilst we understand KAS related information has recently been of extra interest to CMVP in relation to SP800-56Ar3 transition, we don't see why this need to be called out as it's own section in the Security Policy where-as other algorithms aren't. Where we can we should look to simplify and remove opportunity for duplications and/or inconsistencies in the security policy but where this section seems to introduce the opportunity for inconsistencies with the Approved Algorithm Section that otherwise will contain this information.	Thales	For many of the requirements addressed by the IGs (these included as well as other), many of the shall statements are answered by the algorithm table or the SFI table. Over time, and now that we have a specific SP structure, we can interpret the shall statements and indicate more specifically how they should be addressed in the SP. The information need not be duplicated. The algorithm/SFI information would be displayed here (not duplicate entry) along with other SP required information. We still believe it is beneficial to have specific sections of the SP that address certain implementations.
B.2.4.1 - Authentication Methods Table	"Strength Per Minute" fields are not found in SP800-63B nor FIPS 140-3. Provide clarification to reasoning of including this column not previously found in the original SP800-140B or allow for the column to be optional.	atsec	This column is optional.

<table>
<tr><th>Category</th><th>Comment</th><th>Source</th><th>CMVP Response</th></tr>
<tr><td rowspan="2">B.2.4.6 - Approved Services Table</td><td>Therefore too many columns and are already going out of page margin in the 800-140B document

Concise the required information and instead of writing the SFI/Algorithm, include the respective index (row number) from the B.2.2.17 table

<table><tr><th>Name & Description</th><th>Indicator</th><th>Input</th><th>Output</th><th>SFI table Index</th><th>Roles</th><th>SSP access</th></tr><tr><td>RSA Signature generation</td><td>“1”</td><td>data</td><td>private key</td><td>Row 4</td><td>CO</td><td>Private key: W</td></tr></table></td><td>atsec</td><td>In Web Cryptik, this column would be a “lookup” to the SFI table.

Also remember that these tables define the structure of json information collected and not the format that they will be displayed.</td></tr>
<tr><td>The example does not match the table. Specifically, the Security Function Implementation (SFI) table states that each SFI must be in the Security Functions (SF) table; however, the example does not show this. Also, if the SFI must be in the SF table, should one follow the other to help reduce errors in connecting information between the two tables?</td><td>Cisco</td><td>The example was only there related to the two columns it presents. Yes, this should be completed after the SFI table.</td></tr>
<tr><td>B.2.4.7 - Non-Approved Services Table</td><td>Per IG 2.4.C the indicator is only required for an approved service

Remove the "Indicator" column</td><td>atsec</td><td>Agreed.</td></tr>
<tr><td>B.2.4.9, 'Multi-Operator Authentication'</td><td>- we can't see the justification for having this as a separate section. Should this simply not be information that's added as requested if applicable to section B.2.4.1, 'Authentication Methods'? As with comments above, the more redundancy we build into the security policy, the more opportunity there are for inconsistencies.</td><td>Thales</td><td>Yes, we have included this in the previous Authentications section.</td></tr>
<tr><td>B.2.5.3 – Executable Code</td><td>Please provide clarification on information to be provided for “executable code”</td><td>Cisco</td><td>We have moved this to the Op Env section.</td></tr>
<tr><td>B.2.7.3 and B.2.7.5 – Reference Photos</td><td>Please provide additional details, such as picture size and type of image, black and white or color, jpeg, bmp</td><td>Cisco</td><td>These are details are not defined and left up to the vendor.</td></tr>
<tr><td>B.2.7.8 – Unused Seals</td><td>The SP can state that a CO must inspect the seals and store any unused seals. However, the User defines the policy. Therefore, what is the intent of this requirement? It is not reasonable to put the policy in the SP as this is controlled by the User. The SP should</td><td>Cisco</td><td>This requirement is from Annex B and states that the SP needs to specify the</td></tr>
</table>

<table>
<tr><th>Category</th><th>Comment</th><th>Source</th><th>CMVP Response</th></tr>
<tr><td></td><td>just provide guidance that this policy must be defined. If anyone, outside the User, is going to dictate this policy it must be the CMVP.</td><td></td><td>operator role responsible, not the details of how.</td></tr>
<tr><td rowspan="2">B.2.9.1 - Storage Areas
B.2.9.2 - SSP Input/Output
B.2.9.3 – Zeroization
B.2.9.4 – SSPs</td><td>There are currently four tables related to SSPs. Please consider consolidating tables as there is increased opportunity for error when managing information across tables. What is the purpose of the table starting on Line 2218? This pulls elements from the above tables and does not provide added information.</td><td>Cisco</td><td>There will be connections between the tables that will restrict information, preventing errors.

The table on line 2218 is a continuation (more columns) of the table on line 2217.</td></tr>
<tr><td>In FIPS 140-2 SP all the required information on SSP used to be listed under 1 table. Currently in the proposed draft there are 5 tables with lot of overlapping information. E.g. 1. Second table under B.2.9.4 asks about import/export (which is same as input/output) and zeroization already covered in B.2.9.2 and B.2.9.4 respectively. 2.SSP type seems redundant because Name and description of SSP will provide this information

Include only the following required information in single table by using rowwise Heading

<table><tr><td>SSP Name</td><td>RSA</td></tr><tr><td>SSP Size/Strength</td><td>2048 bits/112 bits</td></tr><tr><td>SSP Description & Usage</td><td>Signature key</td></tr><tr><td>Generated or Established By</td><td>Generated using FIPS 186-4</td></tr><tr><td>Input/Output with format</td><td>Via API call in plaintext</td></tr><tr><td>Entry/Distribution</td><td>MD/EE</td></tr><tr><td>Zeroization Method</td><td>RSA_Free() writing with zeros</td></tr></table>If there is any additional information needed then please provide the details on what is required in following columns.</td><td>atsec</td><td>Separating some of the information provides more clarity and allows us to see the details/structure of the module’s cryptography better. For example, the storage areas. Now, to know what are the different storage areas, we’d need to parse the SSP list and identify them. This requires labs/vendors to specifically and individually identify the storage areas and then use those when identifying SSP storage.

In our experience, many times the names vendors choose for the SSPs don’t make it clear what they are used for.</td></tr>
</table>

Category	Comment	Source	CMVP Response
	1. Related SSP's in 2nd table under B2.9.4 2. Operator Initiation capability		We agree that the import/exports terms (which come from Annex B) are confusing and mean the same as input/output. We've changed the column names. The type column will include CSP or PSP and then other information about the type of SSP.
	"whether the SSP(s) is imported or exported". Should this be "what method is used to import or export SSP(s)". This proposed change would be to facilitate create a mapping with the SSP I/O methods listed in the separate table. As written, the question can be answered with a 'yes' or 'no' which doesn't seem to be what's intended.	Thales	Agreed – changed.
	To keep things specific, should 'Generated or Established By and User By' not all map to an SFI? i.e. I think it's confusing to suggest these could be mapped directly to Algorithms which opens the question as to how 'Algorithms' should be differentiated from 'SFI'.	Thales	Agreed – they might not all map, but they could. This is optional.
B.2.9.5 – Entropy Sources	We agree that the ESV cert number (where applicable), entropy source name, and type should be listed in the SP; however, what is the intent of the additional information? The information in NIST SP 800-140Brev1 significantly extends what is required by the ISO and provides no value to the User. This information is only valuable to CMVP for analysis and is provided in the detailed Entropy Report. Why is this information repeated in section B.2.11.3? Maintaining information in more than one place in a document leads to error. The entropy information must only be provided in one place.	Cisco	We've updated the table and the columns. We have removed the Entropy info from Section 9.
	IG D.J (Module Specification) and IG 9.3.A (SSP Management) both ask for listing the available entropy in bits from the entropy source. IG D.J however talks about a general entropy value, whereas IG 9.3.A may touch specific security strengths per SSP.	atsec	

Category	Comment	Source	CMVP Response
	Clarify how the information of IG D.J shall be listed in Module Specification, and how the information of IG 9.3.A shall be listed in SSP Management. The clarification can be done through the use of examples.		
B.2.10.1 - Pre Operational Self-Tests and B.2.10.1 - Conditional	Type column details provide examples of KAT, PCT etc. But per IG 10.3.A, PCT is not allowed for pre-operational test. Also, per 140-3 checklist provided in June CAST test even though executed at power on should be categorized as conditional test Specify the examples of type as "KAT, fault induction test, comparison test, integrity test"	atsec	These tables were updated and the notes now include more specific information related to what is required.
	"Details" it is not clear what related information is required here Either remove the "Details" column or make it optional	atsec	Agreed – it is now optional.
	It is not clear why OE column is specified Because per FIPS rule it is not allowed for same module to execute diff algorithms on different OE, the OE only supports extra acceleration which will be included in table on line #2000. Per our understanding if there are different algorithms supported by different OEs then the module needs to be split and submitted as two different modules because in that case the offered services from the module will change based on OE. Remove the "OE" column or clarify in what situations the OE will differ.	atsec	There can be different implementations of an algorithm and this column was intended to indicate which implementation is being tested. We have changed the heading name to Location instead of OE.
	- it's not clear why these tables would list and OE? i.e. this is particularly not important for a hardware module but even for other module types, the self-tests are going to run on what-ever the platform the module is deployed on. This doesn't seem a relevant entry to have here.	Thales	
B.2.10.4 - Error States Table	"Condition" column needs to be added to specify the cause for entering into the respective Error state Replace the "Description" column with "Error condition"	atsec	Agreed. We added Condition and Recovery Method columns.
B.2.11 Life-cycle assurance	What is meant by “Rich Text Box”? Who creates this and how is it used?	Cisco	This information is now entered in the Word template.