Legend (type of comment)

E = Editorial
G = General
T = Technical

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212			A number of my comments to the previous version of FIPS 140-3 were rejected with a generic rationale that "additional detail why change X should be made needs to be provided." NIST did not contact me to request additional information to determine if the specific comments should actually be accepted or rejected. NIST should allow all reviewers the opportunity to provide the additional information that was never explicitly solicited by NIST.	
2.	NSA	TWG	New	T	Suggest that a requirement be added that states that the following critical functions should not be interruptible: key load, key zeroization, key generation, self-tests, software/firmware load, RBG for any key-related function, RBG initialization especially after power-up/restart.	
3.	CMVP	Kim Schaffer	General	G	If a form of the definition of allowed presented above is permitted then we can focus on approved rather than continuous approved and allowed statements used.	
4.	CMVP	Kim Schaffer	General		When referencing any external documents within the standard, explicitly state that these documents are "as amended".	
5.	CMVP	Matthew Scholl	General		Amendable document shall not contain shalls.	

6.	Oracle Solaris Security	Darren Moffat	General	T/G	Would the Intel AES-NI instructions be regarded as an SFMI or an HMI ? In general need clearer advice on how cryptographic instructions on an otherwise general purpose CPU should be treated. Would a PKCS#11 module on a general purpose machine using Intel AES-NI instructions be regarded as a hybrid module or a software module? Where would the cryptography boundary lie, i.e. are the AES-NI instructions inside or outside of the boundary ? Particularly when those instructions are unprivileged and can be executed either inside or outside of a FIPS module. Currently it still takes multiple instructions to implement a full algorithm like AES as the instructions tend to be at the level of key expansion and an AES round.	
7.	Oracle	Matt Ball		G	FIPS 140-2 was pretty good about using the active voice when describing the subject for a 'shall' requirement. I've noticed several instances where FIPS 140-3 uses the passive voice in a 'shall' statement, leaving the subject somewhat ambiguous. Consider combing the entire standard and ensuring that each sentence that contains the word 'shall' be written in the active voice with a clear subject to which the requirement applies. This subject is typically either "the cryptographic module", or "documentation". It should not be "the operator" or other entities that are external to the cryptographic boundary.	
8.	Oracle	Matt Ball	General	G	Consider defining the word 'shall', possibly as follows: "shall: a keyword that indicates a requirement for conformance to this standard."	
9.	Orion	MS	Overall	G	The current draft FIPS 140-3 offers several clarifications and some improvements over FIPS 140-2. For example, the concept of the trusted channel is expanded to cover remote	

					control, testing has been modified to better accommodate smart cards, and software/firmware has its own Section. None required.	
10.	Orion	MS	Overall	G	However, the case can be made that the latest draft has been watered down. FIPS 140-2 Level 4 hardware and FIPS 140-2 Levels 3 and 4 software offered a challenge to those vendors who wanted to put in the extra effort in building advanced cryptographic modules. That is no longer the case with this FIPS 140-3 draft. Establish a working group to add a Level 5 for hardware and a Level 3 for software that embody the best cryptographic principles know today. This could be a separate addendum to the initial FIPS 140-3 standard.	
11.	RSA Security LLC	Kathy Kriese and Peter Robinson	Not yet addressed	G	Certificate 1051 was awarded to a module that is a "privately linked library". On page 41 of the FAQ document http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf : ***Does the CMVP validate source code?*** No – given current technology and the requirements of FIPS 140-2, source code itself cannot be validated. ***Does the CMVP validate static libraries?*** No – given current technology and the requirements of FIPS 140-2, static libraries themselves cannot be validated. Given the Implementation Guidance and certificate 1051, we would appreciate clarity on what must be done with a "privately linked library" to ensure the module complies with the Implementation Guidance document.	

12.	Secure64 Software Corp	Bill Worley, CTO			The evident progress in the FIPS 140-3 Draft is gratifying. Clearly, much thought has gone into making the certification process more "software" friendly. It□s good to see this progress. For Secure64□s systems, though, particularly in light of actual customer experiences, we would like to offer suggestions that would further enhance the aptness and benefits of FIPS 140-3. Hence, the following five comments and explanations: 1) The categories of cryptographic modules and their operational environments are not an ideal fit to a newly emerging class of system of which Secure64□s DNS products are examples. Such systems are variously called "minimum complexity", "software appliances", or "purpose-built". We believe this class of system, containing FIPS 140-3 certified cryptographic modules, will be widespread during the FIPS 140-3 epoch. These systems are entirely software, execute on standard industry hardware platforms, and have enormously simpler operating systems. They typically embed a fixed, non-modifiable set of applications. In quantitative terms, the load image of a Secure64 DNS product is less than 10 MB in total size. The benefits of such systems are that they offer higher performance, a smaller attack surface, and a level of simplicity that enables stronger IA properties and attack defenses. In FIPS 140-3 Draft terms, software minimal complexity operating systems provide "non-modifiable" or "limited" operational environments. Cryptographic modules in such systems are solely software modules that execute on standard industry hardware platforms. But such modules cannot be	

					certified as “software” modules because the FIPS 140-3 Draft requires that “software” modules execute only under operating systems that provide fully general, modifiable operational environments. This constraint on software modules seems excessively limiting. The ideal fit for minimal complexity systems would be that FIPS 140-3 permit software operating systems to offer limited or non-modifiable operational environments as well as modifiable operational environments. This would permit cryptographic modules in such systems to be regarded as solely software and to be certified as software cryptographic modules – expanding the certifiable types of solely software systems.	
13.	Secure64 Software Corp	Bill Worley, CTO			2) The proposed Authorized and Allowed cryptographic repertoire, to the extent we see it described, is too restricted either to provide the best state of the art algorithms or to meet already known customer needs. Three examples are: PKCS#1, V2.1 (14 June 2002), on Page 15, recommends “RSAES-OAEP for new applications,” and states that “RSSAES_PKCS1-V1.5 is included only for compatibility with existing applications and is not recommended for new applications.” Countries in eastern Europe are now requesting the GOST cipher for symmetric encryption and signatures for DNSSEC. These capabilities appear impossible to provide in a cryptographic module executing in a FIPS 140-3 Approved mode. DNSSEC content is ubiquitously being signed with RSA digital signatures. In practice we find countries and organizations often selecting non-standard key sizes. One Swedish firm, for example, signs zones using 1300-bit keys (162.5 bytes). Another customer insists on 1200-bit zone signing	

					keys. With present restrictions, signatures for DNS records from multiple organizations cannot be generated within a FIPS 140-3 cryptographic module executing in FIPS approved mode. Although we understand (perhaps incorrectly) that signatures with all such key sizes can be validated, no algorithm certification, to our knowledge, exists to certify RSA cryptographic algorithms for arbitrary key lengths. It would be good to see these problems addressed in a manner that would permit a FIPS 140-3 certified cryptographic module to be sufficiently comprehensive, without high overheads for switching among multiple modes of operation. Otherwise, US Government and commercial systems will be forced also to rely upon cryptographic capabilities extraneous to FIPS 140-3 certified cryptographic modules. This is the situation we presently face with FIPS 140-2.	
14.	Secure64 Software Corp	Bill Worley, CTO			3) Future systems, both standard and custom, will tightly integrate Trusted Platform Modules (TPM□s) into both hardware and software. Although TCG specifications may be expansive and complex, TPM□s do offer basic functions that can be beneficial for high IA systems. Many TPM□s contain hardware non-deterministic random number generators, useful for seeding deterministic RBGs. Each TPM also contains a unique “endorsement key” and its certificate (often RSA 2048-bits RSAES-OAEP for reasons cited in comment 2). This can provide a cryptographically usable root of identification for a specific hardware platform – a basis for a key tree to ensure a system loader has not been compromised, to recover keys permitting decryption of an encrypted and signed loadable system image, and to ensure that a system image is loadable only on an authorized customer hardware platform. We encourage FIPS 140-3 to embrace TPM□s on standard hardware platforms, and	

					sanction at least their limited employment for software operational environments and cryptographic modules. We recognize this may be regarded as a controversial suggestion, but we are convinced it can and will strengthen overall system security.	
15.	Secure64 Software Corp	Bill Worley, CTO			4) The new requirement to provide an operator command to repeat the Software and Firmware load integrity tests seems in need of clarification for cryptographic modules implemented in software. When a module first is loaded, the contents could include executable code, internal read-only data, and internal read-write data. Once the module is in operation, the read-write data may have been altered. Repeating the load integrity test would be valid only for the executable code and read-only data. Was this the intent, or was the intent only to revalidate the executable code? In either case, the specification should clarify this point.	
16.	Secure64 Software Corp	Bill Worley, CTO			5) The Draft seems mostly to focus upon cryptographic modules that require manual initialization, interaction, and other controls. Our customers want server systems that are automatic, do not require manual management, and automatically can restart themselves when needed. The 140-3 requirements should provide for such automatic operation of cryptographic modules, as well as for their manual management.	
17.	Thales e-Security		General	E	The Publication has been issued for review without the supporting Derived Test Requirements or Implementation Guidance (as referenced by some of the Annexes). Given that both of these documents help resolve issues of interpretation over 140-3 statements it is difficult to assess the full requirements of 140-3 and provide a full response. Consider issuing further draft with supporting	

					Derived Test Requirements and Implementation Guidance	
18.	NIST	Elaine Barker	General		The difference between “Appendix” and “Annex” needs to be explained, e.g., an Appendix is included in the standard, whereas an annex is on the web site.	
19.	atsec	Fiona Pattinson	Section 1 Para 5	T	The second sentence states the “The operator of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.” It is not possible to require that an operator have these responsibilities as an operator may be a process as well as an individual (see glossary of terms and acronyms) Review this statement and the expected responsibilities for the operator. Suggest “The operator of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted by the owner of the information.”	

20.	atsec	Fiona Pattinson	Section 1 Para 5	T	The second sentence states the “The operator of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.” It is not possible to require that an operator have these responsibilities as the operator (either an individual or process) of the module may not have access to or knowledge of crypto officer functions or documentation, and may not know who the owner of the information is, which residual risks apply or whether it is accepted by the information owner. Review this statement and the expected responsibilities for the operator. Suggest defining a “crypto module manager” in the glossary who is an individual and who has these responsibilities. “The manager of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted by the owner of the information.” We note that the crypto officer as well as the operator as currently defined may also be a process and therefore cannot have this human responsibility.	

21.	atsec	Fiona Pattinson	Section 1 Para 5	T	The second sentence states the “The operator of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.” It is not possible to require that an operator have these responsibilities as the operator (either an individual or process) of the module may not have access to or knowledge of crypto officer functions or documentation, and may not know who the owner of the information is, which residual risks apply or whether it is accepted by the information owner. Review this statement and the expected responsibilities for the operator. Suggest defining a “crypto module manager” in the glossary who is an individual and who has these responsibilities. “The manager of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted by the owner of the information.” We note that the crypto officer as well as the operator as currently defined may also be a process and therefore cannot have this human responsibility.	

22.	atsec	Fiona Pattinson	Section 1 Para 5	T	The second sentence states the “The operator of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.” It is not possible to require that an operator have these responsibilities as the operator (either an individual or process) of the module may not have access to or knowledge of crypto officer functions or documentation, and may not know who the owner of the information is, which residual risks apply or whether it is accepted by the information owner. Review this statement and the expected responsibilities for the operator. Suggest defining a “crypto module manager” in the glossary who is an individual and who has these responsibilities. “The manager of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted by the owner of the information.” We note that the crypto officer as well as the operator as currently defined may also be a process and therefore cannot have this human responsibility.	

23.	JCMVP		Draft Revised 1.4 2nd paragraph	T	There is a statement: “resulting in the immediate zeroization of all plaintext CSPs.” However, the requirement for security level 4 is that all CSPs are subject to be zeroized, whether CSPs are plaintext or not. Please remove “plaintext” from that sentence.	
24.	Cryptsoft	Tim Hudson	1.4	G	“This level includes all the appropriate …” – which of the security features of the lower levels are **not** appropriate? Suggested resolution: delete “appropriate”	
25.	(1)	(2)	(3)	(4)	Update the text: (5) *“… include special environmental protection features designed to detect fluctuations and respond accordingly (i.e. zeroize plaintext and encrypted CSPs or module shutdown), or…”*	
26.	(6)	(7)	(8)	(9)	(10)	
27.	Motorola	Kirk Mathews	1.4, 3rd paragraph	G	Please provide clarification on how the multi-factor authentication requirement applies to embedded modules where this type of authentication would necessarily take place outside the crypto boundary.	

28.	Motorola	Ken Fuchs	General	G	I strenuously object to the fact that software-only modules can achieve level-2 but are exempt from the Physical Security requirements. Software only modules should be limited to level-1 because they can be tampered with and there is no way to provide evidence of tamper or tamper resistance without special hardware.	
29.	NSA	TWG	1.1	E	3rd para., need "a" in "For example, the implementation of **a** Security Level 1..."; need "'" in "....provide greater security of the module**'**s CSPs, ennabling...."; and "in" in "...the module is operating **in** is crucial...."	
30.	NSA	TWG	1.2	E	3rd para., need "a" in "...discretionary access control with **a** robust...."	
31.	NSA	TWG	1.3	E	1st para., need "a" in "...Security Level 3 provides **a** requirement to mitigate...."	
32.	NSA	TWG	1.4	E	3rd para., need "a" in "At **a** minimum,...."	
33.	RSA Security LLC	Kathy Kriese and Peter Robinson	Page 2, Section 1.1, first paragraph, last sentence	T	"The module does not provide protection of Critical Security Parameters (CSPs) used or generated by the module" is unclear.	
34.	NIST	Elaine Barker	1.2, Security Level 2		“ and with the capability of assigning each user to more than one group, and that protects against unauthorized execution, modification, and reading of cryptographic software” The sentence structure here needs work,, but I couldn’t suggest a fix right now.	

35.	NIST	Elaine Barker	1.3		"If a module may operate in both an Approved and non-Approved mode, Security Level 3 requires an unambiguous indication when the module is in the Approved mode. " Wouldn't it be better to indicate when it is in the non-Approved mode? By the way, we're not supposed to capitalize "Approved" except by normal English capitalization tules.	
36.	NIST	Elaine Barker	1.4		"or to undergo environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module." When? During validation instead of providing protection features? Text changed to: "or to undergo environmental failure testing prior to validation to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module."	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Peter Kim	2.1 Approved mode of operation	E	To be clear, it should be stated or implied within the definition that non-approved algorithms are still permissible as long as they are not used in lieu of an Approved or Allowed algorithm to provide any sort of data protection, data integrity, or data authentication. It is stated later in this standard that non-Approved algorithms may be used as long as they are not claiming any cryptographic strength. Reword: "Approved mode of operation: a mode of the cryptographic module that employs only Approved or Allowed security functions (not to be confused with a specific mode of an Approved security function, e.g., AES CCM mode) to meet the requirements of this standard." OR Reword: "Approved mode of operation: a mode of the cryptographic module that employs only Approved or Allowed security functions (not to be confused with a specific mode of an Approved security function, e.g., AES CCM mode) to provide cryptographic strength."	
2.	atsec	Peter Kim	2.1	E	Several of the definitions include a portion of the word being defined in the definition itself, which is circular. Two examples: Key Establishment, Key Transport Revise the definitions or define the words being re-used within the definitions (i.e., establishment, transport).	

3.	atsec	Peter Kim	2.1 Bypass AND 4.3.3.1	T	The use of “cryptographic function” implies that it would be considered a bypass mode of operation if the module were to circumvent any sort of cryptographic processing, even if it is only a hash. Also, the definition is unclear on whether any sort of circumvention is considered a bypass or only circumvention that can be toggled. For instance, a module may only have the ability to output data to a directly connected, external storage unit in plaintext, but it might also communicate that same data encrypted over a network through a different physical port (or maybe even the same, but without the ability to toggle encryption over the network communication). In this case, it could be perceived that the directly connected transmission was a “circumventing” of the cryptographic function. Reword to: “Bypass Capability: the ability of a given service to toggle between providing cryptographic protections and wholly (or partially) circumventing those cryptographic protections.” This definition attempts to clarify that the service itself must have the option to toggle the cryptographic protections, whether by a parameter sent through or a configuration setting. If no such option exists, then it is not a bypass. In the case where any cryptographic function would be considered a bypass, then “functions” can be re-instated in place of “protections” above.	

4.	atsec	Fiona Pattinson	2.1 Key transport	T	The definition is ambiguous as the language used “secure transport of cryptographic keys (CSPs)” is not clear about what is intended. The term CSPs (Critical Security Parameters) has a broader definition than cryptographic keys, and so the meaning of the current definition is obscure. Change Key Transport definition “secure transport of cryptographic keys (CSPs)” to “secure transport of cryptographic keys” Or “secure transport of CSPs” To convey the intention of the authors	
5.	atsec	Peter Kim	2.1 Sensitive data	E	The definition is potentially restrictive and implies that it can only be considered sensitive data if the User role defines it so; however, the User role is optional. The distinction between a user and the optional User role can further be made by using “operator” in place of user. Reword: “Sensitive Data: information for which the operator requires protection.” Or Reword: “Sensitive Data: information for which the cryptographic module is designed to protect.”	
6.	atsec	Peter Kim	2.1 Trusted channel	T	The definition states, “…generally established for the transport of the SSPs, data and other critical information shared by the cryptographic module and *the other operator.*” It is unclear who the other operator is, since the module could potentially only support a single operator. The intent of the word “exists” is better served as “established”, since a Trusted Channel could exist without actually being established.	

					It is unclear how a Trusted Channel would protect against physical tampering within the module, as this would be a matter for physical security. It is also unclear how a host operating system would physically protect a communication link between the cryptographic module and itself, seeing as that the current definition implies a local and directly attached communication link might be simply fulfilled by a RJ-45 or RS-232 connector. The host operating system could only provide physical protection once the SSPs and data have been successfully communicated. While in transit, only logical protections would be available over any sort of connector. Reword: "Trusted channel: a cryptographically protected communication link established between the cryptographic module and an endpoint specified by the operator, generally used for the transport of SSPs and data. It includes a verification component used to confirm the Trusted Channel has been established. A Trusted Channel protects against eavesdropping, man-in-the-middle, and replay types of attacks along the module's communication link with the intended endpoint. A Trusted Channel may be of one of the following types: • Internal: a physical communication link established between the cryptographic module and an endpoint specified by the operator that is entirely local and directly attached to both the endpoint and the cryptographic module with no intervening systems in between. • External: a communication link established between the cryptographic module and a remote endpoint. In this case, the Trusted Channel is intended to cryptographically protect	

					the SSPs and other critical data, during entry and output, and does not allow misuse of any transitory SSPs. This type of Trusted Channel uses only Approved or Allowed security functions to establish the channel and transfer data."	
7.	atsec	Peter Kim	2.1 Trusted role AND 4.3.1 3rd Para	T	This is a dangerous concept, because it implies that the Crypto Officer can configure a role that can be autonomous without authentication or supervision by even the Crypto Officer once configured. This also implies that upon a power-cycle, the Trusted role may continue to function without authentication, since the necessary configuration settings may persist across power down. A scenario can be envisioned where vendors see this as an opportunity to authenticate once during "initialization" and then forever more be in a Trusted role, which circumvents the intent behind operator authentication and the clearing of authenticated states across power down. If, however, this role is not intended to persist across power down, then the definition should be revised. Reword: "Trusted Role: a state of the module, achieved only upon configuration by a Crypto Officer, where the module can perform cryptographic operations and other Approved or Allowed security functions on behalf of the Crypto Officer until the Crypto Officer's authenticated state is cleared by log out or power down.	

8.	atsec	Peter Kim	2.1 Zeroization	E	The definition implies that deallocation of CSP memory or power dissipation for volatile memory would likely be sufficient without the need for an active over-write. Clarify the definition.	
9.	Cisco	Max Pritikin IEEE 802.1AR Editor	2.1	T	Re: Trusted Role If the IDevID is within the module then it must be enabled for automated use when the device is installed/brought-up on site. This text would benefit from a specific definition of the role played by the manufacturer when installing credentials. The manufacturer is acting as a “Crypto Officer” in that they are performing cryptographic operations with the module as a final step in the manufacturing process but this should not be confused with the idea of an ‘owner operator’. Add the sentence: “The factory default settings may enable a state of the module wherein it can perform cryptographic operations appropriate for authenticating itself.”	
10.	CSEC	Jean Campbell	2.1	G	Page 9 “*Port*: a physical entry or exit point of a cryptographic module that provides access to the module for physical signals represented by logical information flows **(physically separated ports do not share the same physical pin or wire).”** Why do we have requirements in the “glossary” section?	

11.	JCMVP		Draft Revised 2.1	E	Approved cryptographic module is no longer used in the main body, so please delete the term and the definition.	
12.	JCMVP		Draft Revised 2.1	T	The definition of “fault induction” is missing. Please define “fault induction” in the “Glossary of Terms”	
13.	JCMVP		Draft Revised 2.1	E	In Section 2.1, there are two types of colon (:). One is italic, the other is not. Please revise the document for consistency.	
14.	JCMVP		Draft Revised 2.1	E	The definition of "Non-security relevant" is strange, because the paragraph defines the notion of the adjective, "Non-security relevant", by the noun "requirements". Please define this term by an adjective phrase.	
15.	JCMVP		Draft Revised 2.1	T	The definition of System Software says that system software is within the cryptographic boundary. Is it really true? If so, system software would be subject to the self tests. It seems strange.	
16.	JCMVP		Draft Revised 2.1	T	In the definition of “System Software”, compilers are listed as an example software within the cryptographic boundary. However, compilers should not exist within the cryptographic boundary. Please remove compilers from the example.	
17.	JCMVP		Draft Revised 2.1	T	The definition of trusted channel mentions “SSPs, data and other critical information”. What is “other critical information”? Please show examples of other critical information.	
18.	CMVP	Kim Schaffer	2.1 Allowed security function:	T	A security function considered to meet the approved requirements under FIPS 140-3. Often this points to a security function that has been approved but has no recognized standard that FIPS 140-3 can reference.	
19.	CMVP	Beverly Trapnell, Caroline Scace, Kim	2.1 Approved	T	FIPS – Approved and NIST – recommended are not defined.	

		Schaffer				
20.	CMVP	Kim Schaffer	2.1 Digital Signature	T	Digital signatures are used as an organization as well as an individual. In the case of organizational representation non-repudiation may be overstating since it is one of many.	
21.	CMVP	Kim Schaffer	2.1Firmware module	T	A firmware module always has hardware considerations also. Perhaps a module that is based on software in a limited or non-modifiable environment.	
22.	CMVP	Kim Schaffer	2.1 HSMI and HFMI	T	Reduce to Hybrid Module Interface. Firmware or Software is dependant on the operating environment.	
23.	CMVP	Kim Schaffer	2.1 Key loader	E	Not used or needed. Not well defined.	
24.	CMVP	Kim Schaffer	2.1 Limited operational environment	T	Unnecessarily constrained and not needed.	
25.	CMVP	Kim Schaffer	2.1 Low-level testing	T	Unnecessary and ambiguous. Dependant on the definition of High-level testing which varies.	
26.	CMVP	Kim Schaffer	2.1 Minimum Entropy	T	It is not clear why minimum entropy is defined here. Refer to 800-90 as needed.	
27.	CMVP	Kim Schaffer	2.1 Entropy	T	Should refer to 800-90 and not be a generic definition. It confuses the vendors as to why a mathematical definition needs to be in the standard.	
28.	CMVP	Kim Schaffer	2.1 Hard/Hardness	E	Hard is an adjective, hardness a noun.	
29.	CMVP	Kim Schaffer	2.1 Hardware module	T	Can contain software.	
30.	CMVP	Kim Schaffer	2.1 Passivation	T	Passivation is not a protection against modification other than from exposure to the environment.	
31.	CMVP	Kim Schaffer	2.1 PIN	T	Can be used to authenticate identity or a role, important distinction for this document.	

32.	CMVP	Kim Schaffer	2.1 Production grade	T	Manufactured using industry accepted practices. Most are not “standards”.	
33.	CMVP	Kim Schaffer	2.1 Public Security Parameter	T	Modification does not necessarily lead to compromise, it could lead to denial. Maybe use “invalidate the operation of the □ryptographic module.”	
34.	CMVP	Kim Schaffer	2.1 Runtime environment	T	Should be removed. This is one example of a runtime environment.	
35.	CMVP	Kim Schaffer	2.1 Seed key	T	Often misused, let the standard that uses it define it. Best not here.	
36.	CMVP	Kim Schaffer	2.1 Sensitive Security Parameters	T	Specific configuration or operation data that if unprotected could weaken or compromise the strength of the cryptographic operation.	
37.	CMVP	Kim Schaffer	2.1 strong	T	The definition does not add to anything a standard dictionary would provide.	
38.	CMVP	Kim Schaffer	2.1 System Software	T	The standard software bundle an Operating System manufacturer would provide for the operation of processor based hardware.	
39.	CMVP	Kim Schaffer	2.1 Trusted channel	T	Overly restrictive and inconsistent definition.	
40.	CMVP	Kim Schaffer	2.1 Validated	T	Accepted as meeting the requirements by the authoritative organization.	
41.	CMVP	Kim Schaffer	2.1 Zeroization	T	The operation of removing electronically stored data in a manner which prevents the recovery of the data.	
42.	Cryptsoft	Tim Hudson	2.1 Administrator Guidance	E	Administrator Guidance is the document; whether or not the Crypto Officer uses it should not be part of the definition. This definition should be consistent with the “Non-Administrator Guidance” definition. Suggested resolution: reword as “Information and procedures for configuring, maintaining, and administering the cryptographic module in a secure manner”	

43.	Cryptsoft	Tim Hudson	2.1 Approved cryptographic module	G	“a validation authority” – there is only one validation authority and it should be referenced here.	
44.	Cryptsoft	Tim Hudson	2.1 Approved integrity technique	E	“or a digital signature algorithm.” wording makes it unclear if it is approved or not and is inconsistent with the wording of the other two algorithm types. Suggested resolution: “or digital signature.”.	
45.	Cryptsoft	Tim Hudson	2.1 Executable Form	T	This definition is entirely ambiguous. If the intent is to exclude “source” from the definition then it needs to be reworded in a manner identical to that of “firmware”. As it stands, a cryptographic module which includes a compiler or interpreter extends this definition beyond what was intended. This definition should be consistent with “Software”. Suggested resolution: “for the purpose of this document, an encoded set or collection of computer instructions (referred to as code) that is designed to execute on the CPU of the cryptographic module”.	
46.	Cryptsoft	Tim Hudson	2.1 Limited Operational Environment	T	“that successfully passed the Software/Firmware Load Test” This is ambiguous and not relevant to the definition of the environment. Suggested resolution: delete “that successfully passed the Software/Firmware Load Test” or reword as “an operational environment that only allows post-validation functional updates in a controlled manner”. If the intent is to require that all updates are themselves validated then it should be clearly and simply stated. That leads to a	

					requirement for a control – as there is no technical mechanism for a module to determine if an update has passed validation.	
47.	Cryptsoft	Tim Hudson	2.1 Minimum entropy	E	Reference to “SP800-90” should be via one of the Annexes rather than referenced directly in the standard. All other references to algorithms or details which will vary outside of the FIPS140 update process are contained in an Annex and this should be handled in a consistent manner.	
48.	Cryptsoft	Tim Hudson	2.1 Non-administrator guidance	E	Non-Administrator Guidance is the document; whether or not the User uses it should not be part of the definition. This definition should be consistent with the “Administrator Guidance” definition. Suggested resolution: reword as “Information and procedures for use of the cryptographic module in a secure manner”	
49.	Cryptsoft	Tim Hudson	2.1 Periodic Self-Test	E	“A suit” Suggested resolution: “A suite”	
50.	Cryptsoft	Tim Hudson	2.1 Periodic Self-Test	T	The definition should not vary according to the security level. The timing/circumstances of activation are not part of the definition. Suggested resolution: “a suite of pre-conditional and conditional self-tests executed on-required or on a periodic basis as specified in the Security Policy”.	
51.	Cryptsoft	Tim Hudson	2.1 Runtime Environment	T	“a virtual machine state” This definition is entirely inappropriate. If the intent is to cover virtual machine environments then it should be defined as such. Suggested resolution: delete “virtual” and delete last sentence.	

52.	Cryptsoft	Tim Hudson	2.1 Software	T	This definition neither includes nor excludes "source code". This definition should be consistent with "Executable Form". Both "Executable Form" and "Software" seem to be trying to define the same thing.	
53.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**2.I Glossary of Terms**	G	Manual key transport should be defined. Suggest adding a definition for manual key transport to the glossary.	
54.	IBM	Hugo K	**Page 5, Digital Signature definition**		I would suggest to drop the mentioning of non-repudiation as a required service for digital signatures (currently defined in page 5). In the current application non-repudiation is not a requirement; in particular, non-repudiation is essentially a property that involves potential validation by a third party which is not the case here.	
55.	InfoGard		Section 2.1	E	The glossary provides a definition for Multi-Factor Authentication but no definition is provided for Role-Based Authentication or Identity-Based Authentication. Provide a definition for Role-Based Authentication and Identity-Based Authentication.	
56.	InfoGard		Section 2.1	E	The glossary doesn't provide a definition for Critical Functions. This term has been used loosely in the past, providing no clear requirement. Solidifying this definition might help identify functions more explicitly (e.g. RSA encrypt/decrypt function for key wrapping). Provide a definition for Critical Functions.	

57.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	G	Acronyms should be spelled out in with their first usage. Examples of acronyms that are not defined are HMAC, AES, CCM, PIN, etc. Rationale: Provide reader, both experts and novices, with a clear understanding of what is being discussed.	
58.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	Add to the list of operations under "Cryptographic Key" the following: Generation of cryptographic keys Generation of pseudorandom bit streams Rationale: These functions are described in NIST SP 800-90.	
59.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	G	Change "Hybrid module: a module whose cryptographic functionality is contained in software or firmware, which also includes some special purpose hardware within the cryptographic boundary of the module." to "Hybrid module: a module whose cryptographic functionality is contained in software or firmware, which may include some special purpose hardware within the cryptographic boundary of the module." Rationale: Not all Hybrid modules will need "special purpose hardware". General purpose processors (GPPs) and Field Programmable Gate Arrays (FPGA) can be used to build very capable cryptographic modules without requiring "special purpose" hardware.	
60.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	G	Combine the definitions of "Hybrid Firmware Module Interface" and "Hybrid Software Module Interface" to a single "Hybrid Module Interface". Rationale: The underlying technology implementing a security function, hardware or firmware, is not important to the user of the function. For example, a cryptographic module developer may place a hashing function in firmware, since it is unlikely to change for a long period of time and	

					encryption functions in software to be able to implement new algorithm modes of operation in the future. If this vendor in the future decides to upgrade the product and implement the same hashing function using software based logic (GPP or FPGA), they would have to update their documentation to identify this change in how the security feature is implemented. This could increase the effort to recertify this upgraded module and could cause updates to all systems that use this module, since the interface to the function has changed and might result in a change to the APIs used by application software.	
61.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	Change “Key establishment: the process by which cryptographic keys are securely established among cryptographic modules using key transport and/or key agreement procedures” to “Key establishment: the process by which cryptographic keys are securely established among cryptographic modules using hardware programming during manufacture, key transport and/or key agreement procedures”. Rationale: Some keying material, trust anchors or device unique keys, may be placed into the device during the manufacturing or device initialization process. This is likely to be done with special hardware fixtures and/or software tools.	
62.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	Change “Key loader: a self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.” to “Key loader: a self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into or received from a cryptographic module.” Rationale: A key loader should be useable load and receive keys from a cryptographic	

					module.	
63.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	In the definition of “Logical Protection” is protection against side channel attacks (timing, cache hit, predictive branch analysis, …) included or excluded from this definition? Rationale: These techniques have been used to extract CSPs from cryptographic hardware. Sidechannelattacks.com, Cryptographic Hardware and Embedded Systems (CHES) proceeding, Crypto proceedings and International Association of /for Cryptographic Research (www.iarc.org) contain papers on these techniques. FIPS 140-3 needs to address these powerful methods of extracting/determining CSPs.	
64.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	Change “Operational environment: the set of all software and hardware required for the module to operate securely” to “Operational environment: the set of all software, hardware and/or firmware required for the module to operate securely”. Rationale: Required security functions may be implemented in firmware.	
65.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	E	Change “Periodic Self-Tests: a suit of pre-conditional” to “Periodic Self-Tests: a suite of pre-conditional” Rationale: Correct typo.	
66.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	E	Change “Public key certificate: a set of data that contains a unique identifier associated with an entity, contains the public key associated withy” to “Public key certificate: a set of data that contains a unique identifier associated with an entity, contains the public key associated with”. Rationale: Correct typo.	

67.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	G	Change “Removable cover: a part of a cryptographic module’s enclosure that permits physical access to the contents of the module” to “Removable cover: a part of a cryptographic module’s enclosure that permits physical access to some or all the contents of the module”. Rationale: A cryptographic module may have multiple covers, each protecting different portions of a cryptographic module. There may be a covers for the plaintext and ciphertext areas of a cryptographic module.	
68.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	Change “Service: any externally invoked operation and/or function that can be performed by a cryptographic module” to “Service: any internally or externally invoked operation and/or function that can be performed by a cryptographic module”. Rationale: A module can perform services based on internal decisions or time limits. Session keys may be automatically re-negotiated after a time period has expired or a certain volume of data protected. Reseeding of deterministic key generators after a certain amount of data is required in SP 800-90.	
69.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	G	Combine the definition of “Software/Firmware Module Interface (SFMI)” into with “Hybrid Firmware Module Interface” and “Hybrid Software Module Interface” and form a single Module Interface definition. Rationale: See rationale above for comment on “Hybrid Firmware Module Interface” and “Hybrid Software Module Interface”.	
70.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	Add “The split process may allow a subset of the multiple key components to be loaded to obtain the original key” to the end of “Split knowledge: a process by which a cryptographic key is split into multiple key components, individually providing no knowledge of the original key, which can be subsequently input into, or output from, a	

					cryptographic module by separate entities and combined to recreate the original cryptographic key." Rationale: Some split key processes can recover the key with less than all splits present. This may require a majority of the splits to be present which prevents a denial of service if some splits are missing.	
71.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.1	T	Change "Trusted channel: a trusted and safe communication link established between the cryptographic module and the module's operator, generally established for the transport of the SSPs, data and other critical information shared by the cryptographic module and the other operator." to "Trusted channel: a trusted and safe communication link established between the cryptographic module and an entity external to the module or established between/among components within the module, generally established for the transport of the SSPs, data and other critical information shared by the cryptographic module and the other operator." Rationale: As worded, a module to an operator the defined external trusted path may not be valid, this path could be used by an operator to control the cryptographic module or it could be used to obtain updated keying material from a key management infrastructure. Trusted channels may also be established within the cryptographic module to protect the distribution and generation of SSPs within the cryptographic module.	
72.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	2.2	E	Acronyms ECB and KAT are not used within the document except in the acronym list. Remove these from the acronym list. Rationale: Not used.	
73.	The MITRE Corporation 202 Burlington Rd	James Cottrell jxc@mitre.or	2.2	E	The following acronyms are used in the document: FISMA; AES; CMS; EME; SP; nm; BIST; VHDL; and, I/O. Add these to the	

	Bedford, MA 01730	g 781-271-7212			acronym list Rationale: Accuracy and completeness.	
74.	Motorola	Jan Hintermeister	2.1, definition for approved mode of operation	G	Can non-approved security functions be used in Approved mode? In some situations a device may use an algorithm (e.g. MD5) to perform some tasks not relevant to FIPS 140-3 requirements. Or an IETF RFC may specifically require an algorithm not in the Annex A list. In this case, if the device is forced to use an algorithm from Appendix A to implement an IETF protocol, the device is non-compliant with an RFC and loses the abililty to interoperate with other devices. Can the definition of "approved mode" be modified to accommodate these scenarios?	
75.	Motorola	Jan Hintermeister	2.1, definition for approved mode of operation	E	The glossary states that the approved mode "only" uses Approved and Allowed security functions. Maybe this "only" should be changed to "at least one" to be consistent with Section 4.1.3.	
76.	NSA	TWG	2.1	E	Periodic Self-Tests definition; need "an" in "...either upon **an** operator's request..." and Sensitive Data definition: "data that, in user's view, requires protection" is missing some words; and "Software/Firmware Load Test definition: need "that" in "a set of tests **that** a software or firmware..."	
77.	NSS Project	Wan-Teh Chang	Section 2.1, last paragraph of page 9	Technical	A “runtime environment” is not necessarily a virtual machine and its primary purpose is not necessarily platform independent programming. A “runtime environment” can also be a set of libraries that supports programs written in a particular programming language. See http://en.wikipedia.org/wiki/Run-time_system and http://en.wikipedia.org/wiki/Run_time_%28co	

					mputing%29 (the third paragraph).	
78.	OpenSSL Software Foundation	Steve Marquess	2.1 Executable Form	T	The definition of “executable form” is quite vague. Does this definition include or exclude compiled source code? Runtime interpreted source code? Runtime interpreted byte-code? Virtual machine or emulated code? This definition should be consistent with “Software”. Any ambiguity around source based validations should be resolved as part of FIPS140-3. FIPS140-3 should not exclude types of modules which were previously permitted.	
79.	OpenSSL Software Foundation	Steve Marquess	2.1 Executable Form	T	This definition of “firmware” appears to be at odds with the general use of that term in the software industry. First, the definition references designer “intent” and not functional characteristics. Second, the definition does not exclude many implementations that commonly considered as “software”, such as read only file systems and media. Redefinition of commonly used technical terms to new meanings in the context is confusing to the practitioners attempting to implement validated products.	
80.	OpenSSL Software Foundation	Steve Marquess	2.1 Executable Form	E	Why is SP800-90 referred to directly while all other references are via the Annexes? This should be handled in a consistent manner with all other algorithms.	
81.	OpenSSL Software Foundation	Steve Marquess	2.1 Executable Form	T	The definition should not vary according to the security level. The timing and circumstances of activation should not form part of a definition.	
82.	OpenSSL Software Foundation	Steve Marquess	2.1 Executable Form	T	The definition of “software” is quite vague. The correlation with the general industry usage of the unqualified term “code” is unclear. Does this definition include or exclude compiled source code? Runtime interpreted source code? Runtime interpreted byte-code? Virtual	

					machine or emulated code? This definition should be consistent with "Executable Form". It is unclear what distinction is attempting to be made between "Executable Form" and "Software" and the purpose of that distinction elsewhere in FIPS140-3. Any ambiguity around source based validations should be resolved as part of FIPS140-3. FIPS140-3 should not exclude types of modules which were previously permitted	
83.	OpenSSL Software Foundation	Steve Marquess	2.1 Executable Form	T	The definition of "executable form" is quite vague. Does this definition include or exclude compiled source code? Runtime interpreted source code? Runtime interpreted byte-code? Virtual machine or emulated code? This definition should be consistent with "Software". Any ambiguity around source based validations should be resolved as part of FIPS140-3. FIPS140-3 should not exclude types of modules which were previously permitted.	
84.	Orion	MS	Section 2, definition of "periodic Self-test	E	Should "pre-conditional" be "pre-operational"? If not, then please define "pre-conditional". Clarify or define.	
85.	SPYRUS, Inc.	WSM	2.1		Definition of **Trusted Channel** for **Internal** type states no "additional" cryptographic protection is necessary. The intension is unclear. Does this imply there is NO cryptographic protection for the Internal Type? Give an explicit basic requirement for cryptographic protection in the main definition; leave Internal definition as is. OR: state "no cryptographic protection" for Internal type (not recommended).	
86.	Thales e-Security		2.1 (Tamper evidence), 4.6.1 and	T	The glossary entry for "Tamper evidence" states that "The evidence of the tamper attempt should be observable by an operator	

			4.6.3.		subsequent to the attempt." This requirement is not practical for un-removable embedded CMs and is not consistent with sections 4.6.1 and 4.6.3 that do not require operator observation. Inspection procedures for the overall product to identify the potential triggering of tamper evidence mechanisms for embedded CMs should be identified in the CM's Security Policy and User Guide.	
87.	NIST	Elaine Barker	2		We need to harmonize the definitions in our various publications (e.g., SP 800-56 and 57). Thois means that the definitions should be the same, unless one needs to be more general or specific.. We should probably coordinate definitions so that changed in whatever document appropriate. For example, trusted channel is used in other documents and should be harmonized, but not identical.	
88.	NIST	Elaine Barker	2.1		*Allowed*: NIST allowed or permitted. Is there any mention about how allowance is publicized?	
89.	NIST	Elaine Barker	2.1		*Approved*: FIPS-Approved and/or NIST-recommended. Do these need to be defined?	
90.	NIST	Elaine Barker	2.1		*Approved data authentication technique*: an Approved method that may include the use of a digital signature, message authentication code or keyed hash (e.g. HMAC). HMAC is a message authentication code.	

91.	NIST	Elaine Barker	2.1		*Approved SSP management technique*: a technique used for the establishment and continued management of SSPs as specified in Annex C. This assumes that SSP management techniques will remain in a separate annex from security functions. It would be easier to handle in this document if they are combined. If the decision is to remain separate, then each occurrence of "security function" should be checked to see whether the SSP management techniques also need to be included.	
92.	NIST	Elaine Barker	2.1		*"Encrypted key*: a cryptographic key that has been encrypted using an Approved or Allowed security function with a key encrypting key. " No such thing as a Allowed encryption function	
93.	NIST	Elaine Barker	2.1		*"Firmware:* for the purpose of this document, an encoded set or collection of computer instructions (referred to as code) that is designed to execute in a non-modifiable or limited environment. " Should it include the processors, registers and paths that are executed or used?	
94.	NIST	Elaine Barker	2.1		*"Hardware module*: a module composed primarily of hardware, which may also contain firmware. " Wouldn't this make it a hybrid module?	

95.	NIST	Elaine Barker	2.1		*"Integrity*: the property that sensitive data has not been modified or deleted in an unauthorized manner without detection." Deletion is a form of modification	
96.	NIST	Elaine Barker	2.1		*Key agreement*: a key establishment procedure (either manual or electronic) where the resultant key is a function of information by two or more participants, so that no party can predetermine the value of the key independently of the other party's contribution. I suggest removing this, as it's confusing. It sounds too much like using key components and split knowledge.	
97.	NIST	Elaine Barker	2.1		*Key transport*: secure transport of cryptographic keys (CSPs) from one cryptographic entity to another entity. For this standard, this definition could refer to either manual or electronic key transport, but this concept should be thought about before saying it.	
98.	NIST	Elaine Barker	2.1		*Logical protection:* protection against unauthorized access (including unauthorized use, modification, substitution, and, in the case of CSPs, disclosure) by means of the Module Software Interface under operating system control. Logical protection of software SSPs does not protect against physical tampering. Substitution is a form of modification	
99.	NIST	Elaine Barker	2.1		*Modifiable operational environment*: an operational environment that is designed, post validation, to accept functional changes that may contain non-validated software.	

					Do we need to say anything about not making changes to the validated software?	
100.	NIST	Elaine Barker	2.1		*Radiation hardening:* improving the ability of a device or piece of equipment to withstand nuclear or other radiation; applies chiefly to dielectric and semiconductor materials. Are both of these needed? Could we just say semiconductor technology? Dielectric - A material such as glass or porcelain with negligible electrical or thermal conductivity Semiconductor - A substance as germanium or silicon whose electrical conductivity is intermediate between that of a metal and an insulator; its conductivity increases with temperature and in the presence of impurities	
101.	NIST	Elaine Barker	2.1		*Sensitive Security Parameters (SSP)*: Critical Security Parameters and Public Security Parameters. Not clear why this would be sensitive. Perhaps something should be added to this definition indicating that either the confidentiality or integrity of the parameters is sensitive (this would allude to why a public parameter, which needs integrity protection, would be considered to be sensitive).	
102.	NIST	Elaine Barker	2.1		*Software/Firmware Load Test*: a set of tests that software or firmware has to pass successfully before it can be loaded into the cryptographic module and executed. When and where would this take place in the case of firmware? I thought firmware was loaded during manufacture (but maybe I don't	

					understand the process).	
103.					*Validation authority*: the entity that will validate the testing results for conformance to this standard. Does this need to be more specific? We want the CMVP, rather than some arbitrary entity.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	CSEC	Jean Campbell	3.	E	“To protect a cryptographic module from unauthorized operation or use. “ Change to: “To protect a cryptographic module from unauthorized, **access**, operation or use. “	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Yi Mao	Section 4 “Security Requirements” Table 1: Summary of Security Requirements	T	Table 1 on page 15 in FIPS 140-3 introduces a confusion of applying security levels 1 through 4 to an overall cryptographic module (CM) as well as to each individual section of requirements. The way that Table 1 is constructed invites people to apply the Security Levels 1 through 4 to individual sections as well, which doesn't make sense for some sections. For instance, the section Cryptographic Module Specification has only TWO distinct levels of requirements. The security levels 1 through 4 defined in section 1 of FIPS 140-3 and referenced throughout the standard are ONLY meant to be the overall security level for a CM in regards to a minimum set of assurance requirements that the CM has met. I hope this point can be explicitly stated and stressed somewhere in the standard, for instance, before or after Table 1. To avoid confusion, I'd suggest using "security grades" for the distinct sets of requirements for individual sections, in order to differentiate it from the overall "security levels". By introducing the "security grades" notion for individual sections, the intended meaning of "an CM with overall security level 1 and grade 2 for Cryptographic Module Specification" is much clearer than that of "a CM with overall security level 1 and level 3 for Cryptographic Module Specification". In addition, "a CM with overall security level 1 and level 4 for Cryptographic Module	

					Specification" and "a CM with overall security level 1 and level 3 for Cryptographic Module Specification" actually satisfy the same set of requirements, regardless the fact that they are claimed to have met different security levels for a specific section. This indicates that the "security level", being an overall assurance measure, is really not applicable to individual sections. On the contrary, since grades for individual sections are intended to label DISTINCT sets of requirement, they won't misleadingly refer to the same set of requirements using different grade numbers. Thus the problem can be avoided.	
2.	atsec	Fiona Pattinson	Section 4 Para 1	T	Section 4 states that “The security requirements cover areas related to the secure design, implementation, operation and disposal of a cryptographic module.” No mention of the disposal of a cryptographic module is made in the standard, its appendices, or annexes. Either remove “disposal” from Section 4 or include some discussion of the topic in the standard. Suggestions include a) Requiring some discussion of disposal in the security policy (Appendix “B” section 10 is suggested. b) Including a relevant entry in the bibliography for secure disposal c) Make specific requirements in the standard/ Section 4.10 is a suggested location.	
3.	atsec	Peter Kim	4. 4th Para	E	The term “user” can be confused with the User role. Suggest using “operator”, instead. Reword: “All documentation, including copies of the operator and installation manuals, shall be provided to the testing laboratory by the vendor.”	

4.	atsec	Fiona Pattinson	4 5th (last) para.	E	There are six annexes specified. A-G. There is no annex titled “test metrics.” Change 5th paragraph to “Annexes A through G provide references to Approved and Allowed security functions, Approved and Allowed SSP Management Techniques, Approved Authentication Techniques, Non-Invasive Attack Methods and Allowed operating environments.”	
5.	CSEC	Jean Campbell	4. Table 1	G	Page 15 Section 3. Roles, Authentication, and Services “Definition of module’s roles and services” This is a general requirement. It does not apply only to Security Level 1.	
6.	CSEC	Jean Campbell	4. Table 1	E	Page 15 “Approved digital signature or keyed message authentication code- based integrity test. “ Change to “Integrity test using approved digital signature or keyed message authentication code.”	
7.	JCMVP		Draft Revised 4. 4th paragraph	E	Please replace the phrase, "Appendices A and C" by "Appendices A and B", because the Appendix C does not include requirements.	
8.	CMVP	Kim Schaffer	Table 1 non-modifiable vs limited	T	Today’s manufacturing environment has almost no code that cannot be modified, even microcode. Non-modifiable is an extremely small subset of limited and should be combined to limited.	

9.	CMVP	Kim Schaffer	Table 1 Physical security	E	Zeriozation circuitry is not on doors, zeroization is the desired result of tamper response	
10	CMVP	Kim Schaffer	Table 1.	E	It was stated that the requirement build on previous levels in section 4. This does not need to be emphasized in an overview table.	
11	CMVP	Kim Schaffer	Table 1 Delivery and operation	T	Initialization procedures (1st time) and startup procedures (every time for transition to operation) are needed.	
12	CSD	Matthew Scholl	Table 1	T	"Annotated source code, schematics or HDL." Reword to "Annotated technical information such as schematics or HDL."	
13	InfoGard		Section 4	E	Please provide a description for Annex G.	
14	InfoGard		Section 4	G	Will an annex of Approved Protection Profiles be published? If not, are any CC approved PPs acceptable in FIPS 140-3?	
15	InfoGard		Section 4, Table 1	E	Area 3, Security Level 2: To satisfy this level, the text identifies the option of either Role-Based or Identity-Based Authentication. This is not consistent with the information found in Section 4.3.2. Level 2: Delete the reference to Identity-Based Authentication.	
16	InfoGard		Section 4, Table 1	E	Area 8, Levels 3 and 4: Trusted Channel is listed here as a requirement but this is already identified under Area 2. This is redundant. Delete the Trusted Channel text under Area 8.	
17	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Table 1	T	Could a software cryptographic module running on top of a "high assurance" virtual machine be evaluated to Security Levels 3 or 4? Rationale: Since virtual machines are being	

					used to computing services at different security levels, shouldn't this FIPS allow a software cryptographic module AND virtual machine to be evaluated at the higher Security Levels?	
18	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Table 1	G	Recommend rethinking automatically classifying all software modules as not being able to possess secure methods for software updates. Rationale: A software only product could implement updates through the use of signed or signed and encrypted software packages. The signature on the update package and the resulting signature on the entire software image would have to be checked before allowing the update to occur.	
19	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Table 1	T	For "Physical Security" row entry under "Security Level 4" change "EFP or EFT for temperature and voltage. Tamper detection and zeroization circuitry for multi-chip modules. Fault Injection Mitigation." to "EFP or EFT for temperature and voltage. Tamper detection and zeroization circuitry for single and multi-chip modules. Fault Injection Mitigation." Rationale: Certification shouldn't be allowed for a single chip module at this level that doesn't zeroize CSP upon detecting a tamper event. Otherwise an adversary may be able to obtain a device, open it up and extract CSPs. This extraction could be done either by invasive or non-invasive means, nullifying any non-invasive protection methods (Simple Power Analysis, Differential Power Analysis, RF emanations analysis, …) provided by the product.	

20	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Table 1	T	For “Physical Security Non-invasive Attacks” “Security Level 4” change “Mitigation against non-invasive attacks with specific test requirements for this security level, specified by the validation authority (mandatory for single-chip cryptographic modules and optional for all other hardware module embodiments).” to “Physical Security Non-invasive Attacks” “Security Level 4” from “Mitigation against non-invasive attacks with specific test requirements for this security level, specified by the validation authority (mandatory for single-chip, multiple-chip standalone cryptographic modules and enclosed multiple-chip embedded modules and optional for all other hardware module embodiments).” Rationale: The ability to perform side channel attacks should be reduced for ALL enclosed cryptographic module configurations. Allowing a cryptographic module consisting of two chips, a cryptographic engine and a simple IC (clock or power regulator) to be certified to a Security Level 4 AND NOT protect against side channel attacks should not be certified greater than 3, if mitigation technique(s) are described and are technically reasonable, or greater than 2, if no documentation on mitigation technique(s) are supplied! To do otherwise would be a disservice to users believing that they are using a Security Level 4 product.	
21	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Table 1	T	For “Physical Security Non-invasive Attacks” “Security Level 3” change “Review of documented mitigation techniques against applicable non-invasive attacks listed in Annex F (mandatory for single-chip cryptographic modules and optional for all other hardware module embodiments).” to “Review of documented mitigation techniques against applicable non-invasive attacks listed in Annex F (mandatory for single-chip,	

					multiple-chip standalone cryptographic modules and enclosed multiple-chip embedded modules and optional for all other hardware module embodiments).” Rationale: The design features to protect against side channel attacks should be provided for ALL enclosed cryptographic module configurations. Allowing a cryptographic module consisting of two chips, a cryptographic engine and a simple IC (clock or power regulator) to be certified to a Security Level 3 AND NOT describe mitigation technique(s) implemented in the product that are technically reasonable should result in a rating of Security Level 2! To do otherwise would be a disservice to users believing that they are using a Security Level 3 product.	
22	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Table 1	T	For “SSP Management” change “Requirements for Random Bit Generators, SSP generation, SSP establishment, SSP entry and output, SSP storage, and CSP zeroization. Electronically transported CSPs entered or output only encrypted” to “Requirements for Random Bit Generators, SSP generation, SSP establishment, SSP entry and output, SSP storage, and CSP zeroization. Electronically transported CSPs output only encrypted and entry can be unencrypted or encrypted”. Rationale: As stated in a comment above, NIST evaluated products are used to protect unclassified NSS information. NSA and some services, Army in particular, require that NSA be the source of all keying material and NSA’s key management infrastructure may or may not be able to accept contractor/vendor generated keys, Army regulations prohibit proprietary key management systems.	

23	NSA	TWG	4	E	1st para. "tests methods" should be "test methods"	
24	NSA	TWG	Table 1	E	Operational Environment: missing some word(s) in "Controlled loading of additional through the ..."	
25	NSS Project	Wan-Teh Chang	Section 4, Row 9 “Self-Tests” of the table on page 15	General	“Cryptographic algorithm tests specified in Annexes A through E.” I don’t see any cryptographic algorithm tests specified in Annexes A through E.	
26	Oracle Solaris Security	Darren Moffat	4 Table 1 Development	T	Justification for requiring high level language seems out of step with the current trend of adding cryptographic function level instructions to general purpose CPUs.	
27	Orion	MS	Section 4, Table 1, Operational Environment (limited)	E	Missing word in “Controlled loading of additional through”. Add “code” between “additional” and “through”.	
28	Orion	MS	Section 4, Table 1, Self-tests	T	Don’t see that Pair-wise consistency test is restricted to L3 and L4 only. Instead it is performed on all generated keys as specified in Annexes A through F. However, an error log containing the most recent error is required at L3 and L4. In the table, remove or correct pair-wise consistency check for L3 and L4 only when entered into the module. Add error log at L3 and L4.	
29	Orion	MS	Section 4, Table 1, Self Tests	E	At L1 and L2 operators **shall** be able to initiate self-tests but this is not shown in the table. At L3 and L4 vendor **shall** specify a critical time period before self-tests are performed. Show that at L1 and L2 the module **shall** have self-test capability. Show that at L3 and L4, a critical time for self-test **shall** be specified.	

30	RSA Security LLC	Kathy Kriese and Peter Robinson	Page 15, row 3 “Roles, Authentication, and Services”	E	In the cell for Security Level 3, the text says, "Identity-based operator authentication". Should the word "operator" be here? Should this match what was said for Security Level 2?	
31	SPYRUS, Inc.	WSM	4, Table 1		Row for **Development** under **Life-Cycle Management** states “Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components **is** completed.” Change “is” to “are”.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	Atsec	Peter Kim	4.1	E	Inconsistent with the definition of a cryptographic module given in the Glossary. Reword: "A cryptographic module shall be a set of hardware, software and/or firmware that implements Approved or allowed cryptographic algorithms, functions or processes."	
2.	Atsec	Fiona Pattinson	4.1.1 2nd bullet	T	The definition of a "software module" is not good English and is very hard to comprehend. From "Software module is a module whose cryptographic boundary delimits the software solely component(s) (may be one or multiple software components) that execute(s) in a modifiable operational environment." To "Software module is a module comprised solely of software and whose cryptographic boundary delimits one or more components that execute(s) in a modifiable operational environment."	
3.	Atsec	Fiona Pattinson	4.1.1 4th bullet	T	The definition of a "hybrid module" is confusing. The current text "Hybrid module is a module whose cryptographic boundary delimits the composite of a software or firmware component and a disjoint hardware component (i.e. the software or firmware component is not contained within the cryptographic hardware physical boundary). "precludes the combination of a software module AND a firmware module with the hardware module. This may be necessary for more complex modules.	

					The commenter understands that a SW + HW = hybrid FM + HW = hybrid But SW+FM+HW ≠ hybrid This seems to preclude a module that has both software and firmware components as well as the hardware, It also does not allow a software and firmware hybrid. How will these types of modules be addressed. Either reword to allow these combinations for a hybrid, or clearly state that they are not allowed.	
4.	atsec	Helmut Kurth	4.1.1 last paragraph	T	For a hybrid module the current draft states: "Sections 4.6 and 4.7 requirements shall be met at the composite cryptographic boundary of a hybrid module." Since those sections are not applicable to software, they can not be applied to the composite cryptographic boundary. They can (and should) be applied to the cryptographic boundary of the hardware or firmware part of the hybrid module. Change the text to: "Sections 4.6 and 4.7 requirements shall be met at the cryptographic boundary of the hardware or firmware components of a hybrid module."	
5.	atsec	Fiona Pattinson	4.1.2.1 2nd para	T	The definition of the cryptographic boundary for a software module is specified as including the storage media. The sentence is ambiguous and may be read so that the storage media are included in the cryptographic boundary. If this is the case then further issues become apparent as "storage media" may include internal devices as well as external devices. This is also conflicting with para 4.1.1 2nd bullet where the definition of the cryptographic	

					boundary is said to be solely software. This intent of the requirement needs clarification and the language of 4.1.2.1 and 4.1.1 amended to agree.	
6.	Atsec	Fiona Pattinson	4.1.2.1 3rd para	T	The definition of the cryptographic boundary for a firmware module is not described in terms of any physical structures/components. 4.1.1 para 3 states that for a firmware module the physical security requirements apply. Describe the extent of the boundary that will be subject to the physical security requirements and if necessary distinguish that boundary from the cryptographic boundary.	
7.	Atsec	Peter Kim	4.1.3 1st Para, 2nd sentence	E	The requirement is inconsistent with the definition of a cryptographic module as defined by the Glossary. Reword: "An Approved mode of operation shall provide services for at least one Approved or allowed security function"	
8.	Atsec	Peter Kim	4.1.3.1 6th bullet	G	Zeroization is not required when switching from an Approved mode to a non-Approved mode. Why is it more restrictive for a Level 3 or 4 module to transition from one secure state to another secure state than to transition from a secure state to an insecure state? Remove the zeroization requirement stated here.	
9.	Atsec	Peter Kim	4.1.3.2 3rd bullet	G	The requirement should explicitly state the failing security function is to be disabled. Please also clarify what isolation requires. Is the intent to ensure the failing function does not affect the other functions? If so, then disabling the offending function should cover the intent.	

					Reword: “Non-operational security functions shall be disabled and isolated from the remaining security functions of the cryptographic module.”	
10.	Cisco	Max Pritikin IEEE 802.1AR Editor	4.1.3.1	T	Re: “Security Levels 1 and 2: Upon re-configuration from one Approved mode of operation to another, CSPs shall not be shared or accessed between the Approved modes.” Manufacturing installed authentication CSPs need to be accessible and usable by all levels and all modes (or all appropriate levels/modes). It would be unreasonable for manufacturers to provide a product that is able to communicate via WiMAX or DOCSIS only when in one specific mode. The alternative, to have manufacturers install multiple credentials is also prohibitive. Although a discussion of Multilevel Security could be provided at this point to enable certain CSPs to be shared “up” Approved Modes (but not “down” to lower modes) this is likely too complex of a topic to address in this document. It is likely appropriate to only present the option of specific shared CSPs to and indicate that appropriate rationalization must be provided (e.g. in Appendix B) Clarification should be added concerning the existence of CSPs that are intended to be shared across modes.	

11.	Cisco		4.1.3.3 4.1.3	T	The statement: “CSPs shall not be shared or access provided between Approved and non-Approved modes of operation.” Seem to be in conflict with the requirement: “For Security Levels 1 and 2, the operation of the cryptographic module in an Approved mode shall, at a minimum, be by policy” If FIPS Mode/non-FIPS mode can be enforced by policy, requiring a technical means to separate CSPs in FIPS mode and non-FIPS mode essentially nullifies the second requirement allowing FIPS mode to be set by policy. Clarify that the first requirement is only applicable for level 3 and 4 to be consistent with the other section requirements.	
12.	CSEC	Claudia Popa	4.1.3	E	Page 18- For consistency throughout the document change **appendix B** to **Appendix B**.	
13.	CSEC	Claudia Popa	4.1.3.2, the third bullet	T	“non-operational security functions **shall be isolated** from the remaining security functions of the cryptographic module” It is not clear what “shall be isolated” means.	
14.	CSEC	Jean Campbell	4.1.2.1	E	The fourth bullet, add section 4.7 • physical structures that implement the requirements of Section 4.6 **and 4.7**,	

15.	CSEC	Jean Campbell	4.1.2	E	"The requirements of this standard shall apply to all functions and components **at and** within the module's cryptographic boundary." On the same page: "The defined name **and version number** of a cryptographic module shall be representative of the composition of the components within the cryptographic boundary."	
16.	CSEC	Jean Campbell	4.1.2.1	E	Page 18, first bullet, ad a comma "…hardware component boundary**,** and software or …"	
17.	CSEC	Jean Campbell	4.1.3	E	"An Approved mode of operation shall provide services for at least one Approved or **Allowed** security function or key establishment mechanism."	
18.	CSEC	Jean Campbell	4.1.3	E	"For Security Levels 1 and 2, the operation of the cryptographic module in an Approved mode shall, at a minimum , be **set** by policy (see **A**ppendix B)."	
19.	CMVP	Kim Schaffer	4.1	T	Approved should be Approved and allowed according to draft, however works with my recommendation of combining those.	

20.	CMVP	Kim Schaffer	4.1.1.	T	Physical security requirements should not always be optional for software modules. In some cases the physical security requirements should be met. For example, if a software module controls physical security attributes, such as access doors and panels, the module should also meet physical security and non-invasive requirements.	
21.	CMVP	Kim Schaffer	4.1.2	T	“Non-cryptographic or non-security relevant functions or components may be included within the cryptographic boundary.” Should be replaced by “ Non-security relevant algorithms, security functions, processes or components may also be used in an approved mode of operation. Non-security relevant algorithms, security functions, processes or components which are used in an approved mode of operation shall be implemented in a manner to not interfere or compromise the approved operation of the cryptographic module.”	
22.	CMVP	Kim Schaffer	4.1.2	E	“The defined name of a cryptographic module shall be representative of the composition of the components within the cryptographic boundary.” Does not belong with the paragraph as it is a completely different thought.	
23.	CMVP	Kim Schaffer	4.1.2	T	“ Excluded components shall not affect or compromise the correct operation or requirements of this standard of the security relevant components within the cryptographic boundary.” Reword to “ The excluded hardware, software or firmware components shall be implemented in a manner that does not interfere with or compromise the approved operation of the cryptographic module.”	
24.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.1 Hybrid module definition	T	The definition of hybrid module addresses the composite cryptographic boundary rather than the module. Each needs to be defined separately.	

25.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.1 Last paragraph	T	“Sections 4.6 and 4.7 requirements shall be met at the composite cryptographic boundary of a hybrid module.” This is unnecessary, the cryptographic boundary of a hybrid is defined as a composite in the subsequent section.	
26.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.2.1 Hardware boundary	E	“other components types not listed above “ should be reworded to “other component types not listed above”	
27.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.3 Modes of Operations	E	Consider rewording to Modes of Operation	
28.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.3 Modes of Operations	T	“For multi-threaded modules, the indication shall be provided for each called service” does multithreaded need to be defined.	
29.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.3.1	T	“Different Approved modes of operation are defined as each mode having services that provide a different suite of Approved or Allowed security functions or key establishment mechanisms.” Consider revising for clarity.	
30.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.3.1	E	“Each Approved mode of operation implemented in the cryptographic module and how each mode is configured **shall** be described (see appendix B.) ” Replace “how” with “the way.”	

31.	CMVP	Kim Schaffer	4.1.3.1	T	Security Levels 1 and 2: Upon re-configuration from one Approved mode of operation to another, CSPs **shall not** be shared or accessed between the Approved modes. Consider that it may be better for the vendor to state why sharing CSPs may make sense.	
32.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.3.1	T	"Upon re-configuration of Approved modes at Security Levels 3 and 4, the RBG state shall be re-seeded." What is the state and is it necessary?	
33.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.3.2	T	"Degraded mode of operation shall be entered only upon the detection of a failure and after the module has transitioned through the error state." Now that this is allowed why not other considerations such as power requirements?	
34.	CMVP	Beverly Trapnell, Caroline Scace, Kim Schaffer	4.1.3.2	T	"Non-operational security functions shall be isolated from the remaining security functions of the cryptographic module." What is the criteria for demonstrating or testing this? Maybe this is a level 4 type requirement where more resources would be expected?	
35.	CMVP	Beverly Trapnell, Kim Schaffer	4.1.3.3	T	"A non-Approved mode of operation is one where only non-Approved services are provided or the requirements of this standard are not met." Is there any reason why approved services cannot be used in a non-Approved mode? Consider "A non-Approved mode of operation is one in which non-Approved services are provided or all of the requirements of this standard are not met."	
36.	CMVP	Beverly Trapnell, Kim Schaffer	4.1.4	T	Consider allowing decryption only of non approved algorithms for a more universal module that meets US government requirements. There is no reason to test decryption of these non approved algorithms since you could	

					consider them a form of plaintext or obfuscation.	
37.	Cryptsoft	Tim Hudson	4.1	E	“Approved cryptographic” Should be “Approved or Allowed cryptographic”	
38.	Cryptsoft	Tim Hudson	4.1.2.1	T	“One or more processors” and “by the processor”. The reference to processor or processors should be consistent between software and firmware cryptographic modules. It is unlikely the intent here was to preclude multi-processor firmware modules but that is the current wording.	
39.	Cryptsoft	Tim Hudson	4.1.2.1	T	“saved in memory” This statement is limiting and technically incorrect. Suggested resolution: delete both occurrences of “saved”.	
40.	Cryptsoft	Tim Hudson	4.1.3.1	T	“Security Levels 1 and 2: Upon re-configuration from one Approved mode of operation to another, CSPs shall not be shared or accessed between the Approved modes.” Certain CSPs are ‘global’ to the module and hence are ‘shared’ by definition – e.g. module integrity keys, loadable module keys – i.e. persistent CSPs. All non-persistent CSPs should either not be shared or should be zeroised. Are multiple-approved modes allowed to be	

					simultaneously active in a cryptographic module? The current wording effectively allows this for L1 and L2. Suggested resolution: reword as “Security Levels 1 and 2: Upon re-configuration from one Approved mode of operation to another, non-persistent CSPs shall not be shared.”	
41.	Cryptsoft	Tim Hudson	4.1.3.2	T	The intent of discussion around degraded mode of operation was to allow delaying self-tests for a specific algorithm until it was required by a user of the module. The current wording suggests only “failure” of the self-test rather than allowing for simply not yet executing the self-test. Suggested resolution: Reword first two sentences as: “A cryptographic module may be designed to support degraded functionality (e.g., a module may delay the self-test for one encryption algorithm or detect an error during operation) within an Approved mode of operation. Security functions that tested correctly are considered operational, and those that were delayed or failed are considered non-operational.” Corresponding changes will be necessary to the wording in the bulleted list.	
42.	Cryptsoft	Tim Hudson	4.1.3.3	T	“and then back to a different (not the original)” There should be no requirements when switching modes that do not apply independent of whatever mode is involved. Suggested resolution: delete “different (not the original)”	

43.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.1, 4.1.1, *Hardware module*	E	Although rare, the CST laboratory has had a case of a hardware module with a modifiable operational environment. Suggest stating that firmware and/or software may be included within the hardware cryptographic boundary.	
44.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.1, 4.1.2.1 Definitions of Crypto-graphic Boundary, Paragraph 3	T	Since physical security is applicable for a firmware cryptographic module, physical structures that implement the requirements of Section 4.6 will need to be specified for a firmware cryptographic module. Add this to the cryptographic boundary identification	
45.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.1, 4.1.3.1 Multiple Approved Modes of Operation, First bullet	T	If allowing multiple Approved modes of operation with all the specified requirements for them, why not allow different Security Levels for them? Would add a complication in regards to validation but potentially could be done. Suggest considering the allowing of Approved modes of operation at different Security Levels.	
46.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.1, 4.1.3.1 Multiple Approved Modes of Operation, Bullets 5 and 6	T	Authentication data, a CSP, should not need to be not shared or zeroized when re-configuring from one Approved mode of operation to another. Specify only that secret and private keys cannot be shared or accessed between the Approved modes at Security Levels 1 and 2 and that authentication data does not need to be zeroized when re-configuring from one Approved mode of operation to another at Security Levels 3 and 4.	

47.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.1, 4.1.3.2 Degraded Mode of Operation, Bullet 3	T	Need to define what is meant by isolating non-operational security functions. Does this mean to make the non-operational security functions non-callable or add a warning before the non-operational security function runs? Suggest adding a definition in the standard either here or in section **2.1 Glossary of Terms**.	
48.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.1, 4.1.3.3 Non-Approved Mode of Operation, Paragraph 1	T	Could not an "Approved" service be run in a non-Approved mode of operation but not using a secret or private key from an Approved mode of operation? Suggest rewriting "where only non-Approved services are provided" as "where provided services are not Approved".	
49.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.1, 4.1.3.3 Non-Approved Mode of Operation, Bullet 1	T	It should be required to have a separate set of authentication data and/or public keys for non-Approved modes of operation. Suggest specifying that secret and private keys shall be shared or access provided between Approved and non-Approved modes of operation instead of all CSPs.	
50.	IBM Research, Zurich	Visegrady, Tamas	4.1.3		We perceive a conflict between testing and status reports in case of parallelism, either in hardware or multithreaded execution. While 4.1.3. allows a per-request display of mode, 4.1.3.1 mandates startup testing for each mode change. The latter is not realistic in parallel environments, where requests of different modes coexist. If such a multithreaded backend is available--which is the current IBM practice, even currently--and integrity checks are comprehensive, regardless of mode, no assurance improvement is achieved through initial testing upon mode switching. We recommend mandating mode-change related selftests if per-request testing does not cover the same components. As an example, since current IBM hardware modules	

					continually cross-check computations, additional known-answer tests would not increase the assurance level. Note that chip-internal parallelism will lead to multithreaded execution and mixed thread modes during the lifetime of the standard.	
51.	InfoGard		Section 4.1.3.1, Bullet 2	E	Consider rewording this bullet. Suggested text: *"The Security Policy shall describe each Approved mode of operation implemented in the cryptographic module and how each mode is configured (see Appendix B)."*	
52.	InfoGard		Section 4.1.3, Paragraph 3.c	T	"For multi-threaded modules, the indication shall be provided for each called service." The intent of this requirement is understood in the sense that there should be a clear way for the operator to determine if the module is in a FIPS mode. It is desirable for this indicator to always be active. However, due to the complexity and diversity of modules we encounter and validate, accomplishing this objective may be problematic. • Modules are designed with multiple physical and logical interfaces. Many of the logical interfaces and protocols are very specific. Attempting to add another status indicator into the return value of each service may not allow the module to be in compliance with other existing industry standards. • If this requirement is only asking that the module provide one constant indicator (e.g. display or LED), this may not satisfy the intent. Some modules are designed such that the majority of the services are performed remotely (e.g. telnet, VPN). Would a physical, local indicator really satisfy the intent?	

					Suggest deleting the last sentence of this paragraph (“For multi-threaded modules, the indication shall be provided for each called service”) and deleting “or service” from the second sentence so it reads “…shall be explicit and unambiguous as to the state of the module operating in an Approved or non-Approved mode.”	
53.	InfoGard		Section 4.1.3.1, Bullet 1	T	“The overall security level of the module shall be maintained when configured for different Approved modes of operation.” Since Section 4.1.3.1 also includes the requirements that (1) CSPs not be shared between modes (Levels 1 and 2) or (2) zeroization of CSPs occur (Levels 3 and 4), what is the intent of only allowing switching between modes if the overall security level of the module is maintained? If the module is able to maintain a ‘sandbox’ for each configuration, including CSPs, this should be of no more concern than allowing the module to switch between FIPS mode and non-FIPS mode, which is allowed provided that CSPs are not shared (Section 4.1.3.3). Delete the Bullet 1 requirement and allow modules to switch between two Approved modes of operation provided that (1) CSPs not be shared between modes (Levels 1 and 2) or (2) zeroization of CSPs occurs (Levels 3 and 4). For Levels 3 and 4, similar to a FIPS/non-FIPS mode status indicator, require that the module provide a status indicator.	
54.	InfoGard		Section 4.1.3.2, Bullets 4 and 5	T	The text in Bullet 4 appears to imply that a pre-operational self-test failure could result in a transition into the degraded mode but Bullet 5 appears to say differently. There are scenarios where it could be acceptable for the module to enter a degraded mode if one of	

					the pre-operational self-tests fail: • If the firmware failed the pre-operational self-test, the module might be designed to default into a bootloader mode, which is hardcoded in ROM, with limited services. This could potentially allow the error to be repaired (e.g. load new firmware). • The bypass pre-operational self-test might fail due to an algorithm error. If the module can transition into a degraded mode due to an algorithm KAT error, the module should also be able to transition into a degraded mode if the bypass test fails. Delete Bullet 5. Similar to Bullet 2, where this requirement is specific to algorithm failures, add requirements for all pre-operational self-test scenarios.	
55.	InfoGard		Section 4.1.3.2, Bullet 2	T	If a failure is detected when a module is in operation (having previously passed all self-tests), does this statement mean that all self-tests to be ***repeated*** prior to entering a degraded mode? Suggest rewording Bullet 2 as follows: *When the cryptographic module operates in a degraded mode of operation, each operational security function shall **have passed** all applicable self-tests.*	
56.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.1.1	G	This paragraph contains definitions for cryptographic module types that are not identical to those in the definitions section. For instance, the definition section provides this definition for a Hybrid module “a module whose cryptographic functionality is contained in software or firmware, which also includes some special purpose hardware within the cryptographic boundary of the module” and 4.1.1 contains this definition “is a module	

					whose cryptographic boundary delimits the composite of a software or firmware component and a disjoint hardware component (i.e. the software or firmware component is not contained within the cryptographic hardware physical boundary)". Rationale: The definition section states the "special purpose hardware" is within the cryptographic boundary and doesn't state whether the software or firmware is inside or outside of the cryptographic boundary and the definition in 4.1.1 explicitly states the firmware and software is outside of the cryptographic hardware physical boundary. Having multiple conflicting definitions will lead to confusion in the development, evaluation and certification of cryptographic products. Specification of three types of modules may make the document clearer. These three types are: Software module – all security functions are provided by the software product. Hardware module – all security functions are provided by: hardware; and, software and/or firmware. Hybrid module – all security functions are provided by a hardware modules and software running outside the physical boundary of the hardware module. Note: This new and the current Paragraph 4.1.1 definition of hybrid module limit the hybrid module to a maximum of Security Level 2, since Software cannot be evaluated above this Security Level.	

57.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.1.2.1	T	For the definition of the firmware cryptographic module change the second bullet from “The instantiation of the cryptographic module saved in memory and executed by the processor” to “The instantiation of the cryptographic module saved in memory and executed by one or more processors”. Rationale: With single FPGA chips providing multiple general purpose processing cores, limiting a firmware module to a single processor it too limiting. This matches the definition of a software module which addresses implementations on multi-processor cores or multiprocessor systems.	
58.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.1.3	E	Change “The module’s security policy shall describe how the operator” to “The module’s security policy shall describe how an operator”. Rationale: A cryptographic module may support more than one operator simultaneously.	
59.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.1.3.1	T	It appears that a device cannot support multiple approved modes simultaneously, as stated by “Upon re-configuration from one Approved mode of operation to another, the cryptographic module shall perform the pre-operational self-tests” and “Upon re-configuration, the conditional self-tests shall be reset and re-performed on condition for all Approved and Allowed security functions used in the selected Approved mode of operation” Recommend changing this sentence to “Upon instantiation of the first or a new Approved mode of operation, the cryptographic module shall perform all required pre-operational and conditional self-tests”. Rationale: With today’s complex Systems on Chip (SOC) and other highly capable products, the ability to perform two or more security functions simultaneously is possible.	

					Requiring that at FIPS evaluated product be able to provide a single security function at a time could require uses to purchase more cryptographic devices than current, or near term, technology can provide.	
60.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.1.3.1	T	The last bullet states “Upon re-configuration of Approved modes at Security Levels 3 and 4, the RBG state shall be re-seeded.” What requirements, if any should be met if the RGB is hardware based, such as one based on ring oscillators as described in “A Provably Secure True Random Bit Generator with Built-in Tolerance to Active Attack” by Sunar Berks of Worcester Polytechnic Institute paper? – (paper attached in email) Rationale: The requirement as written is fine for a deterministic Random Bit Generator (RBG) but is not applicable to a non-deterministic RBG (nd-RBG). If there are specific requirements for a nd-RBG these should be added to the FIPS.	
61.	Motorola	Ashot Andreasyan	4.1.3.2, 3rd bullet	G	How must non-operational security functions be isolated from the remaining security functions of the cryptographic module? Please provide an example in the FIPS 140-3 standard or Implementation Guidance documentation to clarify this.	
62.	Motorola	Ken Fuchs	4.1.2.1	G	Please provide an example or two of a Hybrid Cryptographic Module.	
63.	NSA	TWG	4.1.1	E	Section 4.1.1 for both Sofware module and Firmware module misuse (?) of "soley" in "delimits the software/firmware **soley** component(s)..."	

64.	NSA	TWG	4.1.2.1	E	need comma at end of bullet: "...converters, etc.**,**" and remove "s" from "other component**s** types not listed above" in that bullet	
65.	NSA	TWG	4.1.3	T	The second sentence states, “An Approved mode of operation shall provide services for at least one Approved security function or key establishment mechanism. However, the first sentence in section 4.1.4 states “In an Approved mode of operation, a cryptographic module shall implement at least one Approved or Allowed security function or technique. Furthermore, the definition in section 2.1 for “Approved mode of operation” states: a mode of the crypto module that employs only Approved or Allowed security functions. Is there a contradiction between section 4.1.3 and sections 4.1.4 and the definition?	
66.	NSA	TWG	4.1.3.2	T	Are the last two bullets in that section contradictory with each other: • The module **shall remain in the degraded mode** of operation until all pre-operational and conditional self-tests have been completed successfully. • If the module fails the pre-operational self-tests, the module **shall not enter a degrade**d mode of operation".	
67.	NSS Project	Wan-Teh Chang	Subsection 4.1.3, page 18	Editorial	“For Security Levels 1 and 2, the operation of the cryptographic module in an Approved mode shall, at a minimum, be by policy (see appendix B.)” It is not clear what “by policy” means. Please clarify or reword it. Appendix B, section 1 on page 56 has the same issue: “For Security Levels 1 and 2, the operation of the cryptographic module in an	

					Approved mode of operation shall, at a minimum, be **by policy** as specified in the security policy."	
68.	NSS Project	Wan-Teh Chang	Subsection 4.1.3, page 18.	Editorial	"For multi-threaded modules, the indication shall be provided for each called service." The word "multi-threaded" is usually used to describe software. Since Levels 3 and 4 do not apply to software modules in this draft, it's not clear what "multi-threaded modules" means in a requirement for Levels 3 and 4.	
69.	NSS Project	Wan-Teh Chang	Subsection 4.1.3.3, page 19.	Editorial	"A non-Approved mode of operation is one where only non-Approved services are provided …" "**Only** non-Approved services are provided" is too restrictive. How about "**some** non-Approved services are provided"?	
70.	OpenSSL Software Foundation	Steve Marquess	4.1.2.1 Executable Form	T	"saved in memory" This statement is inaccurate in that "saved" is indicating a level of persistence.	
71.	OpenSSL Software Foundation	Steve Marquess	4.1.2.1 Executable Form	T	It needs to be clear that algorithm self tests are able to be delayed until the algorithm is first used. This issue was raised against FIPS140-2 which conflicts with practical use of general purpose cryptographic modules containing a large set of algorithms and a complicated set of startup tests. The current wording suggests only "failure" of the self-test rather than delayed execution. This area warrants additional clarity in FIPS140-3.	

72.	Oracle	Matt Ball	4.1.2.1, last line, page 17	E	A firmware cryptographic module may execute on more than one processor. Recommend changing last sentence to match that of a software cryptographic module: "... executed by **one or more processors**"	
73.	Oracle	Matt Ball	4.1.3.1, second bullet	E	It is difficult to discern the subject of this sentence. Consider rewriting: "Documentation (see appendix B) shall describe each approved mode of operation that the cryptographic module implements and shall describe the configuration for each mode of operation." (notice the rewriting of the passive voice into the active voice)	
74.	Oracle	Matt Ball	4.1.3, first sentence	E	This requirement does not apply to the operator, but to the cryptographic module. Consider rewording as such: "The cryptographic module shall allow the operator to operate the cryptographic module in an Approved mode of operation" (Also note that the word 'module' should always appear as 'cryptographic module')	
75.	Oracle	Matt Ball	4.1.3.1, third bullet	T	The requirement that the cryptographic module re-run the pre-operational self-tests is unnecessarily onerous for cryptographic modules that need to continually switch between approved modes of operation. Consider changing this requirement so that the self tests only need to be run when the system is initially configured. It is unclear that this requirement adds any meaningful assurance of security beyond the assurance received when running the initial self-tests after power-on. (same comment applies to the forth bullet as well)	
76.	Oracle	Matt Ball	4.1.4, first sentence	E	If the parenthetical information is removed from this sentence, then the words 'Approved' or 'Allowed' are not sufficiently defined. Consider rewording as follows: "..., a cryptographic module shall implement at least one Approved or Allowed security function or technique as listed in Annexes A, B, C, D and E."	

77.	Orion	MS	Section 4.1.2	T	"The cryptographic boundary **shall**, at a minimum, encompass all security relevant functions and components of a cryptographic module." This does not seem true for software modules in a modifiable environment since the operating system is not included in the module. Remove the requirement.	
78.	Orion	MS	Section 4.1.2, hybrid cryptographic module	T	"The cryptographic boundary of a hybrid cryptographic module: shall be the composite of the module's component boundary and software or firmware component(s)." What restrictions are placed on the data passed between the boundaries and the channel over which data passes? Unless this data is protected, the composite module may not be secure. Please clarify.	
79.	Thales e-Security		4.1.3.3,	T	This section states that when switching between approved modes of operation, all CSP within the module shall be zeroised. Where other high-assurance mechanisms exist to provide long term secure storage of CSPs and ensure appropriate usage, zeroisation may not be necessary and could have serious operational consequences. The standard should state a requirement for ensuring that the CSP is not used; a specific solution (i.e. zeroising) should not be stated in this case.	
80.	NIST	Elaine Barker	4.1.1		"For hardware and firmware modules, the physical security and non-invasive security requirements found in Sections 4.6 and 4.7 **shall** apply. " Since the definition does not include the processor, etc., should this be included with the software module?	

81.	NIST	Elaine Barker	4.1.3, first para		"The operator **shall** be able to operate the module in an Approved mode of operation. An Approved mode of operation **shall** provide services using at least one Approved security function or SSP management technique. " It would be easier to combine the security functions and SSP management techniques into a single annex, since the currently anticipated management techniques could be considered to be security functions.	
82.	NIST	Elaine Barker	4.1.3, Sl 3 & 4		In addition to the requirements of Security Levels 1 and 2, for Security Levels 3 and 4, a cryptographic module **shall** indicate when the module is operating in an Approved mode of operation. Wouldn't it be better to indicate when it is NOT operating in an approved mode?	
83.	NIST	Elaine Barker	4.1.3.1		a. Each Approved mode of operation implemented in the cryptographic module and the configuration for each mode **shall** be described (see Appendix B.) b. Upon re-configuration from one Approved mode of operation to another, the cryptographic module **shall** perform the pre-operational self-tests (Section 4.9.1). Configuration and re-configuration as used here needs to be defined. The only definition is for configuration management, which nis not the same thing.	

84.	NIST	Elaine Barker	4.1.3.1		• Upon re-configuration of Approved modes at Security Levels 3 and 4, the RBG state **shall** be re-seeded. What is the reason for this? What does re-configuraion entail? A validated RBG will hopefully be able to protect itself. Need to discuss this.	
85.	NIST	Elaine Barker	4.1.3.2		If the module fails the pre-operational self-tests, the module **shall not** enter degraded mode of operation. 1) Change “enter” to “exit” 2) Need to include a case whereby some of the security functions or SSP mgmt. techniques that were non-operational now pass the tests and can be moved to the operational list.	
86.	NIST	Elaine Barker	4.1.3.2		However the output of an Approved RBG may be provided to a non-Approved mode without the zeroization of the RBG seed as long as the seed cannot be accessed in the non-Approved mode 1) Change to: “However the output of an Approved RBG may be provided to a non-Approved mode without the zeroization of the RBG seed or state as long as the seed or state cannot be accessed in the non-Approved mode. “ 2) Also, the specification of the RBGs (including the construction document) and the associated validation will hopefully prevent this.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Fiona Pattinson	4.2 1st sentence	E	"A cryptographic module shall restrict all logical information flow to only those physical access points and logical interfaces that are identified as entry and exit points to and from the cryptographic boundary of the module." Does not allow for software modules that have only logical interfaces. Note that the SFMI interface in the second bullet after this section specifies the cryptographic boundary, which in a software module will be purely logical (per section 4.1.1) Change to "A cryptographic module shall restrict all logical information flow to only those physical access points and / or logical interfaces that are identified as entry and exit points to and from the cryptographic boundary of the module."	
2.	atsec	Fiona Pattinson	4.2.2 4th para	T	"The cryptographic module specification shall, unambiguously, specify format of input data, including size restrictions for all variable length inputs. During execution the module shall verify the input data format for all input data. If a particular input violates the input data format, it shall be rejected by the module." The same verification should also be made for control data. Add a paragraph to describe the verification of control data. Suggest: "The cryptographic module specification shall, unambiguously, specify the format of control data, including size restrictions and expected values for all control data inputs. During execution the module shall verify the format of all control data. If a particular control data	

					input violates the specified data format, it shall be rejected by the module. “	
3.	atsec	Fiona Pattinson	4.2.2 5th para	E	Documentation shall include all module interfaces including the power interface. Is incorrect in reference to software modules. Documentation shall include all module interfaces including, if applicable, the power interface.	
4.	NIST	Elaine Barker			Except for the software cryptographic modules, all modules **shall** also have the following interface: According to the definition, firmware only includes code, so would not have a power interface.	
5.	atsec	Fiona Pattinson	4.2.3 1st para	E	“A cryptographic module which provides a Trusted Channel over a dedicated interface or port (see Sections 1.3, 2.1, 4.5 and 4.8), shall use this channel to securely communicate SSPs, service requests and service responses over unprotected communications channels.” A word is missing. “A cryptographic module which provides a Trusted Channel over a dedicated interface or port (see Sections 1.3, 2.1, 4.5 and 4.8), shall use this channel to securely communicate SSPs, service requests and service responses over otherwise unprotected communications channels.”	
6.	atsec	Peter Kim	4.2.3 Last para	T	Auditing capabilities can be difficult for certain modules, such as single-chip devices with no persistent memory. Remove the auditing requirement or replace it with a requirement to provide the status to the operator instead of a log.	

7.	atsec	Fiona Pattinson	4.2.3 7th para 2nd bullet	E	Missing word Change “identification of the initiator and target of a Trusted Channel.” To “identification of the initiator and the target of a Trusted Channel. “	
8.	atsec	Fiona Pattinson	4.2.3 Para 7 (audit)	T	“The following events **shall** be recorded by an audit mechanism: …” Although it is understood that not every module at level security level 3 or 4 has access to date and time, For those modules that do, this information should be recorded in audit records Add a bullet. “date and time (unless the cryptographic module does not have date and time information.)	
9.	CSEC	Jean Campbell	4.2.2	T	Page 21 “During execution the module **shall** verify the input data format for all input data. If a particular input violates the input data format, it **shall** be rejected by the module.” Should this be a requirement only for security level 3 and 4?	
10.	JCMVP		Draft Revised 4.2.2	T	Control output interface is added to FIPS 140-3 RD. For instance status information, as the response of control output, should be separated from data input.	

					Why data input and status input (status information from another module) are not separated?	
11.	JCMVP		Draft Revised 4.2.2, bullet 3	Ed	The examples listed for control output interfaces look strange, because items, such as switches, buttons, and keyboards, are not output devices but input devices. We suppose that the control output interface makes sense only for hybrid cryptographic module. If this interface shall also be documented for software/hardware cryptographic module, what kinds of thing do correspond to the interface? We would like to know more appropriate examples.	
12.	JCMVP		Draft Revised 4.2.3	T	It seems strange if requirements for security level 3+ are applied to single-chip cryptographic module because it seems no JCMVP realistic that a single-chip module supports the services of trusted channel.	
13.	NSRI(National Security Research Institute)	Korea CMVP (Jihoon JEONG)	4.2.2(1st para) pp. 21		First bullet : What's the meaning of **'output commands'** of the Control output interface? This word shall be replaced by **'return codes'.**	
14.	NSRI(National Security Research Institute)	Korea CMVP (Jihoon JEONG)	4.2.2(1st para) pp. 21		Third Bullet : If the Status output interface in FIPS 140-2 is divided into Status & Control output interface in FIPS 140-3, then the **'return codes'** included in the Status output interface should be moved to the Control output interface.	
15.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.1	E	If these interface descriptions are the same, why is it necessary to repeat because it's a different type of module? Let's just use module interface to replace HMI, HSMI, HFMI, and SFMI.	
16.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.2	E	Interface tacked on to each of the five types is not necessary.	

17.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.2	T	Control input and control output uses exactly the same examples. I cannot discern the technical need of control output from the text provided. If control output is needed (since control input is understood from FIPS 140-2) what makes control output different so that the vendor can understand the requirement? Additionally, how does control output differ from status output?	
18.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.2	T	Power requirement (shall statement) is currently defined addressing only power into the module. Does this need to be broken down into input and output? For example, is the power provided by many standalone devices to USB interfaces to be included? Power from USB interfaces may ultimately be a source of non –invasive attacks.	
19.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.3	T	The requirements for trusted channel appear to only apply to the encrypted link and not the manual link.	
20.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.3	T	A cryptographic module which provides a Trusted Channel over a dedicated interface or port (see Sections 1.3, 2.1, 4.5 and 4.8), shall use this channel to securely communicate SSPs, service requests and service responses over unprotected communications channels. The uses of the word “over” are ambiguous.	
21.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.3	T	The difference between a Trusted Channel service and the Trusted Channel is not clear, maybe the first sentence could be removed.	
22.	CMVP	Beverly Trapnell, Kim Schaffer	4.2.3	T	The following events shall be recorded by an audit mechanism: • attempts to use the Trusted Channel function and whether the request was granted. • identification of the initiator and target of a Trusted Channel. How does this apply to hardware only	

					modules? How is this output?	
23.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.2, 4.2.2 Definition of Interfaces, *Data output interface*	T	It is too much to expect that data output has to be inhibited when the module is performing manual key entry or software/firmware loading if the data output interface is logically disconnected from these functions. Suggest removing manual key entry and software/firmware loading from the list of services for which data output must be inhibit.	
24.	EWA-Canada IT Security Evaluation & Test Facility	Dawn Adams	4.2, 4.2.2 Definition of Interfaces, *Control output interface*	T	It is assumed that these are controls for another cryptographic module. This interface is irrelevant since a cryptographic module, not a system, is validated. Suggest removing this interface type.	
25.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.2, 4.2.2 Definition of Interfaces, Paragraph 4	T	Suggest removing this requirement.	
26.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.2, 4.2.3 Trusted Channel, Paragraph 1	T	Why would everything including PSPs need to use the Trusted Channel? Suggest requiring the Trusted Channel only for the communication of secret and private keys.	
27.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	4.2, 4.2.3 Trusted Channel, SECURITY LEVELS 3 AND 4, Paragraph 4	T	Software cannot be validated at Security Levels 3 and 4 so an audit mechanism would be required for firmware, hardware, or hybrid modules. This is excessive. Suggest removing the events that are to be recorded.	
28.	InfoGard		Section 4.2.1, Bullet 2	T	For the SFMI scenario, is the cryptographic boundary in this sentence referring to the logical boundary? Suggest adding “logical” to Bullet 2 as follows: *“…including parameters that enter or leave the module’s* ***logical*** *cryptographic*	

					boundary…".	
29.	InfoGard		Section 4.2.2, Bullet 6	E	Sentence preceding Bullet 6: "Except for the software cryptographic modules, all modules shall also have the following interface:" Bullet text (second sentence): "A power port is not required, and a power interface may not exist when all power is provided or maintained within the cryptographic boundary of the cryptographic module (e.g., by an internal battery)." Suggest rewording the sentence preceding Bullet 6 as follows: *"Except for software cryptographic modules, modules may also have the following interface:".*	
30.	InfoGard		Section 4.2.3, Paragraph 1	E	The requirements outlined in this paragraph appear to refer to the Internal Trusted Channel type (refer to Section 2.1). Explicitly reference the Trusted Channel type as Internal.	
31.	InfoGard		Section 4.2.3, Paragraph 1	T	The following description requires clarification: "A cryptographic module which provides a Trusted Channel over a dedicated interface or port…shall use this channel to securely communicate SSPs, service requests and service responses over unprotected communications channels." • The definition of an Internal Trusted Channel (refer to Section 2.1) does not make mention of this being a "dedicated interface or port" but rather a local interface without intervening systems. Consistency in the definition is needed. • The existing text implies that all service requests and responses are required to	

					go over this interface. The definition of an Internal Trusted Channel (refer to Section 2.1) only mentions transporting CSPs and other sensitive information. Consistency in the definition is needed. The definition provided in Section 2.1 and the text found in Section 4.2.3 need to be made consistent.	
32.	InfoGard		Section 4.2.3, Paragraph 2	E	The requirements outlined in this paragraph, along with the accompanying three bullets, appear to refer to the External Trusted Channel type (refer to Section 2.1). Explicitly reference the Trusted Channel type as External.	
33.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.2.1	G	For each of the three interfaces defined change “The total set of commands used to request the services of the SPECIFIC module, including parameters that enter or leave the module’s cryptographic boundary as part of the requested service”. to “The total set of commands used to request the services of the SPECIFIC module, including parameters that enter or leave the module’s cryptographic boundary as part of the requested service and status information provided by the module”. Rationale: NOTE: “SPECIFIC” above refers to “Hardware”, “Software” and Hybrid”. As defined only services requested from the module pass on an interface. Interfaces from the module may contain unsolicited status information, for example an alarm indicator.	
34.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.2.2	G	Are these interfaces potentially composite in nature? Most Military Systems I am familiar each physical interface is considered a separate interface. If this is the case, it should be stated in the requirement. Rationale: Ensure all readers have a consistent understanding of the requirements.	

35.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.2.2	G	The definition of Status Output Interface “All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module shall exit via the "status output" interface. Status output may be either implicit or explicit.” is very different from Interface definitions of Military and commercial systems I have worked. Statuses of commands are typically captured in the definition of the command/response interface. Typically these are one or more fields in a response message. Rationale: Dissecting the status portions of a message out of the module response and placing this into a separate logical interface seems counterintuitive.	
36.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.2.3	G	Recommend changing “If a Trusted Channel is provided, then the following requirements shall be met” to “If an external Trusted Channel is provided, then the following requirements shall be met”. Rationale: As written, this requirement would apply to internal trusted channels. This would violate the definition of an internal trusted channel above.	
37.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.2.3	T	Discussion on Trusted Channels used for Security Level 3 and 4 communications with the operator. What cryptographic module will provide the “source authentication and shall prevent unauthorized modification, substitution, disclosure, and playback of sensitive security parameters”. Rationale: Definition of an internal Trusted Channel doesn’t require authentication or other “active” measures to protect the information exchanged. This requirement cannot be met without some protected cryptographic process. An adversary could	

					modify messages and checksums or other non-cryptographic verification means, preventing the “operator” from detecting message modification.	
38.	Motorola	Kirk Mathews	4.2.3	G	For Level 3 and Level 4 modules all SSPs, authentication data, control input, and status output must be communicated over a trusted channel. The requirements for a trusted channel are not clear. How do they apply to embedded modules? Does this mean all service request & response messages must be encrypted and must also include message numbers to prevent replay attacks?	
39.	Motorola	Kirk Mathews	4.2.3	G	For Level 3 and Level 4 modules all SSPs, authentication data, control input, and status output must be communicated over a trusted channel. The requirements for a trusted channel are not clear. How do they apply to embedded modules? Does this mean all service request & response messages must be encrypted and must also include message numbers to prevent replay attacks?	
40.	Motorola	Ken Fuchs	4.2.3	G	What constitutes a Trusted Channel?	
41.	NSA	TWG	4.2	T	Under the discussion of inhibiting the “data output” interface during various critical functions, suggest adding the function of “an internal transfer of a CSP.”	
42.	NSA	TWG	4.2.2	E	All (hardware) modules SHALL have a power interface, but the definition of power interface states that “a power interface may not exist when all power is provided … within the cryptographic boundary.” Either the definition should be modified or the requirement should be relaxed.	
43.	NSA	TWG	4.2.2	T	Why was “To prevent the inadvertent output of sensitive information, two independent internal actions shall be required to output CSPs. These two independent internal actions	

					shall be dedicated to mediating the output of the CSPs" not carried forward from the 2007 draft?	
44.	NSA	TWG	4.2.2	T	Power interface: "Except for the software cryptographic modules, all modules shall also have the following interface" contradicts "…a power interface may not exist when …"	
45.	NSA	TWG	4.2.2	E	Need a "the" in ….unambiguously, specify **the** format…." and a comma in "During execution**,** the module…" Need a period at the end of the last sentence in that section.	
46.	NSA	TWG	4.2.3	T	We have the following statement about the trusted channel for levels 3 and 4, "The Trusted channel shall provide source authentication and shall prevent unauthorized modification, substitution, disclosure and playback of sensitive security parameters". It is assumed that this statement implies that the trusted channel provides confidentiality to all SSPs including PSP's (which by definition, don't require confidentiality). It is not clear what the endpoints of a trusted channel are (one endpoint is the module). In particular this is questioned in the context of certain protocols that exchange what might be considered PSPs unencrypted between two endpoints. For example, TLS, in its handshaking protocol sends the public key half of its digital signature key pair to the other side without encryption.	
47.	NSA	Wan-Teh Chang	Section 4.2.1, page 20.	Editorial	The definitions of HMI, SFMI, and HSMI/HFMI are essentially the same. Why define the same thing three times? Why not just call them "module interface"? Alternatively, please tailor the definitions to each type of module.	
48.	NSA	Wan-Teh Chang	Section 4.2.2, first paragraph of page 21.	Technical	The new "control output interface" is defined in exactly the same way as the control input interface. It's not clear what the control output interface is or how it differs from the status output interface. Please give some examples of the control output interface to clarify this.	

49.	Oberthur Technologies	Clement Capel & Christophe Goyet	§ 4.2.3, § 4.5.1, § 4.9	T	the standard requires many audit logs (§ 4.2.3, § 4.5.1, § 4.9) to store information on trusted channels and test results. This could require a large amount of memory not available on a smartcard. As new generation smart cards like the FIPS 140-2 Level 3 validated Oberthur ID-One Cosmo v7 cards include defensive mechanisms (reset, killcard ...) in case of abnormal event impacting sensitive assets such an audit can reasonably be considered as useless. In the Common Criteria, the audit requirements are generally regarded as not applicable. We recommend therefore to introduce these audits as optional when active defense mechanisms are already implemented.	
50.	Oracle	Matt Ball	4.2.2, third bullet	T	It is unclear why a Control output interface should be a required interface on a cryptographic module. Consider making the Control output interface an optional interface. Maybe this interface needs further clarification.	
51.	Oracle	Matt Ball	4.2.2. third from last paragraph	E	Consider rewording: “The cryptographic module specification shall specify an unambiguous format for the input data, ...”. The format should be unambiguous, not the act of specifying.	
52.	Oracle	Matt Ball	4.2.2, second from last paragraph	E	This sentence does not make it clear how the power interface factors into the requirement. Consider rewording as one of the following: “Documentation shall specify all module interfaces that include the power interface.” or “Documentation shall specify all module interfaces, including the power interface.”	
53.	Orion	MS	Section 4.2.2, Data output interface, last sentence	T	Does this requirement for inhibiting data output prevent multi-threaded applications where several independent sub-modules are placed in a single container used as the physical boundary? In this case one sub-module may be outputting data while another module is performing a pre-operational self-test. It would be nice to allow for this implementation for high speed multi-channel network security. Please clarify.	

54.	Orion	MS	Section 4.2.3, Trusted Channel, Security Levels 3 and 4.	E	For L3 and L4, it would be helpful to provide some guidance as to when the internal trusted channel is used, when the external trusted channel is used, and when both are used. Consider providing guidance on trusted channel.	
55.	Defense Manpower Data Center (DMDC)	CTIS	4.2.3	T	Smartcard token like DoD Common Access Card (CAC) has severely limited amount of memory resources inside the chip. The FIPS 140-3 requires many audit logs to store information on trusted channels and test results. We recommend introducing these audits as optional for smart card	.
56.	Primekey	Anders Rundgren	4.2.3		I believe that the text concerning the "Secure Channel" may not be compatible with most implementations since these will probably use the SKS security model which is quite different to the implicit model used in FIPS-140 (if I understood it correctly...). In SKS: - Crypto modules authenticate to issuers - Issuers do not authenticate to crypto modules - Users authenticate to issuers but not to crypto modules except through optional PIN-codes - Crypto modules authenticate through built-in device certificates and keys Previous version of Secure Channel: http://www.globalplatform.org/specifications/card/GPC_2%202_D-SecureChannelProtocol03-2nd-public_review.pdf SKS: http://webpki.org/papers/keygen2/secure-key-store.pdf	

					http://webpki.org/papers/keygen2/session-key-establishment--security-element-2-server.pdf	
57.	SPYRUS, Inc.	WSM	4.2.3	T	There is no mention of a differentiation of requirement based on type, i.e. Internal vs. External as described in 2.1 under Trusted Channel. Add material from 2.1, or an elaboration of it, to expand 4.2.3 or delete the Internal/External taxonomy from 2.1.	
58.	Thales e-Security		4.2.2	T	4.2.2 States “All electrical power externally provided to a cryptographic module (including power from an external power source or batteries) shall enter via a power interface." This would discount the use of evolving technologies such as Power-over-Ethernet (POE) which could legitimately be used (and share a traffic interface) without negative impact on security.	
59.	Thales e-Security		4.2.3, 4.8.3, 4.8.4 Trusted Channel	T	The Trusted Channel does not allow for either the initial commissioning of a unit or the fact that not all data is required to be protected from disclosure (for example a Public Security Parameter or status outputs such as an LED interface.) Additionally it is hard to see how it would be applied to (i) physically protected point to point channel into the crypto module e.g. key fill interface for red key (ii) remote server distributing already encrypted and signed black key. i.e. Authentication and protection for Black Key packages is already provided using strong encryption and signature and therefore does not need a 'trusted channel'. Regarding the requirement for the port to be dedicated: The use of a Trusted Channel renders the physical nature of the interface irrelevant. Therefore the interface can be shared for other activities.	

60.	NIST	Elain Barker	4.2.3		"The module **shall** provide an indication to the module operator as to whether or not the Trusted Channel is operational." Indicate both states or only one? Preferably indicate when it s not operational.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	Apple, Inc.	Jon Callas	4.3 / 4.3.1	G	It would be good to have more guidance within 4.3 for software systems. Software systems do not have roles such as “Crypto Officer” or “Maintenance.” They have roles such as “Administrator” or an operating system mode (e.g. “kernel mode” or “ring 0”) or privileged processes within the module. Similarly, separate operators do not directly correspond to software subsystems. Consider, for example, a software module that will implement SSL/TLS or a remote-access VPN. The crypto officer role is provided by a combination of file protection, privileged processes, and OS and hardware software protections (kernel mode, process isolation, sandboxing, etc). But the “Maintenance” role is provided by the very same software and is often hard to separate or even distinguish from the “Crypto Officer.” It is not difficult for us to intuit what these mean for software, nor is it difficult for us to create diagrams of what functions belong to what role. Moreover, these diagrams and explanations are artificial. The software is seldom, if ever organized that way. If software makes a kernel-mode call to do a cryptographic operation by reference, it operates within the same software user, but has changed conceptual users and roles by moving from user mode to kernel mode. It would be nice to have a paragraph or so saying pretty much that NIST understands	

					that so long as there are well-defined and explained boundaries (syscall, message passed, etc.) to conceptual roles, there isn't a problem. A use case with a hypothetical module that performs some function like a SSL, VPN or disk encryption can be used illustratively, as well. This doesn't have to be big, but it saves debate over what the roles mean for software.	
2.	Apple, Inc.	Jon Callas	4.3 / 4.3.2	G	Similar to my comment above, 4.3.2 discusses the differences between role-based, and identity-based authentication. In general, FIPS 140 considers identity-based encryption to be better than role-based. Level 2 permits either, while level 3 requires identity-based authentication. Yet software systems do authentication through identity-based mechanisms. A user on a system will have an account identifier and they will authenticate to that identifier. When they have role-based authentication, it is done by creating an account with an identity that names a role (Adminstrator, root, etc). Roles are typically attributes of identities or the system creates identities that represent roles. It is thus somewhat counter-intuitive that a module that cannot achieve level 3 must jump through hoops to have authentication lower than level 3. Consider, for example, a computer with an account for Alice and Bob. Bob is the administrator and crypto officer, and Alice is a non-privileged user. It won't take much, but clarification would be welcome. How does NIST consider this to be role or identity-based authentication? Additionally, there may be cases where the	

					authentication is tacit or derives from system initialization. Consider a system that boots from a signed kernel where hardware/firmware validates the kernel against a trusted cryptographic root, and then launches processes (also from signed executables), including a security daemon that represents the crypto officer. Conceivably, this could be described as either role or identity-based authentication of the services, or it could be considered to be Trusted Channel. Given that every trusted modern software system follows essentially this path (and the untrusted ones merely don't have the signed executables), NIST's guidance would regularize all software modules so that we as an industry described them with the same language. A paragraph or two for each use cases would be invaluable.	
3.	Apple, Inc.	Jon Callas	4.3.2	E	In the list at the end of 4.3.2, it says that for level 2, the module shall employ role-based authentication. It is implied that level 2 can also employ identity-based authentication. This is backed up by the table on page 15 stating the same. But a literal reading of the requirement could lead to the opinion that level 2 shall use role-based, but not identity-based authentication. Please make this agree with the table on page 15, and explicitly say that either is acceptable.	
4.	Apple, Inc.	Jon Callas	4.3.3	T	Please also state a little more how these services should be provided. I presume, for example, that an SSL provider does not need to give its status at all times on all web pages to all users. However, I would expect that it be a requirement for some user if not any user to be able to get that information if they issue the right request, or	

					type the right command on a command line. Again, this is a case where it would help for NIST to explain how this works within a software system.	
5.	atsec	Peter Kim	4.3.1 4th Para, 3rd sentence	T	If zeroization is an option for either entry or exit, then the Maintenance Role could potentially retrieve existing CSPs or introduce CSPs respectively (e.g., swapping out key storage) Clarify the intent. It would seem most prudent to zeroize upon entry and exit, to ensure the maintenance operator cannot compromise the existing CSPs and cannot introduce CSPs.	
6.	atsec	Fiona Pattinson	4.3.1 7th para	E	The term “Authorized role” is used. The term is not defined. The significance of the capitalized “A” is unknown. Note that the term is used again in para 8 without the capitalization. This is confusing. Clarify the meaning of “Authorized role”	
7.	atsec	Peter Kim	4.3.2 4th Para	T	Under FIPS 140-2, we have the ability to use security functions to facilitate authentication (e.g. SHA-1, RSA signature verifications, etc). Reword: “Except for the Trusted Role(s) establishment, Trusted Channel establishment, and facilitating authentication, services using Approved or Allowed security functions shall not be available to an operator until the operator’s authentication is completed successfully. A cryptographic module may permit an authenticated operator to perform all of the services”	

8.	atsec	Peter Kim	4.3.3.2 4th bullet	E	Approved authentication technique is not defined; instead Approved data authentication technique should be used, because it is defined. Reword: "The module shall support an Approved data authentication technique to verify the validity of software/firmware that may be loaded."	
9.	Cisco	Max Pritikin IEEE 802.1AR Editor	General	G	This and the following comments concern the use of an "IEEE 802.1AR Device Identity" for authentication of the device. IEEE 802.1AR details the use of an X.509 certificate that is installed on a device during manufacturing. This allows the automation of secure provisioning and thus provides for an initial level of infrastructure security without costly manual configuration. The advantages of such an approach have been seen across a wide variety of pre-IEEE 802.1AR standards including but not limited to: Data Over Cable Service Interface Specification's (DOCSIS) Baseline Privacy Interface+ (BPI+), Worldwide Interoperability for Microwave Access (WiMAX), various IETF protocols, the Trusted Platform Module (TPM) "Endorsement Key" along with consumer products. Additionally it will be very important for the initial security of wide-scale infrastructure projects such as Smart Grid or the "Internet of Things". The adopters of the IEEE 802.1AR-2009 standard as well as existing uses of pre-802.1AR device identity certificates will be concerned with how and when such credentials should be available (and in which Approved Modes, at which Levels). Note: Initial Device ID (IDevID) is a factory installed credential. 802.1AR also specifies a Locally installed Device Identity (LDevID) which would of course be handled like any	

					other CSP. Include text clarifying interactions with manufacturing installed device authentication credentials at the appropriate locations in the document. In General I suggest an additional sub-section (in section 4) that discusses Device Authentication credentials. This would be analogous to the existing section 4.3 that discusses the device's authentication of users. Specifically existing sections could benefit from clarifications concerning the existence of an IDevID. Additional T comments in this response propose some resolutions intended to address these concerns.	
10	Cisco		4.3.3.1	T	It is under unclear to what extent how bypass decisions are made must be described? Are there further requirements. Provide additional clarification.	
11	Cisco		4.3.3.1	T	The bypass status output requirements seem to indicate that a status output has to be output every time plaintext, plaintext, or a decision to toggle between plaintext and plaintext is made. Some modules handle thousands of simultaneous encrypted and clear text sessions. If the required output is an indicator for each decision on each connection, the output loses its usefulness and could potentially hide other useful status output. Clarify the requirement: Recommendation: Make an on-demand snapshot of encrypted/plaintext connect acceptable	

12	CSEC	Claudia Popa	4.3.2 Authenticatio n	T	"If default authentication data is used to control access to the module, then default authentication data shall be replaced upon first authentication. **This default authentication data does not need to meet the zeroization requirements."** The default authentication data is supposed to be changed the first time the entity accesses the crypto module, and after that the module does not contain "default" authentication data. I don't know why this sentence is needed: **This default authentication data does not need to meet the zeroization requirements."**	
13	CSEC	Claudia Popa	4.3.3.2, first bullet	E/T	"The logic performing the external software or firmware loading shall be logically disconnected from all data output". The sentence is not clear. The **logic…** shall be **logically** disconnected from the **interface** that performs data output, OR from the **logic** performing data output?	
14	CSEC	Claudia Popa	4.3.2 Authenticatio n	E/T	On page 24, "The strength of authentication mechanism shall be described (see Appendix B)". Where are the requirements for the strength of the authentication mechanism defined? Annex E just refers to an Implementation Guidance document that was not distributed.	
15	CSEC	Jean Campbell	4.3.1	T	Page 24 Why there are no requirements for the strength of the authentication?	

16	CSEC	Jean Campbell	4.3.1	E	Do we need a special section for Trusted Channel Requirements? Why don't leave these requirements in specific sections, like: key management, authorization, etc?	
17	CSEC	Jean Campbell	4.3.2	G	Page 23. "For a software cryptographic module at Security Level 2, the operating system may implement the authentication mechanism." Why is this only for Security Level 1 and 2?	
18	JCMVP		Draft Revised 4.3 4th paragraph	T	Does "powered off and subsequently powered on" include power glitching? If not so, you should describe the minimum interval between power-off and power-on.	
19	CSEC	Jean Campbell	4.3.2	E	Page 24 "If the operating system implements the authentication mechanism, then the authentication mechanism **shall** meet the requirements of this section. " Change to If the operating system implements the authentication mechanism, then the authentication mechanism **shall** meet **or be configured to meet** the requirements of this section.	
20	CSEC	Jean Campbell	4.3.2	T	"This default authentication data does not need to meet the zeroization requirements". Suggestion: Maybe for level 3 and 4 it should be zeroized.	
21	CSEC	Jean Campbell	4.3.2	E	Page 23, second bullet: "The Approved Authentication mechanism shall be met…". Change as below: "The Approved Authentication mechanism	

					shall be implemented in the module and not rely on documented procedural controls…"	
22	CSEC	Jean Campbell	4.3.2	G	Page 23 *"Identity-Based Authentication*: If identity-based authentication mechanisms are supported by a cryptographic module, the module **shall** require that the operator be individually and uniquely identified, **shall** require that one or more roles either be implicitly or explicitly selected by the operator, and **shall** authenticate the identity of the operator and the authorization of the operator to assume the selected role or set of roles. The authentication of the identity of the operator, selection of roles, and the authorization of the assumption of the selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module **shall** verify the authorization of the identified operator to assume any role that was not previously authorized". What if the operator is not authorized?	
23	CSEC	Jean Campbell	4.3.2	E	"Except for the Trusted Role(s) and Trusted Channel establishment, services using Approved or Allowed security functions **shall** not be available to an operator until the operator's authentication and **authorization** is completed successfully." Include "authorization".	
24	CSEC	Jean Campbell	4.3.2.	E	"When a cryptographic module is reset, rebooted, powered off and subsequently powered on, the module **shall** require the operator to be authenticated." Include also "change mode of operation" in the list of actions that require the operator to	

					be authenticated.	
25	CSEC	Jean Campbell	4.3.3.2	T	When is the integrity key loaded? Shouldn't be at factory?	
26	CSEC	Jean Campbell	4.3.3.2	E	Second bullet, add the text below: "… • by the cryptographic module itself, or • by another Validated cryptographic module **operating in an Approved mode of operation."**	
27	NSRI(National Security Research Institute)	Korea CMVP (Jihoon JEONG)	4.3.3.2(1st para) pp. 25		First Bullet : '… disconnected from all data output' shall be replace by '… disconnected from **all other interfaces** of the cryptographic module'.	
28	CMVP	Beverly Trapnell, Kim Schaffer	4.3.1		"The Trusted Role is a state of the module where the module can perform cryptographic operations and other Approved security functions without any outside entities authenticated to the module." Can you use trusted role for non-Approved security functions?.	
29	CMVP	Beverly Trapnell, Kim Schaffer	4.3.1	E	"The Trusted Role is a state of the module where …" should be "The Trusted Role is a state of the module in which …"	
30	CMVP	Beverly Trapnell, Kim Schaffer	4.3.1	T	Consider not zeroing maintenance and CO authentication. This would restrict who can perform maintenance and does not open the access to who is first to operate the module.	

31	CMVP	Beverly Trapnell, Kim Schaffer	General	G	It appears that each requirement has an implicit documentation requirement. Can we make this explicit at the beginning of section 4 and then remove all others unless a specific type or content of documentation is needed?	
32	CMVP	Beverly Trapnell, Kim Schaffer	4.3.2	T	The title Authentication should be Operator Authentication	
33	CMVP	Beverly Trapnell, Kim Schaffer	4.3.2	T	If a cryptographic module permits an operator to change roles, then the module shall verify the authorization of the identified operator to assume any role that was not previously authorized. Delete “to assume any role that was not previously authorized. “	
34	CMVP	Kim Schaffer	4.3.2	T	Annex E should contain Approved and Allowed authentication mechanisms	
35	CMVP	Kim Schaffer	4.3.2	E	Security Level 1 should be moved up in this section so that there is not a conflict between authentication requirements and Level 1 lack of authentication requirements.	
36	CMVP	Kim Schaffer, Randall Easter	4.3.2 Security Level 1 requirements	T	Suggest adding: “If a module does not support authentication mechanisms, the module shall [04.44] require that the operator either implicitly or explicitly select one or more roles.”	
37	CMVP	Kim Schaffer	4.3.2	T	Consider replacing “The strength of authentication mechanism shall be described (see Appendix B.)” with ”The strength of the authentication mechanism shall meet the strength requirements in accordance with Annex B).”	

38	CMVP	Kim Schaffer, Randall Easter	4.3.3	T	Consider adding a definition of the services and the information necessary to be considered for a module, suggest “Services shall refer to all of the services, operations, or functions that can be performed by a module. Service inputs shall consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions. Service outputs shall consist of all data and status outputs that result from services, operations, or functions initiated or obtained by service inputs. Each service input shall result in a service output.”	
39	CMVP	Kim Schaffer, Randall Easter	4.3.3.2	T	Replace the requirements with the following: • the loaded software or firmware shall undergo FIPS validation, an independent verification or evaluation scheme as appropriate prior to loading; • the Software/Firmware Load Test specified in Section 4.9.2 shall be performed; • all data output via the data output interface shall be inhibited until the software/firmware loading has completed. It can continue upon failure of the Software/Firmware Load Test; • the cryptographic module shall restart after a successfully passing the Software/Firmware Load Test; and • the modules versioning information shall be modified to represent the addition of the newly loaded software or firmware or the full replacement.	
40	Cryptsoft	Tim Hudson	4.3.2	T	Is delegation of authentication to outside the cryptographic module permitted or not-permitted? Can a trusted channel be established to another cryptographic module where authentication is performed? Typically OTP validations and other such mechanisms are performed outside a cryptographic module. Is this excluded?	

					There should be no ambiguity in the standard as to whether or not the authentication must be contained entirely within the cryptographic module.	
41	Cryptsoft	Tim Hudson	4.3.2	T	"If the operating system implements the authentication mechanism, then the authentication mechanism shall meet the requirements of this section." If the operating system implements the authentication mechanism using Approved functions then this implies that the operating system must be using a validated implementation, however the limitation of the statement to "of this section" introduces an ambiguity in the requirements. Is it allowed for a SW-L2 module to use an operating system which uses approved cryptographic algorithms that are **not** provided by a validated cryptographic module? If not then the wording of this section needs to be changed to preclude this.	
42	Cryptsoft	Tim Hudson	4.3.2	T	"The module shall implement an Approved authentication mechanism as specified in Annex E." There are no approved authentication mechanisms specified in Annex E and accordingly this requirement should be deleted as it cannot be met.	
43	Cryptsoft	Tim Hudson	4.3.3	T	It has been suggested during multiple workshops that a mechanism to enable the operator of a module to compare the software or firmware MAC or digital signature with that which was provided by the Vendor to the Testing Laboratory. A service to support this should be added into the list of required services. Suggested resolution: add	

					"Module's Integrity Check: Output the Integrity Check details of all software and firmware of the Cryptographic Module". Refer to 4.4 Software/Firmware – the service necessary to support those requirements should be documented and accessible to the User/Operator. Note that the requirements in that section simply require a pass/fail indication and nothing which can be compared against external values.	
44	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.3**, **4.3.1 Roles**, Paragraph 7	T	In FIPS 140-2, an operator was allowed to run RNGs without being required to assume an authorized role, i.e., to be authenticated to the module at Security Levels 2 to 4. Will this be allowed for FIPS 140-3? Suggest adding this information to the standard.	
45	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.3**, **4.3.3 Services**, *Zeroize*	T	Although highly unlikely, a module may only support SHS algorithms which, of course, use no SSPs that would need to be zeroized. Suggest specifying this service more specifically as "Perform zeroization of any SSP as specified in Section 4.8.6 (may be performed procedurally).	
46	IBM Research, Zurich	Visegrady, Tamas	**4.3.2 Security level 4**		We consider the proposed Level 4 requirement, two-factor authentication(2FA), to be indistinguishable from other authentication at the module level. We think this requirement may not be properly enforced by modules, as it ties authentication to host policies, i.e., outside the secure module boundary. In our opinion, in the typical restricted environment of hardware security modules (HSMs) or libraries, 2FA will not increase security beyond what's provided by identity-based authentication. Practically, 2FA will most likely use some binary representation of authentication data at the module boundary,	

					and verify this representation---hash, signature from a token or similar bit sequence. The standard already provides adequate requirements on handling similar authentication data. 2FA effectively requires to authenticate by specific auxiliary devices (smartcard readers, physical tokens, biometric processing), but does not provide inherently higher assurance than non-2FA authentication for the binary authentication data itself. An HSM or similar restricted environment can not easily verify _how_ a signature was generated. If the 2FA process relied on external policies to implement 2FA, the module could not enforce overall security. We propose to mandate identity-based authentication for Security Levels 4, mirroring Level 3, optionally allowing 2FA for environments where source verification is feasible.	
47	InfoGard		Section 4.3.1, Paragraph 3	T	Although the concept of the Trusted Role is well understood, some vendors and possibly some laboratories may misuse the role as a way to allow cryptographic services without authentication. Clear requirements, either in the standard or the DTR, should be in place to maintain the intent of the Trusted Role so it cannot be misused.	
48	InfoGard		Section 4.3.1, Paragraph 3	E	The term Trusted Role could be misunderstood, and unintentionally related to the Trusted Channel; especially with the requirement that a Trusted Channel must provide source authentication. Just to remove any confusion, change the name to something else.	

49	InfoGard		Section 4.3.1, Paragraph 4	E	"All unprotected SSPs shall be zeroized when entering or exiting the Maintenance Role." Two comments: • SSPs consist of public key parameters as well as CSPs. There should be no concern in an unauthorized disclosure of a public key parameter. In addition, in some cases, this could cause the module to transition into an unrecoverable state (e.g. public key used to perform the pre-operational self-test for FW integrity). • This is the only place where the standard states that zeroization should occur upon entering or exiting the maintenance role. All other places throughout the standard state that the module should be zeroized upon entering the maintenance role/interface; recommend consistency. Suggested text: *"All unprotected CSPs shall be zeroized when entering or exiting the Maintenance Role."*	
50	InfoGard		Section 4.3.1, Paragraphs 3 & 7 Section 4.3.2, Paragraph 4	T	Is authentication to the module using a cryptographic function considered a Trusted Role function or is it an exception to Section 4.3.1 Paragraph 7 and Section 4.3.2 Paragraph 4?	
51	InfoGard		Section 4.3.1, Paragraph 3, last sentence	T	What configuration of Trusted Role is required? Does this refer to the establishment of SSPs used by a Trusted Role function, for example? Is there a minimum bar for configuration in this context?	
52	InfoGard		Section 4.3.2, Paragraph 5, last sentence	E	"Authentication data within a cryptographic module shall be protected against unauthorized use, disclosure, modification, and substitution." Not all authentication data should have to satisfy the disclosure requirement, as in some instances, the authentication data may not be	

					considered a CSP. Examples include the following: • Public keys (e.g. DSA public key) can be used to support authentication; however, disclosure of such a key would not inadvertently compromise the module by allowing unauthorized individuals to access the module. • Some in industry do not believe that biometric information, such as fingerprint images and even templates, should be considered secret, as the fingerprint is available everywhere the operator touches. Should this also have a blanket requirement that it not be disclosed? Suggested text: *"Authentication data within a cryptographic module that is considered a CSP (e.g., PIN, Passwords, Secret Keys) shall be protected against unauthorized use, disclosure, modification, and substitution. For such authentication data that is not considered a CSP (e.g., cryptographic public keys used to verify digital signatures), the data shall be protected against unauthorized use, modification, and substitution."*	
53	InfoGard		Section 4.3.2, final bullet (top of page 24)	T	What is the minimum bar for additional factors in multi-factor authentication? Does each factor have to meet a minimum strength, with a corresponding rationale? This requirement may not be properly enforced by modules, as it ties authentication to host policies (i.e., outside the secure module boundary). In the typical restricted environment of hardware security modules (HSMs) or libraries, 2FA will likely not increase security beyond what is provided by identity-based authentication. Practically, 2FA will most likely use some binary representation of authentication data at the module boundary,	

					and verify this representation - hash, signature from a token, or similar bit sequence. The standard already provides adequate requirements on handling similar authentication data. We propose to mandate identity-based authentication for Security Level 4, mirroring Level 3, optionally allowing 2FA for environments where source verification is feasible.	
54	InfoGard		Section 4.3.2	G	Where is the strength of authentication requirement (e.g., 1/1x10^6) specified in FIPS 140-3? Is that planned for Annex E?	
55	InfoGard		Section 4.3.3, *Module's Version Number*	T	Is an exact match of name and version information required to be output from the module? The term "correlated" in this bullet suggests some latitude and could allow for not an exact match or correlating the versioning with other sources such as vendor website or Security Policy. The precision of version numbers may prove difficult. The module should be required to list and display the precise version number that would exactly match the validation certificate. Suggest rewording the text as follows: *"Output the name or module identifier and the versioning information of the cryptographic module to allow verification that it matches the corresponding validation certificate (e.g., hardware, software, and/or firmware versioning information)."*	
56	InfoGard		Section 4.3.3, *Zeroize*	E	The Zeroize service is only required for a module with CSPs (e.g., only public keys are stored within the module). Suggest the text indicate that the zeroization service is required when CSPs are stored in	

					the module.	
57	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.3.1	T	Cryptographic modules can be “born” with all necessary cryptographic initialization and NOT require a cryptographic operator role at all. During manufacturing the placement of static memory chips containing required trust anchors and module specific public/private keying material could be performed. When the module is first enabled, it would be able to read and verify that these CSPs exist. These modules would not require a Crypto Officer role. Rationale: Devices could be manufactured that do not support or require this role, so it should not be considered mandatory.	
58	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.3.1	T	States “The operation of the Trusted Role shall be configured by the Crypto Officer.” Some cryptographic modules may be “born” in this trusted role and may not support a Crypto Officer. Rationale: Trusted Platform Modules may be prevented from being FIPS 140 certified by this requirement, since they must be ready to provide services automatically and not require a Crypto Officer role.	
59	Motorola	Kirk Mathews	4.3.2, 6th paragraph	G	"If default authentication data is used to control access to the module, then default authentication data shall be replaced upon first-time authentication." Can this requirement be satisfied by procedural controls (documentation) or does this have to be enforced by the module?	

60	Motorola	Kirk Mathews	4.3.1	G	"Trusted Role: a state of the module, achieved only upon configuration by a Crypto Officer, where the module can perform cryptographic operations and other Approved or Allowed security functions without any outside entities authenticated to the module." Please provide further clarification. Can this role be assumed only after the Crypto Officer has been authenticated or can this role also be assumed on powerup without authentication of the CO role?	
61	NSA	TWG	4.3.2	E	Need “the” in “The strength of **the** authentication mechanism shall be described”.	
62	NSA	TWG	4.3.3.2	T	How does the statement “The module shall support an approved authentication technique to verify the validity of software/firmware that may be loaded” differ from the previous statement “The Software/firmware load test specified in section 4.9.2 shall be performed before the loaded code is executed”.	
63	NSS Project	Wan-Teh Chang	Section 4.3.2, page 23.	Editorial	This section mentions the “strength of authentication requirements of this section”, but such requirements are not found in this section. (They are in FIPS 140-2.)	
64	NSS Project	Wan-Teh Chang	Section 4.3.2, page 23.	Editorial	This section mentions the “strength of authentication requirements of this section”, but such requirements are not found in this section. (They are in FIPS 140-2.)	
65	Oberthur Technologies	Clement Capel & Christophe Goyet	§4.3.3.2, Security level 2, 3 and 4, page 27	T	§4.3.3.2, Security level 3 and 4, page 27, it is required to perform a digital signature on all software and firmware. This is not compatible with performance requirements of portable devices like smart cards. Indeed, a digital signature is a costly computation which could	

					take several seconds to perform on a complete code and most of the time the highest bound for smart card imposed by ISO/IEC 7816-3 is around some hundreds of milliseconds. This is even less when the smart card is just “waived” by a physical access control reader like the PIV card to complete a SP800-116 access control protocol. Our recommendation would be to make this test “on demand” i.e. to have the module offer a command to run that test when requested by any un-authenitcated operator, at least when the module offers other type of protections to prevent physical attacks that could result in change in the module executable code. For instance when the module achieves physical security level 3 or 4.	
66	Oberthur Technologies	Clement Capel & Christophe Goyet	§4.3.3.2, Security level 2, 3 and 4, page 27	T	In §4.3.3.2, Security level 3 and 4, page 27, the module is required to perform a digital signature on all software and firmware. We believe code in ROM should be excluded from this requirement as code in ROM is by nature much more secure than code in EEPROM. This is also what CC certification recommends. We view performing a check on the ROM code when the program to run that test isin the same ROM code as of little value, especially if the modules has a high level of physical protection as is the case for smart cards. If it were possible to perform such an attack (and it is not the case) then it would be possible to modify the ROM code in order to bypass the check, so the real benefit of that test would be offset by the additional cost in terms of performances, especially for portable devices like smart cards.	

67	OpenSSL Software Foundation	Steve Marquess	4.3.2	T	"If the operating system implements the authentication mechanism, then the authentication mechanism shall meet the requirements of this section." Does the operating system authentication mechanism have to come from a validated cryptographic module? This is unclear. The wording should be changed to make this clear.	
68	OpenSSL Software Foundation	Steve Marquess	4.3.2	T	Currently purchasers of purported validated products are generally unable to confirm that the product as delivered from the vendor does indeed utilize a validated cryptographic module. Since the claim of validated status is often a major factor in procurement decisions a mechanism to enable the end-user to compare the cryptographic module they are using to the one tested by the testing laboratory is necessary to prevent the accidental or deliberate misrepresentation of products by vendors. A service to support this should be added into the list of required services.	
69	Oracle	Matt Ball	4.3.1, second paragraph, second sentence	E	This appears to be a requirement on the operator of the cryptographic module instead of the cryptographic module itself. Consider rewording as follows: "If the cryptographic module supports a User Role, then the cryptographic module shall require that the operator assume the User Role when performing general security services, ..." (comment: is the term 'general security service' sufficiently well defined for this requirement? Maybe this requirement should be dropped, due to vagueness)	
70	Oracle	Matt Ball	4.3.1, third paragraph	E	It is unclear whether the 'Trusted Role' is actually a role in the conventional sense or rather a mode. Consider changing the term "Trusted Role" to "Trusted State". Another possibility would be to keep the concept of a Role, and maybe use the term "Internal Trusted Role". Here's a possible rewording: "A cryptographic module may support an Internal Trusted Role. The Internal Trusted	

					Role is a role performed internally by the cryptographic module without control input of an external operator. With the Internal Trusted Role, the cryptographic module may perform cryptographic operations and other Approved security functions without any outside entities authenticated to the module. The operation of the Internal Trusted Role shall be configured by the Crypto Officer."	
71	Oracle	Matt Ball	4.3.2, 4th paragraph, last sentence	T	The requirement for a cryptographic module to re-authenticate after being rebooted or power-cycled does not have any clear correlation to meaningful security. Some devices, like RFID chips, receive power only for a short time, but are still able to securely cache the session state in between receiving power. Also, with devices that enter low-power standby, there may not be any power applied at all, but the session state can be securely stored and be fully restored when power is reapplied. Consider removing the requirement to reauthenticate on reboots or power-cycles. Maybe replace it with the following allowance: "If a cryptographic module is able to accurately maintain its state when power is removed (e.g., by storing SSPs in non-volatile storage), then the cryptographic module may resume its previous state when power is reapplied, including any previously active authentication or Trusted Channels"	
72	Oracle	Matt Ball	4.3.2, third bullet (top of page 24)	E	It is unclear whether the requirement to obscure the feedback of authentication information applies to the cryptographic module or an input device that is external to the cryptographic module. This should be clarified. Here's a possible clarification: "If the cryptographic module includes a method for entering authentication data from within the cryptographic boundary, then the cryptographic module shall not provide a visible display of the authentication data that the operator enters, but may provide non-significant characters instead (e.g., dots	

					instead of characters). If the cryptographic module allows an external device for providing authentication data, then this device should not provide a visible display of authentication data." (of course, this is a big rat's nest because ideally you want to use the word 'shall' instead of 'should' for external devices, but that's outside the scope of this standard...)	
73	Oracle	Matt Ball	4.3.2, 4th bullet (2nd from top on page 24)	T	Unclear how to enforce or test this requirement. Maybe try some concrete requirements. Example: "While receiving authentication data, the cryptographic module shall not provide feedback based on partial validation of the authentication data (e.g., timing differences based on whether the operator entered a correct or incorrect authentication character). The cryptographic module shall only start the validation of the authentication data after receiving all of the authentication data." Any other ideas of specific testable ways to not weaken authentication data?	
74	Oracle	Matt Ball	4.3.2, first sentence after the bullet list	E	Consider rewording in the active voice: "Document (see Appendix B) shall describe the strength of the authentication mechanism."	
75	Oracle	Matt Ball	4.3.3.1, second bullet	T	It is unclear how the requirement to have two independent actions for bypass meaningfully contributes to the security of the cryptographic module. Why two? Ultimately, this does not provide a meaningful increase in security because there is one logic gate that performs the actual bypass, regardless of the number of inputs that feed into this gate. If this gate fails, then a single point of failure caused the module to inadvertently enter bypass. In my mind, this requirement ventures too far into implementation details and is not meaningfully contributing to tangible security. I recommend it be removed.	

76	Orion	MS	Section 4.3.1, first sentence of next to last paragraph	E/T	"An Authorized role **shall** perform all callable services utilizing Approved or allowed security functions or Approved or Allowed key establishment mechanisms *or where the security of the module is affected*. The italicized text seems awkward. Also, the way the text is now written one could use an Approved security function with a non-Approved key establishment mechanism. Change text to say "Where the security of the module is affected, an Authorized role **shall** utilize only Approved or Allowed security functions and key establishment mechanisms".	
77	Orion	MS	Section 4.3.1, last sentence	T	"Documentation **shall** specify all authorized roles supported by the cryptographic module." I think it would be better to require that all roles supported by the module be specified; not just the authorized ones. Change "all authorized roles" to "all roles".	
78	Orion	MS	Section 4.3.2, first paragraph after Identity-Based Authentication	T	"Except for the Trusted Role(s) and Trusted Channel establishment, services … The Trusted Channel establishment should also require operator authentication before any services are used. It should not be an exception. Remove "and Trusted Channel establishment".	
79	Orion	MS	Section 4.3.2, Text between second and third bullet	T	This text permitting the operating system (rather than the module) to perform authentication at L2 seems to contradict the first part of bullet 2. Modify bullet 2 to state: "The Approved Authentication mechanism **shall** not rely on documented procedural controls…" Then follow with the text: "For a software cryptographic module at Security Level 2, …".	

80	Orion	MS	Section 4.3.2, Security Level 2	T	This requirement contradicts Table 1 which allows *either* role or identity based authentication at Level 2. Clarify	.
81	Defense Manpower Data Center (DMDC)	CTIS	4.3.2 para 7	E,G	Requirements to specify minimum authentication strength for numeric PIN FIPS 140-2 explicitly specifies the minimum authentication strength for numeric PIN at 1 in a 1,000,000. FIPS 140-3 has removed this specification of authentication strength. This leaves the minimum requirement up for interpretation and could allow for an inefficient PIN authentication strength. Also, the authentication strength for numeric PIN should increase to 1 in a 10,000,000 to ensure at least 7 digits of strength. Require minimum authentication strength for numeric PIN	
82	Defense Manpower Data Center (DMDC)	CTIS	4.3.3.2, page 27	T	The requirement to perform a digital signature on all software and firmware is not compatible with performance requirements of hundreds of milliseconds for the DoD Common Access Card (CAC). DoD recommends as optional for smartcard.	
83	RSA Security LLC	Kathy Kriese and Peter Robinson	4.3.2 Page 24, after the first two bullet points on the page	E	"The strength of authentication mechanism shall be described (see Appendix B.)". This seems to be an incorrect reference since Appendix B states what should be in a Security Policy.	

84	SPYRUS, Inc.	WSM	4.3.2, para 4	T	First sentence states “Except for the Trusted Role(s) and Trusted Channel establishment, services using Approved or Allowed security functions shall not be available to an operator until the operator’s authentication is completed successfully.” Suggested replacement: “Except for the Trusted Role(s), **RBG services** and Trusted Channel establishment, services using Approved or Allowed security functions shall not be available to an operator until the operator’s authentication is completed successfully.” Many external applications require a service for unauthenticated approved or allowed random number generation.	
85	SPYRUS, Inc.	WSM	4.3.2, audit	G	Under the description of audit for a trusted channel. It is unclear what the “target” of a trusted channel is. Is it a service, data structure or could it be the module as a whole? Also the term “initiator” is ambiguous. Is it the external platform address, or the role or identity of the user? If there is no user role for the device, is it the identity of the current logged-on agent? Define the term “target” and “initiator” to cover relevant contexts.	
86	SPYRUS, Inc.	WSM	4.3.2, para 6	T	There is no explicit definition for “Default authentication data” or firm limit on number of uses. “replaced upon first-time authentication” is too weak a requirement. The description does not effectively preclude the use of “default authentication data” more than once or forever.	

87	Thales e-Security		4.3.2	T	In some scenarios Crypto Modules may be managed remotely via an intermediate Crypto Module (e.g. an operator authenticates to a local Crypto Module and then remotely manages a remote Crypto Module through the modules' shared secure channel). Guidance should be provided on the strength of mechanisms required when relying on existing inter-module authentication mechanisms in this scenario, and how this relates to the requirement for two-factor authentication.	
88	Thales e-Security		4.3.3.1, 4.9.2.5	T	For safety of life (i.e. comms availability) reasons some security devices initialise in bypass mode and therefore cannot meet the requirements of section 4.3.3.1 which assumes that the module has initialised in secure mode. For these devices, the user has to authenticate to enter secure mode and indications are provided that the user is in secure mode. This is not detrimental to secure operation and therefore should not be precluded by the standard.	
89	Thales e-Security		4.3.3.2	T	Section 4.3.3.2 states that "*The Software/Firmware Load Test … shall be performed before the loaded code is executed*." However the conditional tests specified in sec. 4.9.2 will normally occur within the software/firmware and therefore the code must be executed to perform these tests. We believe this statement either assumes that verification is performed by other software e.g. bootstrap or a previous version of the code. Clarification is required.	
90	NIST	Elaine barker	4.3.2		The module **shall** implement an Approved authentication mechanism as specified in Annex E. Annex E has nothing listed. Also, there is no annex for an allowed	

					authentication mechanism. So, there is a big hole.	
91	NIST	Elaine barker	4.3.3		Replace: *Approved Security Function*: Perform at least one Approved security function used in an Approved mode of operation, as specified in Section 4.1. With *Cryptographic Service using an Approved Security Function*: Perform at least one Approved security function or SSP management technique used in an Approved mode of operation, as specified in Section 4.1.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	Apple, Inc.	Jon Callas	4.4	T	The requirement: The software or firmware components of a cryptographic module **shall** only include code that is in executable form (e.g. no source code, object code or just-in-time compiled code). is somewhat peculiar. I disagree with, but at least understand it implicitly disallowing software where the executable code and source code are the same. It would be possible, for example, to have a self-test with Approved digital signatures that would provide a level of integrity as good as binary-only executable code. A module's creator might provide its source code outside of the module itself, which seems to violate the spirit of the requirement, if the requirement is to have the source of a module be unavailable. Similarly, some languages (Java) are easily decompiled, or typically run with their own virtual machine including a JIT compiler for speed. The requirement seems odd to imply either that Java can't be used or that Java can be used so long as the JRE has no JIT compiler. Similarly, this applies to some other quasi-dynamic languages like C#. Perhaps more extremely, there are some systems that dynamically cross-compile or run an emulated CPU on another. For example, Apple's Rosetta system dynamically compiles PowerPC binaries into Intel binaries. While we have no plans to use Rosetta for a module (and are in fact phasing it out in the long run), it is a peculiar requirement.	

					Thus, I must ask what the real requirement is? I hope it is not a statement that NIST believes that modules that are open source can never reach level 2. I also hope that it is not a statement that a level 2 module can never be written in a language like Java or C#, which appears to be a consequence of this requirement.	
2.	Apple, Inc.	Jon Callas	4.4	T	The requirement: The SFMI, HFMI or HSMI **shall not** provide a service to allow the operator to examine the executable code. is also peculiar. While it indeed seems daft to provide a decompiler as part of a cryptographic module, decompilers are a consequence of having to have a module that is created for a CPU, as opposed to implemented in hardware. In some operating systems (e.g. Windows) development tools are extra-cost add-ons. In others (e.g. Mac OS X) development tools are provided with the operating system but not installed by default. In still others, (e.g. Linux) development tools are part of the standard installation. What does this mean for software modules on standard operating systems? That a level 2 module requires removal of development tools? If a level 2 system were digitally signed and verified from some secure root, what would be the harm in letting the operator view the executable code? Similarly, if a system has its source code available, visible executable code is a	

					consequence of having published source. Nothing is said about source code, but one has to wonder what it means for source code. NIST seems to be saying that Kerckhoff's principle (that a system should be secure, when only the cryptographic keys are secrets) is false. Please strike or modify this requirement. Obviously, a module should not allow an operator to view all of the keys in the module. But the operator should be able to view all of the code, and perhaps some of the keys. If a module meets the subsequent requirement (A cryptographic mechanism only using an Approved *digital signature*….), then this requirement, as well as the previous one, is superfluous if not actively harmful.	
3.	atsec	Fiona Pattinson	4.4 1st bullet	E	What is "modification installation" The meaning of this requirement is unclear. Rephrase the text to clarify the intent of the standard.	
4.	atsec	Peter Kim	4.4 1st, 2nd, and 3rd bullets	T	An Approved integrity technique includes a non-keyed hash, such as SHA-256. This is a reduction of security from FIPS 140-2's current requirement for all software modules to use an Approved Authentication Technique. By removing the need for a secret key or signature, the software modules at Level 1 are further made vulnerable to modification. The second bullet implies an authentication code or signature *may* be used, but it does not require it. No change if this was intentional. Otherwise, reword to use "Approved data authentication	

					technique” instead of “Approved integrity technique”.	
5.	atsec	Peter Kim	4.4 Security Level 2	G	At Level 1, the module can perform its own integrity test or have another validated module perform it. For Level 2, the Operating system may perform it, but there is no explicit validation requirement for the security functions used by the operating system to perform the test. Please clarify the intent.	
6.	Cisco		4.4	T	The requirements for Security Level 2 state: "The software or firmware components of a cryptographic module shall only include code that is in executable form (e.g. no source code, object code or just-in-time compiled code)." Depending on interpretation, this statement could or could not include interpreted software elements (such as, TCL scripts). A Software Module or Hybrid Module could include interpreted software components (e.g., TCL scripts, Java) within the cryptographic boundary, although they do not affect the security of the cryptographic module¹s security relevant elements. Whether this is allowed or forbidden from being within the cryptographic module should be made clear. Recommendation: Allow interpretive software elements that do not affect the security of the cryptographic module¹s security relevant elements.	

7.	CSEC	Jean Campbell	4.4.	T	Page 27 "The Approved *digital signature* or *keyed message authentication code* may be performed by the operating system." Why is this deviation from level 1?	
8.	CSEC	Jean Campbell	4.4	G	Page 27 "The private signing key **shall** reside outside the module. " Shouldn't this requirement be in 4.10.4?	
9.	CSEC	Jan Rupar	4.4 Software/ Firmware Security, Security Level 2	T	*"The software or firmware components of a cryptographic module **shall** only include code that is in executable form (e.g. no source code, object code or just-in-time compiled code)."* In addition to being in executable format, code should be stripped of debugging symbols, as reverse-engineering code with debugging symbols is almost as easy as reading source code. Change sentence to *"The software or firmware components of a cryptographic module **shall** only include code that is in **stripped** executable form (e.g. no source code, object code**, debugging symbols** or just-in-time compiled code)."*	
10.	JCMVP		Draft Revised 4.4 Security Level 2, bullet 3 and Security Levels 3 and 4 bullet 1	E	In the following sentence: "The Approved digital signature or keyed message authentication code that shall be applied to the software or firmware shall consist of…", the first "shall" is redundant. Please remove "that shall be" from the sentence.	

11.	CMVP	Kim Schaffer	4. 4th paragraph	G	There are some requirements for security policy and documentation that may require shall statements. Appendices may not be allowed to contain requirement statements.	
12.	CMVP	Kim Schaffer	4.4 Level 1 first bullet	T	Please expand modification installation, I do not understand what this is.	
13.	CMVP	Kim Schaffer	4.4 Level 2, first bullet	T	This is unclear to me. Are MS Access, Visual Basic, windows scripts, JRE and other interpreter based methods allowed?	
14.	CMVP	Kim Schaffer	4.4 Level 2, first bullet	T	This is unclear to me. Are you asking the labs to review for the presence of source code or object code?	
15.	Cryptsoft	Tim Hudson	4.4	E	"without modification installation (Section 4.10.6)." Grammar. Suggested resolution: delete "installation".	
16.	Cryptsoft	Tim Hudson	4.4	T	"(e.g. no source code, object code or just-in-time compiled code)." Object code is executable. JIT is an optimization technique and not a 'code format'. Suggested resolution: replace above with: "(e.g. no source code, or otherwise interpreted or translated code)"	

17.	Cryptsoft	Tim Hudson	4.4	T	"The Approved digital signature or keyed message authentication code may be performed by the operating system." Is it allowed for a SW-L2 module to use an operating system which uses approved cryptographic algorithms that are **not** provided by a validated cryptographic module? If not then the wording of this section needs to be changed to preclude this.	
18.	Cryptsoft	Tim Hudson	4.4	E	"without modification installation (Section 4.10.6)." Grammar. Suggested resolution: delete "installation".	
19.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 1, Bullet 6	E	Since any non-excluded change in the cryptographic module must be covered by a FIPS 140 validation, the statement "A complete replacement shall constitute a new module which would require its own validation as a whole" should be removed. Suggest removing statement "A complete replacement shall constitute a new module which would require its own validation as a whole."	
20.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 2, Bullet 3	E	What is meant by the public verification key or keyed message authentication key still not considered a CSP? Suggest rewriting the statement as "The keyed message authentication key is not considered a CSP if it resides within the module code."	
21.	IBM	Hugo Krawczyk	**4.4** Software/Firmware Security		Is symmetric authentication allowed as an alternative to digital signatures for Software/Firmware validation in Levels 3 and 4? More specifically, would symmetric authentication be allowed if each device has a dedicated symmetric key not shared with other devices (but only with the vendor certifying the code)?	

					We do see a good reason to disallow a scenario where a single symmetric key is shared among multiple devices (in which case the compromise of a single device would compromise all other devices), but we do not see a reason to disallow the case where different devices contain different (and independent) keys known only to the certifying vendor.	
22.	IBM	Hugo Krawczyk	**4.4** Software/Firmware Security		Section 4.4 does not seem to clearly settle this question. It does explicitly refer to the use of a "keyed message authentication code" for level 2 but this is dropped in the specification for level 3 and 4 where only the use of a digital signature is mentioned. We suggest that the option of using a "keyed message authentication code" is added to levels 3/4 under the restriction that a per-device symmetric key is used. We note that we do have applications scenarios (and customer requirements) to support symmetric key authentication.	
23.	IBM Research, Zurich	Visegrady, Tamas	**4.4**		The explicit requirement for a keyed MAC (Level 2,3) or digital signature-based integrity check (Level 4) on software contained within the module is redundant. An _unkeyed_ cryptographically strong integrity test would provide the same assurance level with less overhead. Assuming the module controls--and authenticates, as of section 4.3.3.2--software load into internal trusted storage, one only needs to protect internal code storage from _accidental_ modification, such as hardware failure. A simpler, unkeyed checksum or cryptographic hash function could provide sufficient protection against failure, without requiring an additional integrity key or public-key operations. If the internal integrity check uses a fixed persistent key, which is indeed allowed based on the wording of sections	

					4.9.1.1, 4.9, and 4.8, no actual value is gained from a keyed internal integrity test. We obviously do not question strong integrity checks on software loaded externally.	
24.	IBM Research, Zurich	Visegrady, Tamas	**4.4**		To allow software-assurance checking, we propose to extend the wording in Section 4.4, replacing "operating system" with "underlying loader software". In systems with multiple levels of applications, such as virtualized servers, there are potentially multiple similar hierarchical software levels.	
25.	IBM Research, Zurich	Visegrady, Tamas	**4.4, Software/firmware security**		**Lack of access to executable code:** An explicit mention of allowing firmware to be stored in cleartext within modules would be reasonable, considering that Level 2 requirements specifically prohibit display of executable code (as a regular module service). Along the same lines, it would be reasonable to explicitly mention that firmware updates need not be encrypted, only authenticated. Since modules will generally store their executable code in persistent internal storage, in executable--therefore, in clear or lightly obfuscated--form, one should assume firmware may be obtained from a module even after tamper. Explicitly mentioning that firmware should only be protected by regular module services, and may survive tamper events in clear form, would clarify the section. We perceive firmware encryption a useful feature, but contributing no real security, as firmware could be obtained at the cost of one destroyed module, usually. Explicit mention of _not_ requiring encryption would silence some reservations about transporting	

					firmware without encryption.	
26.	InfoGard		Section 4.4	T	Software integrity checks: Historically, the software/firmware test during power up was there to protect against inadvertent modification of memory or the binary image. The explicit requirement for a keyed MAC (Levels 2 and 3) or digital signature-based integrity check (Level 4) on software contained within the module implies that the fundamental requirement, and threat model, has changed. However, the recommended requirement may not necessarily provide adequate protection since the key providing the integrity test is also stored within the module. Suggest allowing a 32 bit EDC for firmware integrity checks.	
27.	InfoGard		Section 4.4, Level 1, Bullet 1	E	Please define the phrase “modification installation”. Clarify how this bullet is to be evaluated. Can an example be provided of the issue that led to this statement? Suggest adding “during” to the sentence as follows: *“All software and firmware shall be in a form that satisfies the requirements of this standard without modification during installation (Section 4.10.6).”*	
28.	InfoGard		Section 4.4, Level 2, Bullet 1	G	“The software or firmware components of a cryptographic module shall only include code that is in executable form (e.g. no source code, object code or just-in-time compiled code).” This potentially eliminates all Levels 2 - 4 hardware appliances running web servers that use JavaScript unless the vendor is able to	

					exclude this portion of the code.	
29.	InfoGard		Section 4.4, Level 2, Bullet 3, 2nd Sentence	E	The sentence is fragmented, making it difficult to understand the requirement. Reword the text.	
30.	InfoGard		Section 4.4, Levels 3 & 4, Bullet 1, 2nd Sentence	E	The sentence is fragmented, making it difficult to understand the requirement. Reword the text.	
31.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Section 4.4, Security Level 2	T	"The SFMI, HFMI or HSMI shall not provide a service to allow the operator to examine the executable code." In the case of a software module, it is unclear what "executable code" refers to here – is it the stored executable code on disk (or other media), or is it the in-memory image of a given instance that is executing? More generally, it is unclear what the requirement hopes to achieve. While the SFMI itself may not provide such a service (e.g. the Windows crypto modules do not provide any such APIs), an operator in a modifiable operational environment can examine the executable code of a software module using basic OS facilities. For instance, the executable code of the Windows software modules is widely available, and authorized users can use software debuggers to examine the in-memory image of any executing instance.	

32.	Motorola	Ashot Andreasyan	4.4, Security Level 1, 3rd bullet	G	Please clarify the requirements for the error state entered when the integrity test fails.	
33.	NSA	TWG	4.4	T	Under Security Level 2, we have the statement "The SFMI, HFMI or HSMI shall not provide a service to allow the operator to examine the executable code". What if the device is in maintenance mode? (section 4.5.1)	
34.	NSA	TWG	4.4	T	Security Level 2 states that the public verification key or keyed message authentication key may reside within the module code. It doesn't say anything about where the private signing key shall reside (as it does for security levels 3 and 4).	
35.	NSS Project	Wan-Teh Chang	Section 4.4, page 26.	Technical	"The software or firmware components of a cryptographic module shall only include code that is in executable form (e.g. no source code, object code or just-in-time compiled code). Please clarify what the "no source code" requirement means to an open-source software module, whose source code is available elsewhere, if not included in the module. Please define "object code". For example, on Unix, does "object code" mean a **.o** object file, a **.a** archive library, or a **.so** shared library?	
36.	NSS Project	Wan-Teh Chang	Section 4.4, Last paragraph of page 26.	General	"The Approved digital signature or keyed message authentication code that shall be applied to the software or firmware shall consist of the verification of a digital signature or keyed message authentication code which was used to originally sign the code (by the vendor) using an Approved digital signature algorithm or Approved keyed message authentication code."	

					Please clarify how the “sign the code (by the **vendor)**” requirement interacts with FIPS 140-2 Implementation Guidance G.5 “Maintaining validation compliance of software or firmware cryptographic modules”, which allows a **user** to recompile a Level 2 module. Can the user sign the code?	
37.	OpenSSL Software Foundation	Steve Marquess	4.4	T	“(e.g. no source code, object code or just-in-time compiled code).” This does not make sense. If the intent is that “source” is excluded from Level 2 then just “source” should be listed.	
38.	Oracle Solaris Security	Darren Moffat	4.4	T	The implication of the “no source code” statement for Level 2 implies that for Level 1 this is allowed, and thus it is possible to validate an open source software implementation of a cryptographic module. Is this the intent ?	
39.	Oracle Solaris Security	Darren Moffat	4.4	T	The implication of “no … just-in-time compiled code” means it would not be possible for any Java implementation to achieve Level 2. This is an unacceptable restriction, particularly given the desire to use high level languages for the software module implementation. Almost all Java runtime's provide some form of just-in-time code compilation/recompilation. The same is true of other modern languages such as Python.	
40.	Oracle Solaris Security	Darren Moffat	4.4	T	Level 2: How do general purpose tools such as the UNIX nm(1) elfdump(1) and dis(1) tools that allow examining of executable code fit with this ? Are they regarded not to be part of the SFMI ?	
41.	Oracle Solaris Security	Darren Moffat	4.4 / 4.9	T	Level 2: In the case of the cryptographic module consisting of multiple operating system binaries each of which provides one or more approved cryptographic algorithms and where some of the algorithms may be optionally installed does the verification failure of any one (optional but approved) algorithm binary signature require the whole	

					cryptographic module to be in the error state or is it acceptable for just that optional algorithm to be disabled and the module not offer it? For example if the evaluated cryptographic module consists of multiple loadable kernel modules in a UNIX system say aes, des, rsa, dsa and one of them fails verification but the others pass can the module continue to provide services in an approved mode but not provide the functionality provided by the kernel module that failed verification ? Section 4.9 seems to imply that operation without the optional components is acceptable.	
42.	Oracle Security Evaluations	Shaun Lee	4.4, Security Level 1, final bullet	T	"Any replacements or modifications to the software or firmware components of the module other than …" (11)The statement "A complete replacement shall constitute a new module which would require its own validation as a whole." Implies that vendor assertion of modules which have been re-compiled without change in source will no longer be allowed. Is this the intention?– if not clarification will be required. (12)Is it the intent of this section that a software module on a modifiable environment will be required to implement the Software/Firmware Load Test if the modifications are part of an externally applied patching mechanism and no other requirement for the test to be implemented applies?	
43.	Orion	MS	Section 4.4, Security Level 1, bullet 1	E/T	"All software and firmware **shall** be in a form that satisfies the requirements of the standard without modification installation (Section 4.10.6)." It is not clear what "modification installation" means. Is a word (perhaps "after") missing between "modification" and "installation"?	

					However, this requirement would contradict the loading of new approved software. Section 4.10.6 doesn't specifically discuss modification. Clarify. I think modification of software with other Approved software should be allowed after the software/firmware load test.	
44.	Orion	MS	Section 4.4, Security Level 2, first sentence	E	This sentence includes all the Level 1 requirements in Level 2. Level 1 requires an approved integrity technique. One might think that both the Approved integrity technique and the digital signature were required. Clarify that the digital signature can be used as the approved integrity technique required at Level 1.	
45.	Orion	MS	Section 4.4, Security Level 2, bullet 3, sentence 2	T	This long sentence seems to imply that a digital signature is required on another digital signature used by the vendor. I think only one digital signature is necessary and two would be excessive. Clarify whether one or two digital signatures are needed here. If two are required, make the purpose of each clear.	
46.	Orion	MS	Section 4.4, Security Levels 3 and 4, last sentence	T	"The public verification key may reside within the module code (if so, the key is not considered a CSP)". This sentence seems to imply that sometimes public keys are considered CSPs. I think that public keys should always be considered PSPs whether inside our outside of the module code. Change the sentence to just say: "The public verification key may reside within the module code."	

47.	RSA Security LLC	Kathy Kriese and Peter Robinson	Page 26, Section 4.4, first bullet point	T	Does this requirement preclude the privately linked library mechanism from obtaining Level 2 validation?	
48.	RSA Security LLC	Kathy Kriese and Peter Robinson	Pages 26/27 section 4.4, Security Level 1	T	For Level 2 it says, "The public verification key or keyed message authentication key may reside within the module code (if so, the key is still not considered a CSP)." This should apply to Level 1 as well.	
49.	SanDisk	Boris Dolgunov	**4.9.1.1 & 4.4**	G	Pre-Operational Software/Firmware Integrity Test mandatory requires “integrity technique as specified in Section 4.4”. Section 4.4 mandatory requires usage Approved digital signature for security levels 3 and 4 and does not allow keyed message authentication code. The security of message authentication functions is not lower than of digital signature functions while they require much less computational power than digital signature functions and therefore can be executed more frequently during run time. Also message authentication function can use different unique key in every device and therefore disable possibility of device cloning. The digital signature functions provide good solution for code distribution and uploading into secure boundary while message authentication functions fit better for the firmware or software code verification inside secure boundary. I suggest allowing message authentication function Pre-Operational Software/Firmware Integrity Test also for level 3 and 4.	
50.	Smart Card Alliance		4.4, paragraphs 4, 12, 15 and Section 2.1	T	**4.4 Software/Firmware Security states that "**a cryptographic mechanism using an *Approved integrity technique* **shall** be applied to all software and firmware components within the module’s defined cryptographic	

					boundary" The glossary (section 2.1) defines *Approved integrity technique* as "Approved hash, message authentication code or a digital signature algorithm." The approved integrity techniques as listed in the glossary -- namely "Approved hash, message authentication code or a digital signature algorithm" -- are not suitable for smart card architectures and will lead to speed performance issues. Instead, a CRC16, as allowed by FIPS 140-2 standards, matches smart card architectures and should be listed as *Approved integrity technique*.	
51.	SPYRUS, Inc.	WSM	4.4. SECURITY LEVEL 1, bullet 1	G	What is the definition for "modification installation"? The reference to 4.10.6 did not clarify this. Define "modification installation".	
52.	Thales e-Security		4.4 Software/Firmware Security, Security Level 2, 1st bullet point	T	"*The software or firmware … shall only include code that is in executable form (e.g. no source code, object code* …". This definition conflicts with the glossary of terms which states "*a form of code in which the software or firmware is managed and controlled completely by the operational environment*." Suggest making the glossary definition canonical. Too strict an interpretation of the bullet in 4.4 would appear to prohibit use of any kind of high level interpreted code system and does not in any case intuitively add to the system security: a Java interpreter with separate Java class files would presumably be prohibited but an embedded Java interpreter with bundled class files and identified entry points must be allowed, even though the resulting operation is identical.	

53.	Thales e-Security		4.4	T	Section 4.3.3.2 provides an integrity mechanism for the secure loading of software/firmware. The requirement to perform further integrity checks using digital signatures at Security Level 3 raises a number of issues. 54. It either requires the software to validate the authenticity of itself or use a bootstrap which may or may not be approved 55. If the signature algorithm is defined within the firmware, self tests must be run on the algorithm before it can be used - but the implementation must be verified as correct before it can be loaded to run the self tests. 56. Some processors and PICs will not be able to perform signatures, especially a low power PIC that might be used to monitor a security envelope. The only opportunity to modify the software/firmware is through the signed software/firmware load function. The requirement to maintain the integrity of the software/firmware once loaded is limited to accidental corruption scenario. This could be met by non-cryptographic mechanisms.	
57.	Thales e-Security		4.4, 4.8.6	T	Verification keys (PSPs) are used to authenticate Software/Firmware/Keys, and these must be preserved through zeroisation to allow units to be updated. Operationally, however, specific examples exist where root keys should be maintained through zeroisation to protect against malicious modification of software or code by loading a rogue verification root key; the standard should not preclude this.	

58.	NIST	Elaine Barker	4.4. SL3 & 4		The private signing key **shall** reside outside the module. The public verification key may reside within the module code (if so, the key is not considered a CSP). Wouldn't the code be signed by a crypto module, in which case, it would be resident in SOME module?	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Fiona Pattinson	All	G	The significance of the use of italic font used throughout the main text is not explained and appears inconsistent. If the use of italics denotes that the definition of the term in section 2.1 is to be used then the convention should be used consistently. For example: many instances of the term “cryptographic module” should be italicized throughout the text. In section 4.5, Security level 2, first bullet: the terms execution, modification and reading are italicized but do not appear in section 2.1 Explain the usage of italic font. Use the convention consistently	
2.	atsec	Fiona Pattinson	4.5 Last para	T	The paragraph discusses an evaluated operating system under a recognized program. However it is unclear what a “recognized program” is, and specifically who must recognize it. The standard needs to provide more detail on who defines a recognized program (to illustrate this: entities that recognize various evaluation programs include NIST US Government Cryptographic module operator Cryptographic module designer Foreign Government Etc) The term “validation authority” as used in 4.5.1 section 2 may be useful Suggested text “If the operational environment includes an evaluated operating system under a recognized program approved by the validation authority,”… An additional Annex may also be appended,	

					or the information could be included in Annex "G"	
3.	atsec	Fiona Pattinson	4.5.1 1st bullet	T	The use of the word "control" in this context is ambiguous as to the intent of the specification. Define what is meant by "control". Is it intended that other modules should not be able to access them, or change them? It is intended that an instance of a module can have control of its own SSPs, but another can also modify them?	
4.	atsec	Fiona Pattinson	4.5.1 2nd bullet	T	The use of the word "uncontrolled" in this context is ambiguous as to the intent of the specification. Define what is meant by "uncontrolled".	
5.	atsec	Fiona Pattinson	4.5.1 SECURITY LEVEL 2 2nd bullet	E	The word "modules" is incorrect Replace ""modules" with "module's" …"be specified in the module's Security Policy."	
6.	atsec	Fiona Pattinson	4.5.1 SECURITY LEVEL 2 3rd sub bullet (auditing)	G	"The audit mechanism shall be capable of auditing the following events" is an ambiguous statement. The term auditing usually implies a process involving a methodical examination and review and presenting the results appropriately. It is not clear if the authors intended that the items in the sub-sub bullet should be recorded	

					or audited? Resolve the issue and amend the statement if necessary.	
7.	atsec	Fiona Pattinson	4.5.1 SECURITY LEVEL 2 4th bullet (auditing)	G	The use of date and time is specified, but no requirement to ensure the accuracy of the date and time used by a module is made. Consider if the accuracy of the date and time, and whether this can be modified is important to the integrity of the audit records. If necessary specify requirements for ensuring that the date and time (clock) cannot be modified, or that changes to the date and time are recorded in the audit records	
8.	atsec	Helmut Kurth	4.5.1 SECURITY LEVEL 2 4th bullet (auditing)	T	It is unclear if the operating system is also required to be capable of auditing access, deletions, and additions of cryptographic data and SSPs when such an activity is performed by the cryptographic module itself. It should be clarified that this requirement applies to the operating system and all storage objects managed by the operating system and not the cryptographic module (which is executed under the operating system control). Include a clarification of this requirement.	
9.	atsec	Helmut Kurth	4.5.1 SECURITY LEVEL 2 4th bullet (auditing)	T	The audit requirement is defined to be satisfied by the operating system, but also states that “the module shall use Approved cryptographic functions to protect the information when external to the module from unauthorized disclosure and modification”. This requirement is unclear. Is the operating system required to use the module to protect all the information in the audit log? Or is the module required to protect audit information it (the module) generates to be included in the audit log? In this case, is it allowed to have audit records generated outside the	

					cryptographic module to be not protected by an Approved cryptographic function and just protected by the access control mechanisms provided by the Operating system? Please clarify the requirement. As far as we understand the requirement, its main purpose is to ensure that cryptographic data and SSPs do not show up in cleartext in the audit log. There is also the problem that it is useful to have an audit log when the module enters an error state (which may be useful event to be added to the list event that the operating system should be able to audit). Since in this case the cryptographic functions of the module can not be used, how can this audit record be protected?	
10.	atsec	Apostol Vassilev	4.5.1 SECURITY LEVEL 1 2nd bullet	T	There is no way to test the stated requirement on the operational environment without examining the design and implementation of the operating system providing the operational environment for the module. In the past this kind of assurance was obtained from references to other security standards for the operating system. In the absence of such, a CST lab is left with the puzzle of how to ensure that the requirement of the second bullet is indeed achievable. In fact, most operating systems have kernel processes and other system processes in kernel or user mode that have enough privilege to mess with any other process, including the processes of the cryptographic module. Therefore, such a formulation is very imprecise and not useful at all. Make the formulation precise to account for the way processes are managed and protected by most/all operating systems. For example, state that the operating system must be configured to prevent other processes with equal or lesser privilege than the lowest privilege process of the module from having uncontrolled access to the modules CSPs.	

					Make references to other security standards that can provide assurance that the Operating System provides effective control over process separation.	
11.	atsec	Apostol Vassilev	4.5.1 SECURITY LEVEL 2	T	These OS requirements can only be tested if the CST lab has access to the source code and design documentation of the operating system. If FIPS 140-3 wants to include them as intrinsic to this standard and require the CST labs to test for them, this would make FIPS 140-3 extremely difficult to perform validations with for the CST labs. It will also substantially increase the cost and time required for each certification, much more than what customers are used to with the current version of the standard. Also, if one Lab manages to gain access to such documentation for the OS, this will not benefit the module developer community at large or the other CST Labs. Therefore, it may potentially distort the validation market and lead to monopolies in it. If such a situation occurs, it will have dire consequences for the standard itself. Remove such explicit requirements for the operating environment and refer to other standards for assurance about these specific classes of security functionality. It is more useful and feasible to produce a Common Criteria FIPS 140-3 Protection Profile for Operating Systems than to define a self-contained set of OS requirements inside this standard that can be tested efficiently by the CST labs.	

					Please note that all main operating systems have already undergone Common Criteria evaluations at EAL 4 or higher, so asking them to adopt a FIPS 140-3 Protection Profile is much less work for the OS vendor and once complete it will benefit all module developers, CST Labs, NIST, and the Federal Government as a whole.	
12.	Cisco		4.5	T	With industry moving to a virtualized environment, FIPS 140-3 should at minimum discuss modules designed for/in a virtualized environment. Any specific requirements associated with such modules should be delineated in the standard. Include a discussion of virtualization in FIPS 140-3	
13.	Cisco		4.5	T	Within the discussion of virtualization, please discuss if there are any differences between how the standard will address HW virtualization and SW virtualization Include a discussion of virtualization in FIPS 140-3	
14.	CSEC	Claudia Popa	4.5.1 , second bullet		"The operational environment shall be configured to prevent processes outside the cryptographic boundary of the cryptographic module from having **uncontrolled** access to the module's CSPs". This requirement prohibits a process outside the crypto boundary to have "uncontrolled" access to the module's CSPs. Can this process access in a **"controlled"** way the CSPs used by a cryptographic module? Or, the requirement is to restrict the access	

					(controlled or uncontrolled) of another process to the module's CSPs?	
15.	CSEC	Claudia Popa	4.5.1	G	Page 29. "In lieu of the following requirements, an operating environment may be used as allowed by the validation authority as specified in Annex G." Appendix G only refers to an Implementation Guidance document that was not provided.	
16.	CSEC	Jean Campbell	4.5		"An operational environment can be non-modifiable (**e.g.** an environment that can not be modified), *limited* (e.g. an environment which allows controlled modification meeting the requirements of Section 4.9.2.3)" Change "e.g." to "i.e.", not an example	
17.	CSEC	Jean Campbell	4.5		Why do we repeat this: "An operational environment can be non-modifiable (e.g. an environment that can not be modified), *limited* (e.g. an environment which allows controlled modification meeting the requirements of Section 4.9.2.3), or *modifiable* (e.g. an environment which allows uncontrolled modifications). "	
18.	CSEC	Jean Campbell	4.5	G	The question refers to 2., limited operational environment. Does the module control the operation of the environment?	

19.	CSEC	Jean Campbell	4.5.1	E	“The identification and authentication mechanism to the operating system **shall** meet the requirements of Section 4.3.2 and be specified in the **modules** Security Policy.” Correct as below: The identification and authentication mechanism to the operating system **shall** meet the requirements of Section 4.3.2 and be specified in the **module’s** Security Policy.	
20.	JCMVP		Draft Revised 4.5.1	E	The subject of 4.5 is “Operational Environment.” The subject of 4.5.1 is “Operating System Requirements.” The requirement for security level 2 is “In addition to the requirements of Security Level 1 for the operating system,…” Operational Environment, Operating System,… there is a discrepancy of the usage of the term. Please describe the terms consistently.	
21.	JCMVP		Draft Revised 4.5.1, Security Level2, Filled bullet1	E	In the paragraph, following wording is used: "unauthorized execution, modification, and reading of SSPs". We suppose that the SSPs themselves are just data and not executable, therefore it is strange to use the word "execution" for SSPs. In relation to the SSP lifecycle, it is better to use, "generation, modification, reading, and zeroization".	
22.	JCMVP		Draft Revised 4.5.1, Security Level2, Filled Bullet3, Open bullet 1	E	The word,"maintenance mode", is used only here. Please add the definition of "maintenance mode" in Section 2.1.	
23.	JCMVP		Draft Revised 4.5.1, Security Level2, Filled Bullet3, Open bullet 3	E	The word, "Administrative Guidance", is used in the paragraph. If "Administrative Guidance" is used in the same meaning of "Administrator Guidance", please replace "Administrative" by "Administrator".	

24.	JCMVP		Draft Revised 4.5.1, Security Level2, P.30, filled bullet, open bullet 2, filled bullet 2	E	We would like to know what is intended by the word, "authentication data management mechanisms".	
25.	NSRI(National Security Research Institute)	Korea CMVP (Jihoon JEONG)	4.5(4th para) pp. 27		#2 : A **'programmable H/W module'** is described as an example of the 'Limited operational environment'. In FIPS 140-2 **'Java virtual machine on a non-modifiable PC Card'** is described as an example of it. **An example of the FIPS 140-2 is more clear and accurate. So, we would like to propose to use the old one.**	
26.	NSRI(National Security Research Institute)	Korea CMVP (Jihoon JEONG)	4.5.1(2nd para) pp. 28		Last bullet : The security requirements of **the Security Level 1 is too weak** as compared to its of FIPS 140-2. (Everything in FIPS 140-2 is removed and all the requirements are rely on the OS.) Do you have any reason for it?	
27.	CMVP	Kim Schaffer	4.5 First paragraph	T	"This section is not applicable for a hardware module." If this section is optional for hardware as stated earlier in the draft standard then this statement should be removed.	
28.	CMVP	Kim Schaffer	4.5	T	Consider making non-modifiable a special version of limited and dropping the two very similar terms. I am not sure limited needs to require the s/f load test?	
29.	CMVP	Kim Schaffer	4.5	T	"If the operational environment is non-modifiable or limited, then the operational environment components that enforce the non-modifiable or limited environment shall be bound to the firmware module and the operating system requirements in Section 4.5.1 do not apply." Consider rewording to: "If the operational environment is non-modifiable or limited, then the operational environment components that enforce the non-modifiable or limited	

					environment may include attributes of the computing platform, cryptographic module or the operating system. If the operational environment is non-modifiable or limited, then requirements in Section 4.5.1 do not apply."	
30.	CMVP	Kim Schaffer	4.5	T	Consider removing "If the operational environment includes an evaluated operating system under a recognized program, the documentation shall specify the evaluation certificates, protection profiles and extensibility as applicable." Unfortunately without a protection profile or similar agreed upon requirements, this does not necessarily provide assurance to the cryptographic module.	
31.	CMVP	Kim Schaffer	4.5 Level 2	T	ACLs to permit control over SSPs is duplicated. If it is meant to be a separated control it should be removed from "cryptographic programs, cryptographic data (e.g., cryptographic audit data), SSPs, and plaintext data."	
32.	Cryptsoft	Tim Hudson	4.5	G	"If the operational environment includes an evaluated operating system under a recognized program, the documentation shall specify the evaluation certificates, protection profiles and extensibility as applicable. " Where are the 'recognized' programs defined? This should be clearly specified and perhaps warrants another Annex? Or is this what is meant to be in Annex G which is currently empty? It appears the term is meant to be "validation authority" and should be changed accordingly to match.	
33.	Cryptsoft	Tim Hudson	4.5.1	T	There are no "validation authority" entries in Annex G.	

34.	Cryptsoft	Tim Hudson	4.5.1	G	Was it the intent of this section to remove the requirement for Common Criteria validation under certain Protection Profiles? There is nothing in Annex G or elsewhere which references Common Criteria.	
35.	Cryptsoft	Tim Hudson	4.5.1	T	"In this case, running processes refer to all processes, cryptographic or not, not owned or initiated by the operating system (i.e., operator-initiated)." This is a good working definition to use to exclude the privileged process which can read/write/execute SSPs – however this definition should encompass **all** the requirements in this section and not just the single bullet point. Suggested resolution: add to the first paragraph under Security Level 2: "All controls shall be enforced by the Operating System and refer to all processes, cryptographic or not, that are not owned or initiated by the operating system (i.e. operator-initiated)".	
36.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 1, Bullet 6	E	Since any non-excluded change in the cryptographic module must be covered by a FIPS 140 validation, the statement "A complete replacement shall constitute a new module which would require its own validation as a whole" should be removed. Suggest removing statement "A complete replacement shall constitute a new module which would require its own validation as a whole."	
37.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 2, Bullet 3	E	What is meant by the public verification key or keyed message authentication key still not considered a CSP? Suggest rewriting the statement as "The keyed message authentication key is not considered a CSP if it resides within the	

					module code.”	
38.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 1, Bullet 6	E	Since any non-excluded change in the cryptographic module must be covered by a FIPS 140 validation, the statement “A complete replacement shall constitute a new module which would require its own validation as a whole” should be removed. Suggest removing statement “A complete replacement shall constitute a new module which would require its own validation as a whole.”	
39.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 2, Bullet 3	E	What is meant by the public verification key or keyed message authentication key still not considered a CSP? Suggest rewriting the statement as “The keyed message authentication key is not considered a CSP if it resides within the module code.”	
40.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 1, Bullet 6	E	Since any non-excluded change in the cryptographic module must be covered by a FIPS 140 validation, the statement “A complete replacement shall constitute a new module which would require its own validation as a whole” should be removed. Suggest removing statement “A complete replacement shall constitute a new module which would require its own validation as a whole.”	
41.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.4 Software/ Firmware Security**, SECURITY LEVEL 2, Bullet 3	E	What is meant by the public verification key or keyed message authentication key still not considered a CSP? Suggest rewriting the statement as “The keyed message authentication key is not considered a CSP if it resides within the module code.”	

42.	EWA-Canada IT Security Evaluation & Test Facility	Dawn Adams	**4.5**, **4.5.1 Operating System Require-ments for Modifiable Operation-al Environ-ment**, SECURITY LEVEL 2, Paragraph 4, Bullet 2	T	Trusted Channel is only required at Security Levels 3 and 4. Software cannot be validated beyond Security Level 2. Suggest removing any audit requirements for Trusted Channel.	
43.	EWA-Canada IT Security Evaluation & Test Facility	Dawn Adams	**4.5**, **4.5.1 Operating System Require-ments for Modifiable Operation-al Environ-ment**, SECURITY LEVEL 2, Paragraph 4, Bullets 2 and 3	T	It may not be possible to define as events the required audit actions. Audit is an operational environment requirement and not a cryptographic module requirement. Suggest removing the following events as auditable actions: "- attempts to provide invalid input for Crypto Office functions, - requests to use authentication data management mechanisms, - the use of a security-relevant Crypto Officer function, - requests to access authentication data associated with the cryptographic module, and - explicit requests to assume a Crypto Officer role."	
44.	InfoGard		Section 4.5	G	Self-checking for software libraries in authenticated environments: The standard mandates that software modules perform integrity checks on themselves, even if this is theoretically impossible (due to the inherent chicken-egg problem). While we agree with the laudable goal of integrity checking code, in many environments one should be able to delegate integrity checking to a component before module startup, with sufficient assurance. As an example, if an operating system loads	

					only signed binaries, it may verify a digital signature on the binary before any code within the binary is invoked. If the component is a validated crypto provider, it repeats the same signature verification, only at a lower assurance level, as the self-verification code runs before it has verified itself. We propose exceptions for systems where the underlying implementation validates module integrity before module code starts executing. Under these circumstances, if the signature verification code passes KATs and receives an independent FIPS 140 algorithm validation, it could offer equivalent security guarantees.	
45.	InfoGard		Section 4.5.1, Level 1, Bullet 1	T	"Each instance of a cryptographic module shall have control over its own SSPs." How is "control" defined? How much control can a software instantiation have over its own data versus dependency on the operating system?	
46.	InfoGard		Section 4.5, Table 2¶	G	Please confirm that a smart card running a general purpose operational environment can be accepted as a modifiable operational environment, provided that the requirements of Section 4.5 are met. If this is so, can software only applets be validated separately (up to Level 2) for use on such a general purpose environment? Would an agency operating a FIPS 140-2 validated platform and an arbitrary combination of applets (FIPS validated where relevant) be within the validation? Finally, if an applet uses cryptographic functions provided by a FIPS 140-2 validated platform, but the applet does not itself implement any crypto functions or store keys, does the addition of the applet require new validation or re-validation? As an example, a PIV applet may be implemented without itself implementing any crypto or storing keys.	

47.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Section 4.5.1, Security Level 1	T	"The operational environment shall be configured to prevent processes outside the cryptographic boundary of the cryptographic module from having uncontrolled access to the module's CSPs." In a modifiable operational environment, software debuggers and other such tools can obtain complete access to all memory contents, including the CSPs of an in-memory module instance. This can happen without the knowledge of the process or (in some cases) the knowledge of the operating system, so it is not possible for the software module to enter a maintenance mode and zeroize its CSPs. Therefore we do not believe software modules can satisfy this requirement. For a software module, this requirement also appears to assume that the cryptographic boundary includes at least one process. The Windows cryptographic modules are general-purpose libraries that can be loaded dynamically by any process, and it is not possible to make any general claims about all such processes. This requirement (when read together with Section 4.1.2 and Appendix B.1 "Cryptographic Module Specification") seems to imply that in such cases, the process would be defined as the cryptographic boundary but everything other than the cryptographic library would be excluded from evaluation. It would be useful to clarify this requirement.	
48.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.5	T	Definition of limited operational environment "is designed to contain only firmware or hardware but allows controlled modifications. This environment may be firmware operating in a programmable computer (e.g., a programmable hardware module) where the loading of additional firmware is controlled through the Software/Firmware Load Test specified in Section 4.9.2.3." and modifiable operational environment "refers to an operating environment that may be	

					reconfigured to add/delete/modify functionality, and/or may include general-purpose operating system capabilities (e.g., use of a computer O/S, configurable smartcard O/S, or programmable software). Operating systems are considered to be modifiable operational environments if software components can be modified by the operator and/or the operator can load and execute software (e.g., a word processor) that was not included as part of the validation of the module." is confusing. By these definitions a limited operational environment cannot delete capabilities once fielded nor increase capabilities. Yet a "controlled modification" could be to remove support of a specific cryptographic algorithm DES or 3DES. Recommend definition changes provided in earlier comments. Rationale: Changes to a limited operational environment module may be the removal or addition of algorithm or security functionality. For example if a cryptographic module is initially fielded with the hardware required to support providing digital signature, but not the software/firmware to provide the feature, software updates should be allowed to provide these security functions in the future, assuming that required testing verifies that the signature process is correctly implemented.	
49.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.5.1	T	For cryptographic modules with limited audit trail capabilities, the requirement to "The following events and their date and time of occurrence shall be recorded by the audit mechanism - all operator read or write accesses to audit data stored in the audit trail" may allow a rouge operator to obscure more sinister activities by attempting multiple audit trail read requests. Rationale: If the audit requirements are intended to help "catch a thief" then allowing the "thief" to cover their trail with trivial	

					activities defeats the intent to “catch the thief”. Other auditable events should be analyzed for their potential to “cover the tracks of a thief”.	
50.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.5.1	T	If the cryptographic module design provides strong software authentication methods why shouldn’t users be allowed to “The operating system shall be configured to prevent operators in the user role (if supported) or members of the users group from modifying cryptographic module software.”? Rationale: Why shouldn’t users be able to apply software updates that employ strong authentication methods? As previously commented, some cryptographic modules will not require a Crypto Officer role since they can be “born with” necessary trust anchors and CSPs.	
51.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.5.1	T	As previously commented users can repeatedly perform auditable actions that will prevent the detection of “suspicious activity by causing the overwriting of audit trail information. As such, the following requirement “The operating system shall be configured to prevent operators in the user role (if supported) or members of the users group from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.” can only be met if audit logs cannot be overwritten. Recommend that this explicit requirement be added to prevent loss of a significant auditable event. Rationale: Without a requirement to prevent audit trail being overwritten, a rogue user could “hid” sinister actions with massively repeating benign auditable actions.	
52.	NSA	TWG	4.5.1	E	2nd bullet, need an apostrophe in “…access to the module’s CSPs”. Need “a” in next bullet “…discretionary access control with **a** robust mechanism…”. Need an apostrophe in	

					"…Section 4.3.2 and be specified in the module's Security Policy".	
53.	NSA	TWG	4.5.1	T	Use the term "maintenance mode" but not defined anywhere (maintenance role is defined in 4.3.1. Should this be defined?	
54.	NSS Project	Wan-Teh Chang	Section 4.5.1, page 29.	Technical	"When not in the maintenance mode, the operating system shall prevent all operators and running processes from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images)." A debugger can attach to a running process and modify the state of the attached process. Does this requirement mean a debugger shall not be able to attach to a running cryptographic process? If so, please say this explicitly in the requirement.	
55.	Oberthur Technologies	Clement Capel & Christophe Goyet	§ 4.2.3, § 4.5.1, § 4.9	T	the standard requires many audit logs (§ 4.2.3, § 4.5.1, § 4.9) to store information on trusted channels and test results. This could require a large amount of memory not available on a smartcard. As new generation smart cards like the FIPS 140-2 Level 3 validated Oberthur ID-One Cosmo v7 cards include defensive mechanisms (reset, killcard ...) in case of abnormal event impacting sensitive assets such an audit can reasonably be considered as useless. In the Common Criteria, the audit requirements are generally regarded as not applicable. We recommend therefore to introduce these audits as optional when active defense mechanisms are already implemented.	
56.	OpenSSL Software Foundation	Steve Marquess	4.5.1	T	"In this case, running processes refer to all processes, cryptographic or not, not owned or initiated by the operating system (i.e., operator-initiated)." This definition should encompass all the	

					requirements in this section and not just the single bullet point.	
57.	Orion	MS	Section 4.5.1, Security Level 2, first bullet, first sentence	E	The text "…discretionary access control with robust mechanism of defining new groups…" needs rewording. Change text to read: "…discretionary access control with a robust mechanism for defining new groups…"	
58.	RSA Security LLC	Kathy Kriese and Peter Robinson	Page 45: Section 4.9.3, Security Levels 1 and 2, first sentence	E	"pre-conditional" should be changed to become "pre-operational".	
59.	NIST	Elaine Barker	4.5		1. A ***non-modifiable operational environment*** is designed to contain only firmware or hardware. This environment may consist of a firmware module operating in a non-programmable computing platform or a hardware module and its computing platform which cannot be modified. 2. A ***limited operational environment*** is designed to contain only firmware or hardware but allows controlled modifications. This environment may be firmware operating in a programmable computer (e.g., a programmable hardware module) where the loading of additional firmware is controlled through the Software/Firmware Load Test specified in Section 4.9.2.3. Hardware is not being discussed in this section, remove it from above text	

60.	NIST	Elaine Barker	4.5 Table 2 – 2nd row		Either include this text (row 2) in the list above the table 2, or include a reference to the table in the text.	
61.	NIST	Elaine Barker	4.5 Table 2 – 3rd row		"non-validated code" was not mentioned above in the text	
62.	NIST	Elaine Barker	4.5 Table 2 – 4th row		Not mentioned in the list/text above the table. Provide a reference to the table in the text? Why are there two rows for modifiable?	
63.	NIST	Elaine Barker	4.5		"Documentation **shall** specify the operational environment for the cryptographic module. If the operational environment is *non-modifiable* or *limited*, the documentation **shall** specify all hardware and firmware components that enforce the *non-modifiable* or *limited* environment. " Since this section does not discuss hardware, maybe this could be removed, so that it becomes "…specify all components…"?	
64.	NIST	Elaine Barker	4.5 SL2		○ Define and enforce the set of roles or the groups and their associated ACLs that have exclusive rights to *read* cryptographic data (e.g., cryptographic audit data), CSPs, and plaintext data. Wouldn't you want to prevent modification of ciphertext data as well?	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	Apple, Inc.	Jon Callas	4.6.1	T	Does the requirement If tamper evident seals are employed, they **shall** be uniquely numbered or independently identifiable (e.g., uniquely numbered evidence tape or uniquely identifiable holographic seals). require that the seals be logged in a manufacturer's database along with the serial number of the device? It seems that without such a correspondence, an attacker could replace the seals undetectably by moving them from one device to another. It's equivalent to having software signed by an untrusted public key.	
2.	atsec	Peter Kim	4.6.1	G	There is a requirement to zeroize when accessing the maintenance interface, which implies entry or exit. Is there a preference? Please clarify whether the module is to protect against even the maintenance operator by zeroizing both upon entry and exit.	
3.	atsec	Peter Kim	4.6.1 Security Level 2, 3rd bullet	T	It is not possible to completely prevent the gathering of information of a module's internal construction or components by direct visual observation *without* a 90 degree baffle of some sort, which has typically only been required at Level 3. Without a 90 degree turn or baffle, vendors turn to using dust filters, specialized fans, or relying on other sorts of visual obstructions to act as baffles, but ineffectively. At best, without a baffle, you can deter observation, which is to say sensitive components' maker and model cannot be identified, but their general location may be. This can be met by the same methods listed	

					above, but may also be met by placing covers over sensitive components to prevent the complete identification of them. The identification of component locations cannot be prevented without a 90 degree baffle. Unless the intent is to force Level 2 devices to employ the baffles currently employed for FIPS 140-2 Level 3 devices, then reword: "If the cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in a manner to deter the gathering of information of the module's internal construction or components by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or components."	
4.	atsec	Peter Kim	4.6.2 Security Level 3	T	The "OR" between the bullets should be an "AND". Otherwise, "hard" is difficult to define and would not necessarily imply it would render the device inoperable if attacked. Replace "OR" with "AND".	
5.	atsec	Peter Kim	4.6.3 and 4.6.4 Security Level 3, 1st bullet	T	The requirement does not specify a metric for test for the hardness. Reword: "The multiple-chip embodiment of the circuitry within the cryptographic module shall be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum, and attempts at removal or penetration of the coating or pottering material to the depth of underlying circuitry will have a high probability of causing serious damage to the module	

6.	brightsight	Lex Schoonen	4.6.5.1 4.6.5.2	T	EFP should include protection against momentary changes in the environment. It should be more clear that such changes need to be protected against, as their potential typically is much higher than that of gradual or continuous changes in environment factors. As an example, inducing faults through very short glitches in the power supply and/or short laser pulses is a well-established attack technique, which has often been demonstrated to be effective even in the presence of explicit countermeasures. Obviously, this remark should also be taken to cover the EFT, if this is used instead of demonstration of EFP. The main reason to make this coverage more explicit is that if there is ambiguity about this aspect, it will lead to differences in the level of protection provided by a level-4 certified product, and will lead to essential differences in testing procedures in different labs.	
7.	Cisco		4.6.1	T	The module opacity requirements present at level 2 do not provide any additional security for the defined attacker and environment for which the module is intended. Move the opacity requirements to level 3.	
8.	CSEC	Jean Campbell	4.6	E	Page 30 “The requirements of this section **shall** be applicable to hardware, firmware and hardware components of hybrid modules.” Correct as below: “The requirements of this section **shall** be applicable to hardware **and** firmware **modules,** and hardware components of hybrid modules.	

9.	CSEC	Jean Campbell	4.6.1	E	Page 32 This comment refers to the third bullet in the 4.6.1. Should all these requirements be defined in section 4.2 and just referred here?	
10.	CSEC	Jean Campbell	4.6.1	G	Page 32 This comment refers to the second bullet in the Security Level 1 section. When dealing with maintenance there are three aspects: • Maintenance role • Maintenance interface • Perform maintenance Could we present all these in a better package?	
11.	CSEC	Jean Campbell	4.6.1	G	Page 32 “The tamper-evident material, coating or tamper-evident enclosure **shall** either be opaque or **translucent** within the visible spectrum.” Not sure what we try to say. The enclosed can be either opaque or **translucent?**	
12.	JCMVP		Draft Revised 4.6.1, Security Level 3,	T	In FIPS 140-2, there is no word, "translucent", and it is addressed in FIPS 140-2 I.G. for only Security Level2. So the requirements of "opacity" should be addressed for cryptographic modules with Security Level 3.	
13.	CMVP	Beverly Trapnell, Kim Schaffer	4.6 Table 3	T	Recommend changing pick-resistant to tamper resistant, allowing for other types of locks to be considered.	
14.	CMVP	Kim Schaffer	4.6	E	Reword, appears to be grammatically incorrect and adds an additional requirement of fault induced attacks. “Security Level 4 adds requirements for the use of strong enclosures with tamper detection and	

					response mechanisms for the entire enclosure as well as either environmental failure protection (EFP) or environmental failure testing (EFT) and protection from fault induced attacks."	
15.	CMVP	Beverly Trapnell, Kim Schaffer	4.6	E	This appears unnecessary as it is addressed in 4.6.1. "Security requirements are specified for a maintenance access interface when a cryptographic module is designed to permit physical access (e.g., by the module vendor or other authorized individuals)."	
16.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.1 2nd bullet	T	Recommend adding active zeroization based on IG guidance and reword to "Whenever zeroization is performed for physical security purposes, active zeroization shall occur within a sufficiently short period of time to prevent the recovery of the sensitive data between the time of detection and the actual zeroization."	
17.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.1 Security level 1, bullet 1	E	The second shall is unnecessary.	
18.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.1 Security level 2, bullet 1	T	This is too specific and does not address many other instances where tamper evidence is required. "Tamper evidence protections shall only be applied between adjoining solid surfaces."	
19.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.3 Level 1	E	If the cryptographic module is contained within an enclosure that may have a door or a removable cover, then all shall be production grade.	
20.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.3 Level 2	T	Delete section shown as it does not support observation deterrence. The module's components shall be contained in a tamper-evident enclosure ~~to deter direct observation or manipulation of module components and~~ to provide evidence of attempts to tamper with or remove module components,	
21.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.4 Level 3	T	The phrase "such that attempts at removal or penetration will have a high probability of causing serious damage to the module (i.e., the module will not function)." should apply to both requirements under Security level 3.	
22.	CMVP	Beverly Trapnell,	4.6.4 Level 4, end of first	E	Please reword to "The tamper detection mechanisms shall respond to attacks such as	

		Kim Schaffer	bullet		cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure, to an extent sufficient for accessing the contents of the module."	
23.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.5.1	T	"The EFP features shall involve electronic circuitry or devices that continuously measure the operating temperature and voltage of a cryptographic module." is not a needed requirement.	
24.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.5.2	T	Add "Temperature shall be monitored internally at the sensitive components and critical devices and not just at the physical boundary of the module."	
25.	CMVP	Beverly Trapnell, Kim Schaffer	4.6.3 Level 4, 1st bullet.	T	Why is a strong enclosure listed as an example of a tamper detection envelope.	
26.	DOMUS		4.6, Last 2 sentences of page 29	E	The last 2 sentences describe that the requirements of this section are applicable for hardware, firmware, and hardware components of hybrid modules. **Proposed change would suggest stating that the requirements of this section are applicable for software, firmware, and hardware components of hybrid modules.**	
27.	DOMUS		4.6, Last 2 sentences of page 29	T	The second last sentence describes that requirements of this section are applicable for hardware, firmware, and hardware components of hybrid modules however there are no requirements specified for physical security of hybrid cryptographic modules. **Add a 4th embodiment to describe the physical security requirements for a hybrid cryptographic module at levels 1 to 4. If physical security requirements for hybrid modules are applicable for Level 1 only then I believe it must be specified in this section**	
28.	DOMUS		4.6.4, Security Level 3, 2nd bullet	T	The requirement states: "the module **shall** be contained within a strong enclosure such that attempts at removal or penetration of the enclosure will have a high probability of causing serious damage to the module (i.e.,	

					the module will not function)" **The requirement does not address tamper evidence in trying to breach the module cover shall cause tamper evidence. Secondly, the requirement states that breach of the cover will cause serious damage to the module causing it to not function. I believe this requirement will make it difficult for any security appliance vendor to meet this requirement for Level 3 because if the tester is able to breach the cover using physical force and the module continues to operate, the module will fail the physical security requirement for this section. I believe some additional description of the type of attack needs to be mentioned ex. That drilling or milling is either allowed in this type of attack or not allowed in this type of attack.**	
29.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.6 Physical Security**, Paragraph 7	T	What is the required protection from fault induced attacks? Recommend providing an example of something protecting against a fault induced attack.	
30.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.6**, **4.6.1 General Physical Security Require-ments**, SECURITY LEVEL 2, Bullet 2	T	Why should tamper evidence protections only be applied between adjoining solid surfaces? Do not believe this needs to be stated. Suggest removing statement "Tamper evidence protection shall only be applied between adjoining solid surfaces."	
31.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.6**, **4.6.1 General Physical Security Require-ments**, SECURITY	T	If a tamper evident seal can be copied, so can its number. Suggest removing the requirement for uniquely numbered or independently identifiable tamper evident seals at Security Levels 3 and 4.	

			LEVEL 3, Bullet 3			
32.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.6**, **4.6.2 Single-Chip Crypto-graphic Modules**, SECURITY LEVEL 4, Bullet 1	T	Could not a single-chip cryptographic module have a removal-resistant enclosure instead of a coating? Suggest specifying a removal-resistant enclosure as an option for single-chip cryptographic modules at Security Level 4.	
33.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.6**, **4.6.5.2 Environ-mental Failure Testing Procedures**, Paragraphs 3, 4 and 5	T	Good specification of environmental failure testing None	
34.	IBM Research, Zurich	Visegrady, Tamas	**G**		The current standard draft can not easily describe modules integrated below the single-chip level. With the advance of technology, one may encounter chip-integrated modules with their own key management, occupying only a part of a general-purpose chip, during the lifetime of the standard. While ``raw'' clearkey engines---such as those included within IBM mainframe processors---may be included within other modules (such as hybrid modules using their services), the standard does not address entire modules with their entire cryptographic boundary integrated within a general-purpose chip. Assuming technology advances during the lifetime of FIPS 140-3, one could consider adding a new category for hardware devices that are standalone parts of a larger, single-chip hardware device.	
35.	IBM Research, Zurich	Visegrady, Tamas			The current standard draft makes it difficult to describe multi-chip modules which are integrated at a microelectronic level, such as stacked within MCM (i.e., multi-chip carriers).	

					We propose a mention for such multiple-chip modules, which may be treated as single-chip modules for physical security purposes, if packaging makes it infeasible to probe within the common carrier. Strict interpretation of Level 4 tamper-response requirements would mandate a discrete tamper matrix around multi-chip structure, while its internal connections could be equivalently--or even better—protected from within the MCM. As a practical example, direct chip-to-chip connections through a single board, such as a 3D-stacked MCM, would need to be physically attacked through the connecting board. Such a stacked MCM would expose only raw(inactive) die surfaces, and board cross-sections to the outside world. These attack surface may be covered by tamper-detection circuitry within the board, exposing no interconnects, only inactive chip sides, to the outside. With slight changes, the Level 4 requirements in sections **4.6.3** and **4.6.4** could accommodate tamper protection implemented between directly attached chips, without an external tamper-response envelope. Vendors would need to convincingly demonstrate that the exposed interfaces--such as external, inactive surfaces of chips--may not by physically attacked with less effort than attacking an exposed mesh. Such directly connected chips, even if instantiated at multiple chips, are closer to a single-chip module.	
36.	InfoGard		Section 4.6	G	Chip-integrated modules: The current standard draft cannot easily describe modules integrated below the single-	

					chip level. While 'raw' clearkey engines, such as those included within mainframe processors, may be included within other modules (such as hybrid modules using their services), the standard does not address entire modules with their entire cryptographic boundary integrated within a general purpose chip. Assuming that technology advances during the lifetime of FIPS 140-3, one could consider adding a new category for hardware devices that are standalone parts of a larger, single-chip hardware device.	
37.	InfoGard		Section 4.6, Page 31, Last Paragraph, Last Sentence	T	"…and protection from fault induced attacks." There is a wide range of fault induced attacks from heat, cold, optical, UV, power spikes, laser, x-ray, radiation, to electromagnetic and beyond. They are continually changing and evolving. Some have become rather inexpensive and effective for specific technologies while other techniques are quite expensive yet effective on a wider range of technologies. Simply stating the requirement as "shall provide protection from fault induction" puts a significant burden on the vendor and laboratory to demonstrate that the cryptographic module protects against all possible techniques of fault induction. The requirement for fault induction should either be removed or explicitly defined in the standard similarly to how EFP and EFT are defined. An Annex could be included that specifically defines the fault induction techniques that are to be protected against. The Annex could be updated as new effective techniques are developed. It may also be more appropriate to include fault induction requirements under Section 4.7 Physical Security – Non-Invasive Attacks and included in Annex F specifying definitions and	

					methods.	
38.	InfoGard		Section 4.6, Page 31, Last Paragraph, 2nd Sentence	T	"Security Level 2 requires…the inability to gather information about the internal operations of the critical areas of the module (opaqueness)." Based on FIPS 140-3 discussion on this topic, the key requirement is composition of the module; the current text appears to focus on "internal operations". Suggest updating the text to be more consistent with IG 5.1: *"Component outlines may be visible from the enclosure openings or translucent surfaces as long as the component's manufacturer and/or model numbers, and/or composition and information about the module's design cannot be determined."*	
39.	InfoGard		Section 4.6.1, Level 2, Bullet 2	T	Security Level 2 requires "…the inability to gather information about internal operations of the critical areas of the module (opaqueness)." Based on FIPS 140-3 discussion on this topic, the key requirement is composition of the module; the current text appears to focus on "internal operations". Suggest updating the text to be more consistent with IG 5.1: *"Component outlines may be visible from the enclosure openings or translucent surfaces as long as the component's manufacturer and/or model numbers, and/or composition and information about the module's design cannot be determined."*	
40.	InfoGard		Section 4.6.2	T	Multi-chip modules (MCM) - integrated modules The current standard draft makes it difficult to describe multi-chip modules which are integrated at a microelectronic level, such as	

					stacked within MCM (i.e., multi-chip carriers). Strict interpretation of Level 4 tamper response requirements would mandate a discrete tamper matrix around such a structure, while its internal connections could be equivalently - or even better - protected from within the MCM. As a practical example, direct chip-to-chip connections through a single board, such as a 3D-stacked MCM, would need to be physically attacked through the connecting board. This attack surface may be covered by tamper detection circuitry within the board, exposing no interconnects, only inactive chip sides, to the outside. With slight changes, the Level 4 requirements in Sections 4.6.3 and 4.6.4 could accommodate tamper protection implemented between directly attached chips, without an external tamper response envelope. Vendors would need to convincingly demonstrate that the exposed interfaces - such as external surfaces of chips - may not be physically attacked with less effort than attacking an exposed mesh.	
41.	InfoGard		Section 4.6.1, Level 4, Bullet 3	T	"The cryptographic module shall provide protection from fault induction." Fault Induced Attacks are many; the general reference to such a term lacks specificity. See recommendation in Item 38.	
42.	InfoGard		Section 4.6.2, Level 3, Bullets 1 & 2	T	The following wording from the second bullet should be added to the first bullet associated with potting material: "…shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function)". Without such a characterization, "hard, opaque, tamper-evident coating" could be rather loosely interpreted and not provide protections adequate for Level 3.	

					Suggested text for Bullet 1: *"The module shall be covered with a hard, opaque, tamper-evident coating (e.g., a hard opaque epoxy covering the passivation), such that attempts at penetration to the underlying circuitry shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function)."*	
43.	InfoGard		Section 4.6.2, Level 4, Bullets 1 & 2	T	"The cryptographic module shall be covered with a hard, opaque removal-resistant coating with hardness and adhesion characteristics such that attempting to peel or pry the coating from the module will have a high probability of resulting in serious damage to the module (i.e., the module will not function)." For Level 4 single-chip modules, the majority that we evaluate have active and passive shielding. Hence, the current bullets should be adjusted to include this or a bullet should be added that accounts for this scenario. Suggest revising the text for Bullets 1 and 2 as follows: *"…(i.e., the module will not function or will zeroize all CSPs)."*	
44.	InfoGard		Section 4.6.3, Level 1	E	"If the cryptographic module is contained within an enclosure or within an enclosure that has a door or a removable cover, then a production-grade enclosure or enclosure with a door or a removable cover shall be used." Please update the text for proper grammar. Suggested text: *"If the cryptographic module is contained within an enclosure, then a production-grade enclosure shall be used."*	
45.	InfoGard		Section 4.6.3, Level 2, Last Bullet	T	"…shall be locked with pick-resistant mechanical locks employing physical or logical keys…"	

					What is the key strength to be used here?	
46.	InfoGard		Section 4.6.3, Level 3, Bullets 1 & 2	T	The following wording from the second bullet should be added to the first bullet associated with potting material: "…will have a high probability of causing serious damage to the module (i.e., the module will not function)". Suggested text for Bullet 1: *"The module shall be covered with a hard, opaque, tamper-evident coating (e.g., a hard opaque epoxy covering the passivation) such that attempts at penetration to the underlying circuitry shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function)."*	
47.	InfoGard		Section 4.6.4, Level 2	T	"…shall be locked with pick-resistant mechanical locks employing physical or logical keys…" What is the key strength to be used here?	
48.	InfoGard		Section 4.6.4, Level 3, Bullets 1 & 2	T	The following wording from the second bullet should be added to the first bullet associated with potting material: "…will have a high probability of causing serious damage to the module (i.e., the module will not function)". Suggested text: *"The module shall be covered with a hard, opaque, tamper-evident coating (e.g., a hard opaque epoxy covering the passivation) such that attempts at penetration to the underlying circuitry shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function)."*	
49.	InfoGard		Section 4.6, Paragraph 4	T	Since multi-chip embedded and multi-chip standalone modules have the same requirement set, is it necessary to distinguish between the two? Either (1) merge the two into a single term called multi-chip cryptographic modules, or (2)	

					leave separate definitions but merge the text so that both embodiments are referenced within one requirement set. This would reduce the redundancy in this standard as well as the future DTR.	
50.	InfoGard		Section 4.6, Table 3	E	Level 3 General Requirements: Tamper Response and Zeroization is not a general requirement as there are other ways to satisfy Level 3 for all embodiment types. Suggested text under Level 3 General Requirements: *"Protection from probing, as applicable."*	
51.	InfoGard		Sections 4.6.1, 4.6.3,, & 4.6.4; Level 3	E	These sections appear to be missing the requirement of "hard, removal-resistant coating".	
52.	InfoGard		Section 4.6.5.2, Paragraph 3	E	The text appears to reference inappropriate module responses to temperature events. Since this is under EFT, the module will not look to shutdown or zeroize CSPs; those responses require detection and response circuitry. If those detection mechanisms existed, the module would be classified under EFP. Suggested text: *"The temperature range to be tested shall be from - 100° to + 200° Celsius (- 150° to + 400° Fahrenheit); however, the test shall be interrupted as soon as the module enters a failure mode (i.e., the module no longer functions)."*	
53.	InfoGard		Section 4.6.5.2, Paragraph 4	E	The text appears to reference inappropriate module responses to voltage events. Since this is under EFT, the module will not look to shutdown or zeroize CSPs; those responses require detection and response circuitry. If those detection mechanisms existed, the module would be classified under EFP. Suggested text:	

					"The voltage range tested shall be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage that causes the module to enter a failure mode (i.e., the module no longer functions). The voltage range tested shall be gradually increasing from a voltage within the normal operating voltage range to a higher voltage that causes the module to enter a failure mode (i.e., the module no longer functions). This shall include testing the reverse polarity."	
54.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.6.1	G	Add a requirement for a "All Maintenance CPSs shall be zeroized when removable covers and doors within the maintenance access interface are closed". Rationale: Maintenance CSPs may be required to allow the cryptographic module to perform maintenance testing, for example test public/private key pairs. Removal of all maintenance CPSs prior to operational use should be required to prevent multiple cryptographic modules from operating with the same maintenance material being present.	
55.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.6.1	T	Do cryptographic modules need to provide protection from non-visible radiation explicitly Xrays? If so at what Security Level? Rationale: The ability to Xray a cryptographic device to determine internal organization can aide an adversary in defeating many physical protection mechanisms such as switches. Access covers or physical structures can be machined away to expose sensitive cryptographic circuits and memories.	
56.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.6.3	T	Could coatings, like those described in the paper titled Read-Proof Hardware from Protective Coating, attached to email, be used to meet Security Level 4? If disturbing this coating prevents secure operation of the cryptographic module and not potting material be applied to all chips performing security critical functions of a multichip module and meet Security Level 4 requirements?	

					Rationale: Coatings and circuits have been documented that allow secure storage and recovery of CSPs. Attempts to probe this coating may, or may not, be detectable to humans but modification of this coating prevents secure operation of the cryptographic device.	
57.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.6.4	T	Could coatings, like those described in the paper titled Read-Proof Hardware from Protective Coating, attached to email, be used to meet Security Level 4? If disturbing this coating prevents secure operation of the cryptographic module and not potting material be applied to all chips performing security critical functions of a multichip module and meet Security Levels 3 and 4 requirements? Rationale: Coatings and circuits have been documented that allow secure storage and recovery of CSPs. Attempts to probe this coating may, or may not, be detectable to humans but modification of this coating prevents secure operation of the cryptographic device.	
58.	NSA	TWG	Table 3	T	Do you need to add “hard opaque coating or enclosure” to the General Reqs for all Embodiments for security level 3? This is listed in Table 1 under Physical Security for level 3.	
59.	Orion	MS	Section 4.6, Table 3, Level 2	T	The table conflicts with the text in that the table allows only opaque covers, coatings, and enclosures while the text for Security Level 2 allows coatings and enclosures that are “either opaque or translucent within the visible spectrum”. Clarify.	
60.	Riscure	Marc Witteman	4.6.1	T	The section states that level 4 modules shall provide protection against ‘fault induction’. We welcome this requirement since fault attacks pose a growing and severe security threat that can break cryptographic systems with modest effort. We consider it appropriate for level 3 modules, which must implement tamper response, to also resist fault attacks.	

					Require resistance to fault attacks for level 3 modules.	
61.	Thales e-Security		4.6.1 General Physical Security Requirements, Security Level 2, 2nd bullet point	T	"*The tamper evident material, … shall either by opaque or translucent* ..." This precludes the use of clear tamper evident seals. Clear seals are useful for ensuring that a physical penetration attack cannot be concealed by an opaque label, and should not be precluded by the standard.	
62.	NIST	Elaine Barker	4.6.1 SL1		The cryptographic module **shall** consist of production-grade components that **shall** include standard passivation techniques (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage). Is "conformal coating" defined anywhere?	
63.	NIST	Elaine Barker	4.6.1 SL4		"When performing maintenance, all unprotected CSPs contained in the cryptographic module **shall** be zeroized. Zeroization **shall** either be performed procedurally by the operator or automatically by the cryptographic module." Is "the operator" the maintenance person? If not, is it done before the maintenance person is allowed access to the module?	
64.	NIST	Elaine Barker	4.6.1 SL4		The cryptographic module **shall** provide protection from fault induction Define "fault induction"	
65.	NIST	Elaine Barker	4.6.3, SL 3		The multiple-chip embodiment of the circuitry within the cryptographic module **shall** be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the	

					visible spectrum, Maybe the definition for the "visible spectrum" (which appears earlier in the section) should be placed in the glossary?	
66.	NIST	Elaine Barker	4.6.5.2		"The temperature range to be tested **shall** be from a temperature within the normal operating temperature range up to the largest negative temperature that either (1) shuts down the module to prevent further operation or (2) immediately zeroizes all CSPs; and from a temperature within the normal operating temperature range up to the largest positive temperature that either (1) shuts down the module to prevent further operation or (2) immediately zeroize all CSPs." The use of negative here is confusing,since the normal operating range may or may not include negative values in Fahrenheit or Celsius. Also, it could fail within the claimed normal operating range. Change the above test to: "The temperature range to be tested **shall** be from a temperature within the normal operating temperature range down to a temperature that either (1) shuts down the module to prevent further operation or (2) immediately zeroizes all CSPs; and from a temperature within the normal operating temperature range up to a temperature that either (1) shuts down the module to	

					prevent further operation or (2) immediately zeroize all CSPs”	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	Anagram Laboratories	Dr. Thomas A. Berson	Section 4.7 Paragraph 2	G&T	The requirement to mitigate non-invasive attacks must be applied to all cryptographic modules: single-chip modules as well as multi-chip modules. The current draft exempts multi-chip modules from the requirement to mitigate non-invasive attacks. There is no technical basis for such an exemption. A module's susceptibility to non-invasive attacks is not a function of whether there are one or many chips in that module. (In fact, more chips may lead to more such susceptibilities). The requirement to mitigate non-invasive attacks must be applicable to all cryptographic modules. NIST earlier in the FIPS 140-3 process confirmed that the requirement to mitigate non-invasive attacks would extend to multi-chip embedded and multi-chip standalone cryptographic modules. The current draft backs away from this requirement. This raises serious security concerns for users, who may be unaware of how many ICs in their module and are simply relying on FIPS 140-3 as a attestation of known quality. Also the unequal requirement creates a loophole through which vendors may gain approval to sell dangerously insecure products by adding an additional (even perhaps superfluous) IC to the module. The unequal requirement puts the whole FIPS 140-3 "brand" in jeopardy.	
2.	Anagram Laboratories	Dr. Thomas A. Berson	Section 4.7 Paragraph 3 & 4	G&T	Mitigation of non-invasive attacks (and certainly at least against simple power analysis) must be required beginning at Level 2. Noninvasive attacks, because they are non-destructive, present a greater security threat	

					than physical attacks. In particular, SPA and DPA easily compromise non-resistant cryptographic modules without leaving any physical trace. Neither do they trigger physical tamper-detection, tamper-evident or tamper-reaction features if these are present. Practical SPA and DPA attacks have been published against most commercially-important cryptographic algorithms. Other unpublished attacks certainly exist. These attacks require only basic equipment (e.g., a low-cost A/D board or an oscilloscope). As currently proposed, FIPS 140-3 requires that products validated at Level 2 have anti-tamper and tamper-evidence capabilities [e.g., Section 4.6.2 of the current draft]. It is poor security engineering, dangerously misleading, and illogical to claim value in physical tamper-resistance and/or tamper-evidence capabilities for a product which offers no protection against easier-to-mount and non-invasive attacks. Physical tamper-evidence and tamper-resistance features are irrelevant if keys can be trivially extracted by external power measurements, such as in SPA. I conclude that mitigation of non-invasive attacks (if not all, at least SPA) must be required beginning at Level 2.	
3.	brightsight	Lex Schoonen	4.7	T	Multi-chip products should not be excluded from the requirements on non-invasive attacks. There is no reason such products would not be vulnerable to these classes of attacks, and excluding these products will lead to undesired differences in the protection level provided by products certified at identical security levels. It will also allow manufacturers to bypass their responsibility by slightly altering their design. It puts an unfair additional burden on manufacturers who try to reduce the component count in their products, which for many reasons and in many situations is an approach which should be	

					applauded, not discouraged.	
4.	brightsight	Lex Schoonen	4.7	T	Security level 2 is characterized by tamper-evidence requirements on the product. Given that non-invasive attacks would by definition bypass the mechanisms that are constructed to satisfy those requirements, that they are well-known in the public domain, and they typically can be mounted using only low-cost equipment, brightsight is of opinion that mitigation of such attacks should be present in products even before mitigation of invasive attacks is to be considered. Therefore, some requirements should be present at security level 2. In order to achieve the gradual increase of security as the security level increases, we would suggest introduction of coverage against SPA/SEMA and timing attacks at level 2, either by the manufacturer's demonstration of coverage, or by testing.	
5.	brightsight	Lex Schoonen	4.7	T	Analogous to the previous point, which points out that mitigation of SPA/SEMA classes of attacks should be mandated at level 2, brightsight recommends that security level 3 explicitly requires manufacturers to provide demonstrably effective mitigation techniques against DPA/DEMA. As experience shows that it is very easy to correctly implement a countermeasure which is effective in concept, the demonstration of effectiveness should include tests by an independent lab.	

6.	CSEC	Jean Campbell	4.7	G	"The requirements of this section **shall** be applicable to single-chip cryptographic modules and single-chip components of hybrid modules. The requirements of this section are optional for all other hardware module embodiments." What is this paragraph saying? Are there any methods that can be applied to other hardware modules?	
7.	CSEC	Jean Campbell	4.7.		Security Level 4 "In addition to the requirements for Security Level 3, the module **shall** undergo testing, and **shall** meet the requirements defined by the validation authority, for each of the applicable non-invasive attacks and the Approved or Allowed security functions which are relevant to those attacks, as specified in Annex F." Will this testing include probe insertion through vents, like RF antenna?	
8.	EWA-Canada IT Security Evaluation & Test Facility	Dawn Adams	**4.7 Physical Security – Non-Invasive Attacks**	T	There are no standards for mitigating against these types of attacks. The specified testing is not conformance testing so this requirement section should be removed. These requirements will further restrict the number of Security Level 4 validated cryptographic modules. It would be better to specify mitigation mechanisms rather than the testing. Suggest removing this requirement section.	

9.	Infineon Technologies	Joerg M. Borchert	**4.7**		The FIPS PUB 140-3 section 4.7 Physical Security – Non-invasive attacks. This section sets the requirements for non-invasive attacks only for single-chip modules and single-chip components of hybrid modules, but leaves it optional for all other hardware modules. Based on our research we recommend that the requirements to fight off the non-invasive attacks should be applied to ALL cryptographic modules. These should include single-chip modules, multi-chip embedded modules and multi-chip standalone modules The reasons are 1.1 It does not make sense from a technical point of view to apply different security requirements based on the physical embodiment or the number of chips (>1). The physical embodiment does not change the threat of the observant attack class scenarios. Non invasive attacks such as SPA, DPA and EMA can be used independently of the form factor against any device which uses or contains secret keys and does not have the appropriate countermeasures implemented. The only scenario we can foresee which would make the threat of observant attacks irrelevant are products which are always used in physically protected rooms. 1.2 Packaging technology can be easily used by manufacturers as a decisive factor to circumvent the requirements to harden a cryptographic module against non-invasive attacks. The option might create an incentive to avoid the more costly measure to make a module more secure. The result can counter the original intent of FIPS 140-3. 1.3 The inconsistency in the requirements favors vendors who design lower-security multi-chip products. This creates situation where adding additional module complexity will reduce the requirement for true hardware	

					security countermeasures into individual ICs.	
10.	Infineon Technologies	Joerg M. Borchert	**4.7**		Infineon Technologies North America recommends adjusting the levels for section 4.7. Specifically : **Level 2 should require the protection against basic non-invasive attacks** The section 4.7 requires no protection measures against the non-invasive attacks for security levels 1 and 2. However, the basic side channel attacks are publically available, and no longer a specific knowledge base. The investment for an attacker is minimal. The section 4.6.2 on the other hand requires for Level 2 already means “to deter direct observation or manipulation of the module and to provide evidence of attempts to tamper with or remove the module”. Therefore, FIPS 140-3 requires a basic protection against the manipulative and semi-invasive attack class but excludes the observing attack class. These different requirements for level 2 from our perspective are inconsistent. This would result in an available option to lower the security requirement for level 2 for all attack classes to “no protection” which does not seem to be the intention of FIPS 140-3 Section 4.6.2. The recommendation is to include the observing attack class with non-invasive attacks countermeasures at level 2 in section 4.7. The benefits in security would be substantial while the investment for the vendors in implementation and testing would be limited especially as the lower-level	

					validations allow for vendor documentation of the tests in place of third party lab testing. Even if this practice might seem counterintuitive, it is a better practice in comparison to the alternative to allow the dangerous attack class at level 2.	
11.	Infineon Technologies	Joerg M. Borchert	**4.7**		Infineon Technologies North America recommends adjusting the levels for section 4.7. Specifically : **Level 3 should already require testing against non-invasive attacks** As already mentioned above the observing attack class is a serious threat to the module's CSP. Therefore, we recommend that validation testing should be required already at level 3. Infineon Technologies North America Corp. sees the advantage of a common testing methodology to achieve the level 3. This will give the confidence and confirmation of the presence of countermeasures. As the non-invasive attacks are a serious threat to the CSP, the testing requirements for the higher level certifications should include independent security laboratory validation testing. This requirement should be applicable for Level 3 and above. A common test methodology should be used to allow the application of a metric on the countermeasures. Infineon Technologies has a long positive experience with the Common Criteria methodologies, and the related security evaluations which cover all 3 major attack classes. NIST and the testing labs should apply a similar metric. If the FIPS140 approved test entities are unable to do these tests by themselves there are alternative options like outsourcing within US or internationally.	

12.	Infineon Technologies	Joerg M. Borchert	**4.7**		Infineon Technologies North America Corp sees tremendous value to include the observant attack class i.e. non-invasive attacks into FIPS 140-3. It reflects the ongoing research and development in the field of security and the related threats to cryptographic modules. The new structure of the standard allows to add new specific requirements based on new threats into the Annex to the standard which makes it flexible. Infineon strongly recommends applying the same requirements to all CSP independent of the form factor. The non-invasive attacks as part of the observant attack class are independent of the form factor and therefore the requirements should be the same for a single chip module and the multi chip module. The differentiation between a single chip module with compulsory requirements and multichip modules with optional requirements is from a security perspective, arbitrary, and inappropriate. The consequence of the proposed standard as written can result in an uneven playing field, and a perceived security level for multi chip modules where the dangerous attacks of non-invasive attacks is not mitigated. Infineon Technologies further recommends applying a higher standard for non-invasive countermeasures at the lower security levels than which is proposed in the current draft of FIPS 140-3. The wide proliferation of the SPA and DPA attack tools makes it simple to perform the attacks for a large number of people with limited knowledge and investment. This draft does not take into consideration this situation. The consequences can be potentially dangerous, if not devastating for entities relying on the FIPS 140-3 standard and the evaluation by the FIPS 140 laboratories	

13.	Cryptography Research, Inc.		4.7 para 2	G,T	**The standard should not apply a lower security requirement for multi-chip modules.** The latest revision of FIPS140-3 draft for public comment v2.2, section 4.7 Physical Security – Non-Invasive Attacks, states that the requirements to mitigate non-invasive attacks shall be applicable to single-chip cryptographic modules and single-chip components of hybrid modules, and optional for all other hardware module embodiments. We strongly believe that the requirement to mitigate non-invasive attacks should be applicable to all cryptographic modules, including single-chip modules, multi-chip embedded modules and multi-chip standalone modules. Non-invasive attacks such as SPA and DPA can be used to attack any device that uses secret keys, unless the device includes countermeasures to mitigate these attacks. All form factors of cryptographic modules are equivalently susceptible. As a result, it is not appropriate to apply different security requirements on the basis of physical embodiment or the number of IC chips contained within a physical embodiment. Additionally, making the requirements to mitigate non-invasive attacks optional for multi-chip modules would arbitrarily favor vendors who produce lower-security multi-chip products and create an uneven playing field. Further, exempting multi-chip modules could create an incentive for manufactures to circumvent requirements by making trivial changes to packaging technology. In comment number 381 submitted following the first draft of FIPS140-3, NIST resolved that requirements to mitigate non-invasive attacks would apply to multi-chip embedded	

					and multi-chip standalone cryptographic modules. The latest draft of the specification contradicts this resolution. Discussion: The latest revision of FIPS PUB 140-3 (Revised DRAFT 09/11/09), section 4.7 Physical Security – Non-Invasive Attacks, states that the requirements to mitigate non-invasive attacks shall be applicable to single-chip cryptographic modules and single-chip components of hybrid modules, and is optional for all other hardware module embodiments. We strongly believe that the requirement to mitigate non-invasive attacks should be applicable to <u>all</u> cryptographic modules, including single-chip modules, multi-chip embedded modules and multi-chip standalone modules. The reasons include: a. It is not technologically appropriate to differentiate security requirements on the basis of physical embodiment or the number of IC chips contained within a physical embodiment. Non-invasive attacks such as SPA and DPA can be used to attack any device that uses secret keys, unless the device includes countermeasures to mitigate these attacks. There is no relationship between a cryptographic module's susceptibility to a non-invasive attack based upon the number of ICs that it incorporates. Multi-chip modules, whether standalone or embedded, are similarly susceptible to non-invasive attacks as their single-chip counterparts. (If a distinction is required for modules where power analysis and related threats are inapplicable, we would suggest that NIST exclude products whose usage ensures they will always be in high-security physically protected rooms, and such products should be excluded from all tamper-	

					resistance and tamper-evidence requirements.) b. Since more than 90% of the FIPS 140-3 validated cryptographic modules to date are multi-chip modules, the proposed exception would eviscerate the requirement and leave the majority of modules without any requirement to be protected from a widely-known and catastrophic class of vulnerabilities. c. It is inconsistent to make the requirements to mitigate non-invasive attacks optional for multi-chip modules. If not corrected, the resulting standard would arbitrarily favor vendors who produce lower-security multi-chip products and create an uneven playing field. d. Exempting multi-chip modules from requirements to mitigate non-invasive attacks could create an incentive for manufactures to circumvent requirements by making trivial changes to packaging technology. e. In comment number 381 submitted following the first draft of FIPS140-3, NIST resolved that requirements to mitigate non-invasive attacks would apply to multi-chip embedded and multi-chip standalone cryptographic modules. The latest draft of the specification contradicts this resolution. f. A brief review of the current FIPS 140-2 validated modules identifies numerous examples where the proposed exclusion for multi-chip modules does not make sense and would apply unequal requirements to similar products. We have attached **Exhibit A** which illustrates	

					specific examples, including: ▪ There are existing FIPS 140-2 validated modules that (1) perform the same security function; (2) have the same form factor; and (3) share the same cryptographic boundary, but differ in their categorization as single-chip, multi-chip embedded or multi-chip standalone modules. ▪ There are existing FIPS 140-validated multi-chip modules that perform similar functions as their single-chip counterparts, and differ only with respect to form factor. For example, a single-chip secure access or ID deployment at a given FIPS security level has numerous functionally-similar devices (smart cards, secure memory cards, secure USB tokens, etc.) in the multi-chip format. ▪ There are existing FIPS 140-validated modules designed for the same application (e.g. postal security devices (PSDs)), where all three form factors (single-chip, multi-chip embedded and multi-chip standalone) are represented. ▪ There are existing FIPS 140-validated modules with a shared form factor (e.g. USB token) which include a single-chip security element (typically a smart card IC) where the primary difference between the single-chip and multi-chip modules is that the multi-chip modules contain an additional IC for storage. It is also important to note that power analysis attacks are a serious threat to all of the modules and form factors in Exhibit A.	

14.	Cryptography Research, Inc.		4.7 para 3, 4	G,T	**Requirements to mitigate non-invasive attacks should be introduced at Level 2.** We believe that requirements to mitigate the basic forms of non-invasive attacks, such as SPA and SEMA should be introduced at security Level 2, not Level 3, as currently outlined in section 4.7 Physical Security – Non Invasive Attacks. SPA attacks against highly-vulnerable devices are very easy to implement, and require only momentary external access to the module. SPA also requires only minimal attacker sophistication. Basic SPA attacks simply involve visual inspection of traces on an oscilloscope screen. It is not necessary to use special probes, custom attack software, or other analysis capabilities. Level 2 products are intended to have rudimentary anti-tamper and tamper-evidence capabilities. In particular, Section 4.6.2 Physical Attacks requires CSPs "…to deter direct observation, or manipulation of the module…". Non invasive attacks such as SPA are conducted without breaching the security perimeter of the CSP, so approving a module at Level 2 where the module is highly vulnerable to SPA would be both contradictory and inconsistent. Lowering the basic non-invasive attack mitigation requirements to Level 2 would provide major security benefits and would not add materially to the testing cost or overhead. Discussion: We believe that requirements to mitigate the basic forms of non-invasive attacks, such as simple power analysis (SPA), should be introduced at security Level 2, not Level 3, as currently outlined in section 4.7 Physical Security – Non Invasive Attacks. a. SPA attacks against highly-vulnerable	

					devices are very easy to implement, and require only momentary external access to the module. SPA also requires only minimal attacker sophistication. Basic SPA attacks simply involve visual inspection of traces on an oscilloscope screen, and it is not necessary to use special probes, custom attack software, or other analysis capabilities. Level 2 products are intended to have rudimentary anti-tamper and tamper-evidence capabilities. In particular, Section 4.6.2 Physical Attacks requires CSPs "…to deter direct observation, or manipulation of the module…". Non invasive attacks such as SPA are conducted without breaching the security perimeter of the CSP, so approving a module at Level 2 where the module is highly vulnerable to SPA would be both contradictory and inconsistent. b. Lowering the basic non-invasive attack mitigation requirements to Level 2 would provide major security benefits and would not add materially to the testing cost or overhead. In particular, the draft already allows labs to rely upon vendor documentation (instead of performing their own countermeasure testing) for lower-level certifications. As a result, countermeasure requirements can be added at Level 2 with minimal burden. (While reliance on vendor documentation is somewhat controversial due to the potential for security problems to be missed, we believe the approach proposed for FIPS 140-3 is appropriate because it enables countermeasure requirements to be introduced at lower levels.) The burden on implementers is also minor as compared to the security benefits. As	

					discussed in Section 1 above, many products certified under FIPS 140-2 at Level 2 (and below) already include countermeasures to noninvasive attacks. Over 4 billion security products are manufactured annually (including many costing under $0.50 each, but also including larger products) with countermeasures to noninvasive attacks, so countermeasure technologies are both widely available and inexpensive.	
15.	Cryptography Research, Inc.		4.7 para 4, 5	G,T	**Testing should be introduced at Level 3 rather than Level 4.** We are concerned that the requirement for the module's CSP to undergo testing is only introduced at the highest security Level 4. We believe that the requirement for the module to undergo some level of testing should be introduced at Level 3. Because non-invasive attacks are serious threats facing CSPs, testing requirements for moderately high-level certifications (i.e., Level 3 and above) should include some laboratory testing. The minimal equipment necessary to conduct testing is not prohibitively expensive and can be obtained from multiple vendors or built in-house (as many university students and testing labs have done). A common methodology for testing can be achieved using metrics that are acceptable to NIST and the testing laboratories. Evaluation labs for Common Criteria and other security standards have been adept at developing noninvasive testing skills. SPA and DPA testing results have been found to be among the most consistent and definitive of all security tests (and more consistent and definitive than physical testing which FIPS 140 currently includes). FIPS 140 laboratories which are unable to perform testing internally could outsource the work to	

					any of the numerous labs in the U.S. and internationally with this capability. *(Comment: From a security perspective, the requirement for vendors to address non-invasive attack vulnerabilities and implement countermeasures is more important than the testing methodology. As a result, we consider this section's suggestion to be non-critical – unlike the prior two recommendations.)* We are concerned that the requirement for the module's CSP to undergo testing is only introduced at the highest security Level 4. We believe that the requirement for the module to undergo some level of testing should be introduced at Level 3. We believe that, at a minimum, testing should be required at Level 3 to confirm the presence and correct functioning of the mitigation techniques employed by the CSP. Because non-invasive attacks are serious threats facing CSPs, testing requirements for relatively high-level certifications (i.e., Level 3 and above) should include some laboratory testing. The minimal equipment necessary to conduct testing is not prohibitively expensive and can be obtained from multiple vendors or built in-house (as many university students and testing labs have done). A common methodology for testing can be achieved using metrics that are acceptable to NIST and the testing laboratories. Evaluation labs for Common Criteria and other security standards have been adept at developing noninvasive testing skills. SPA and DPA testing results have been found to be among the most consistent and definitive of all security tests (and more consistent and definitive than physical testing which FIPS 140 currently includes). FIPS 140 laboratories which are unable to perform testing internally could outsource the work to any of the numerous	

					labs in the U.S. and internationally with this capability.	
16.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.7	T	Why are software cryptographic modules not required to protect against timing, simple power analysis, differential power analysis, cache analysis (paper titled “Analysis of countermeasures against access driven cache attacks on AES”, file attached to email) and predictive branch analysis (paper titled “On the Power of Simple Branch Prediction Analysis” – file attached to email) side channel attacks at Security Levels greater than 1? Rationale: Research literature contains examples of these, and possibly other, side channel attacks that can be performed against software and this literature contains counter measure for these attacks.	
17.	Oberthur Technologies	Clement Capel & Christophe Goyet	§4.7	T	attacks §4.7 (which are curiously only required to be performed for single chips modules) are very costly and we would like NIST to accept attacks results provided in other evaluation reports such as Common Criteria (from a lab in Europe or in the USA).	

18.	Defense Manpower Data Center (DMDC)	CTIS	4.7 para 2	G,T	Multi-chip modules should be required to mitigate Non-Invasive Attacks FIPS140-3 states that the requirements to mitigate non-invasive attacks shall be applicable to single-chip cryptographic modules and single-chip components of hybrid modules, and optional for all other hardware module embodiments. No cryptographic module should earn some preferential treatment over another. In multi-chip modules a single chip could be handling all cryptographic functions; therefore, all cryptographic modules should be held to the same standard. One requirement will also clear any confusion on whether something should be considered as a single chip versus a multi-chip. Require multi-chip modules to mitigate non-invasive attacks.	
19.	Riscure	Marc Witteman	4.7	T	The title of this section is “Physical Security – Non Invasive Attacks”. Some relevant side channel attacks do require limited invasive action, for instance removal of the plastic cover of smart card chips. These attacks are generally referred as ‘semi-invasive’ and remove physical barriers that have no security function. We do not see the need to restrict these attacks to pure non-invasive. Instead we prefer a clear reference to the side channel nature of the related threat. Rename section to “Side Channel Security”. Remove the strict non-invasive description, or change to: non-invasive and semi-invasive.	

20.	Riscure	Marc Witteman	4.7	T	Level 3 evaluation requires proof for side channel resistance in the form of documentation. For level 4 the resistance must be evaluated through testing. From our extensive experience in side channel evaluation we know that side channel resistance can only be judged by review if the reviewer also has significant test experience, and understands contemporary side channel weaknesses. With the low number of level 4 evaluations compared to level 3 we believe that review results are only trustworthy if performed by experienced side channel test labs. Introduce requirement that level 3 side channel protection reviews may only be performed by labs who can and do perform side channel tests (as required for level 4). Even better: consider to mandate testing for level 3 modules to reduce the risk of vulnerabilities be overlooked.	
21.	Riscure	Marc Witteman	4.7	T	The section states that the requirements are only mandatory for single chip modules. This suggests that multi chip modules are not vulnerable. Practice has proven that this is not true. Furthermore the requirement could encourage manufacturers to include multiple chips in their module to avoid side channel testing. Apply the requirements to all modules, regardless of the number of chips.	
22.	Smart Card Alliance		4.7 para 2	G,T	**Multi-chip modules should be required to mitigate Non-Invasive Attacks** The latest revision of FIPS140-3 draft for public comment v2.2, section 4.7 Physical Security – Non-Invasive Attacks, states that the requirements to mitigate non-invasive attacks shall be applicable to single-chip cryptographic modules and single-chip components of hybrid modules, and optional for all other hardware module embodiments. Require multi-chip modules to mitigate non-	

					invasive attacks. The requirement to mitigate non-invasive attacks should be applicable to all cryptographic modules, including single-chip modules, multi-chip embedded modules and multi-chip standalone modules. For multi-chip modules, if the cryptographic functions are in one chip, then that chip should be required to mitigate non-invasive attacks. In the case where cryptographic operations span the boundaries of more than one chip in a multi-chip module, then the multi-chip module should mitigate non-invasive attacks within the cryptographic boundaries. Example multi-chip modules may include MicroSD devices, USB tokens and security application modules (SAMs) used in readers. There is no technical or security rationale for creating a different security requirement for multi-chip products, since the need for protection from non-invasive attacks is the same regardless of the module type. Excluding multi-chip modules from the requirement will create an uneven playing field while creating serious security risks.	
23.	Smart Card Alliance		4.7 para 3, 4	G,T	**Requirements to mitigate non-invasive attacks should be introduced at Level 2** We believe that requirements to mitigate the basic forms of non-invasive attacks, such as SPA should be introduced at security Level 2, not Level 3, as currently outlined in section 4.7 Physical Security – Non Invasive Attacks. SPA attacks against highly-vulnerable devices are very easy to implement, and require only momentary external access to the module. SPA also requires only minimal attacker sophistication. Non invasive attacks such as SPA are conducted without breaching the security	

					perimeter of the CSP, so approving a module at Level 2 where the module is highly vulnerable to SPA would be both contradictory and inconsistent. More than four billion security products are made each year with protections against both SPA and DPA, demonstrating that it is practical for vendors to address these vulnerabilities in products. Require modules to mitigate non-invasive attacks at Level 2.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Peter Kim	4.8.3 1st para	G	What is the difference between “transport” and “entry”, since they are differentiated here? Manual transport is not defined in the Glossary. Traditionally, there is the concept of “manual establishment” and “manual entry”, but not of manual transport. Please clarify.	
2.	atsec	Peter Kim	4.8.4 5th para, Last sentence	E	The requirement seems to imply the Manual Key Entry test is only required for the entry of CSPs and not PSPs. Please clarify the intent by either keeping.	
3.	atsec	Peter Kim	4.8.4 7th para	T	The statement indicates passwords can be entered and output in plaintext and places no restrictions on this. Under FIPS 140-2, passwords cannot be entered or output in the clear at Levels 3 and 4 without what will not be considered a Trusted Channel. Please clarify the intent of this requirement or move it to the relevant section.	
4.	atsec	Peter Kim	4.8.4 Security Levels 1 & 2	T	There is no restriction for the entry of the CSP to be local, directly connected, or through a Trusted Channel. As a result, the operator could choose to enter a plaintext key through a non-wireless network, despite the number of intermediate systems the key value would likely pass through. Include an additional requirement for manual establishment of plaintext keys to prevent the entry through a non-wireless network.	

5.	Cisco	Max Pritikin IEEE 802.1AR Editor	General	G	IEEE 802.1AR-2009 does not mandate that key material be generated within the module. This is to support devices and solutions which may have insufficient entropy or processing power during manufacturing to effectively generate appropriate key material. IEEE 802.1AR clause 6.5.1 mandates that the generation mechanism used must be reported in the Protocol Implementation Conformance Statement (PICS) as detailed in Appendix A. Clause 6.5.1 does note that the choices made by the manufacturer during manufacturing may substantially effect the subsequent perceived security inherent in this key material. It would be reasonable for FIPS 140-3 to provide some guidance regarding generation of manufacturing installed key material. For example mandating that such key material be generated within the module and after it has passed FIPS-140 tests.	
6.	Cisco	Max Pritikin IEEE 802.1AR Editor	4.8.6	T	Re: “SSPs need not meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key)”. This sentence in unclear. The following terms should be defined: “authentication proxies” “module initialization key”	

7.	Cisco	Max Pritikin IEEE 802.1AR Editor	4.8.6	T	The effect of ‘zeroization’ on manufacturer installed credentials should be specifically stated. The zeroization requirements must clarify if they intend for factory installed credentials, such as IEEE 802.1AR IDevIDs, to be zeroized or not. (Zeroization of such data precludes ever returning the device to factory default behavior, and in many of the examples provided will effectively “brick” the device such that it can not be used again.) A significant number of existing products, that implement standard based protocols which require manufacturing installed certificates, currently achieve FIPS 140-2 certification. With mandated zeroization of manufacturing installed credentials these product manufacturers must choose between FIPS certification or standards compliance. Manufacturer installed credentials appropriate generated within the module (see comment #6) should be specifically exempted from automated zeroization at Levels 1, 2. Manual zeroization at Levels 3 & 4 is an important security consideration but it should be made clear that doing such precludes the device from ever being returned to factory default settings. Automated zeroization of the manufacturing installed credentials due to “Penetration of the cryptographic module enclosure from any direction” (Section 1.4) may be appropriate.	

8.	Cisco		4.8.6	T	“The module shall provide an output status indication when the zeroization is complete.” Some modules are handling thousands+ concurrent cryptographic sessions. Requiring a distinct status output each time a CSP is automatically zeroized could quickly become unwieldy and result in the loss of usefulness of the status output. Clarify the details of the requirement. Recommendations: A counter identifying the # of zeroizations would be an allowable solution. Or This requirement only applies to CSPs that are manually zeroized (rather then automatically zeroized during operation)	
9.	CSEC	Claudia Popa	4.8	G	FIPS 140-2 did not have any requirements or guidance for “cryptoperiods”. NIST SP 800-57 Part 1 has some recommendation on cryptoperiods. Can some of these recommendations be included in the FIPS 140-3 standard?	
10.	CSEC	Claudia Popa	4.8.2	G	“SSPs generated by the module for use by an Approved or Allowed security function or key establishment technique **shall** be generated using an Approved or Allowed SSP generation method listed in Annexes C and D.” The Approved RBG are listed in Annex A. Should this annex also be referred here? Annex D refers to the FIPS 140-3 Implementation Guidance document that was not provided. Annex C does not include NIST SP 800-56B. Annex C refers to the FIPS 140-3	

					Implementation Guidance document that was not provided.	
11.	CSEC	Claudia Popa	4.8.2	G	How do we link the requirements from 4.8.2 with section 7.8 of the FIPS 140-2 Implementation Guidance, “Key Generation Methods Allowed in FIPS Mode”? Will 7.8 “Key Generation Methods Allowed in FIPS Mode”, just be moved to a new Implementation Guidance document?	
12.	CSEC	Claudia Popa	4.8.2	G	FIPS 140-2 did not have any requirements that will not allow the use of a key for more than one purpose (e.g., encryption, authentication, key wrapping) NIST SP 800-57 Part 1 contains some recommendations on Key Usage. Can some of these recommendations be included in the FIPS 140-3 standard?	
13.	CSEC	Claudia Popa	4.8.3	E	The general part of 4.8.3 contains this requirement: “Electronically transported CSPs shall be encrypted”. Later, the same requirement is repeated under the requirements for Security Levels 3 and 4. What does it mean? Does this requirement “Electronically transported CSPs shall be encrypted”. apply only to Security Levels 3 and 4?	

14.	CSEC	Claudia Popa	4.8.3	T	FIPS 140-2 standard has this paragraph: “If, in lieu of an Approved key establishment method, a radio communications cryptographic module implements Over-The-Air-Rekeying (OTAR), it shall be implemented as specified in the TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, *Over-The-Air-Rekeying (OTAR) Protocol*, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January, 1996, Telecommunications Industry Association. This information in not included in the FIPS 140-3. Was this part removed on purpose? Is the intention to have this allowance removed completely or just to move this information in a different document?	
15.	CSEC	Jean Campbell	4.8.4	G	These are the existing requirements. “If split knowledge procedures are used: • The module **shall** separately authenticate the operator entering or outputting each component as a separate identity. • At least two components **shall** be required to reconstruct the original CSP. • Documentation **shall** demonstrate that if knowledge of *n* components is required to reconstruct the original CSP, then knowledge of any *n-1* components provides no information about the original CSP other than the length. • Documentation **shall** specify the split knowledge procedures employed by a module. “ Can we be more specific about what split knowledge procedures can be implemented?	

16.	CSEC	Jean Campbell	4.8.2	E	*"*A module may generate SSPs internally or they may be entered into the module." Change to: " SSPs may be internally generated or they may be entered into the module".	
17.	CSEC	Jean Campbell	4.8.2	T	*"*Documentation **shall** specify each SSP generation method employed by a module. " Documentation shall specify whether a SSP is direct output of a RBG. Documentation shall specify how the output of the RBG is modified.	
18.	CSEC	Jean Campbell	4.8.2	T	*"*SSPs generated by the module for use by an Approved or Allowed security function or key establishment technique **shall** be generated using an Approved or Allowed SSP generation method listed in **Annexes C and D."** Why do we need two annexes? Can we merge these two annexes in one?	
19.	CSEC	Jean Campbell	4.8.3	E	"SSP establishment may consist of SSP transport followed by SSP entry or **output,** or it may consist of a SSP agreement process." Is this "SSP entry or output", or just "SSP entry"?	
20.	CSEC	Jean Campbell	4.8.3	E	"Electronically transported CSPs **shall** be in encrypted form." Change like: "Electronically transported CSPs **shall** be encrypted."	

21.	CSEC	Jean Campbell	4.8.3	T	"Other than when first establishing a Trusted Channel, **SSPs shall** be transported electronically over the Trusted Channel, whether or not they…" Why do PSPs need to be encrypted?	
22.	CSEC	Jean Campbell	4.8.3	E	SECURITY LEVEL 3 and 4 "Electronically transported CSPs **shall** be encrypted." This is a repeat of the information from "general" 4.8.3.	
23.	CSEC	Jean Campbell	4.8.3	E	"The integrity of all electronically transported SSPs **shall** be cryptographically protected (e.g., by an Approved or Allowed security function or an Approved or Allowed key establishment method)." This sentence is not clear.	
24.	CSEC	Jean Campbell	4.8.4	E	Add the text in bold: "Documentation **shall** specify the SSP entry and output methods employed by a module, **and if entered plaintext or encrypted."**	
25.	CSEC	Jean Campbell	4.8.4	E	*"*During manual SSP entry, the entered **values** may be temporarily displayed to allow visual verification and to improve accuracy." Change **value t**o **SSP**	
26.	CSEC	Jean Campbell	4.8.4	T	*"*If split knowledge procedures are used:…" Are there any "approved/allowed" split knowledge procedures? Can we be more specific?	

27.	CSEC	Jean Campbell	4.8.4	T	"Documentation **shall** demonstrate that if knowledge of *n* components is required to reconstruct the original CSP, then knowledge of any *n-1* components provides no information about the original CSP other than the length. " Is there a strength requirement as well for these components?	
28.	CSEC	Jean Campbell	4.8.4	T	"For software modules, CSPs may be entered into or output from the module in either encrypted or plaintext form under control of the module operating system provided that the CSPs are maintained within the operational environment." What is the software module inputs the key from outside physical boundary and the key is maintained within the operational environment?	
29.	CSEC	Jean Campbell	4.8.4	E	Security Levels 3 and 4 "The Trusted Channel **shall** use only Approved or Allowed security functions. " This is already a requirement in 4.2.	
30.	CSEC	Jean Campbell	4.8.4	G	Page 41, and also on page 40 . "In addition to the requirements specified for Security Level 2, a cryptographic module **shall** utilize a Trusted Channel for the input or output of all SSPs, whether or not cryptographically protected." Is this requirement double encryption?	
31.	CSEC	Jean Campbell	4.8.4	E	"Access to plaintext CSPs by unauthorized operators from outside the module **shall** be prohibited. Modification of PSPs by unauthorized operators from outside the module **shall** be prohibited." "operator" shall be replaced by "entity".	

32.	CSEC	Jean Campbell	4.8.6	G	"Zeroization of PSPs, encrypted CSPs, or CSPs otherwise physically or logically protected within an additional embedded validated module **(meeting the requirements of this standard)** is not required." The requierments of this standard as well as FIPS 140-2?	
33.	CSEC	Jean Campbell	4.8.4	G	On page 41, last paragraph for section 4.8.4, there are more requirements for split knowledge procedures. Why don't create a subsection on split-knowledge procedure, i.e. 4.8.4.1?	
34.	CSEC	Jean Campbell	4.8.6	E	Page 42, Security Levels 2 and 3: "Temporary SSPs **shall** be zeroized when they are no longer needed." This requirement is already in the first sentence of section 4.8.6.	
35.	JCMVP		Draft Revised	4.8,	Paragraph 5	
36.	JCMVP		Draft Revised 4.8, Paragraph 5	T	The following disclaimer exits: "Keys used for self-tests specified in Section 4.9 are not considered SSPs." We suppose that this originates from I.G. 7.4 in FIPS 140-2 I.G. However the word, "only", has been dropped in comparison with the I.G. Please insert the word "only" between "used" and "for" in the sentence.	
37.	JCMVP		Draft Revised 4.8.3, Security Levels 3 and 4	E	The word, "shall", is not colored red in the 1st sentence of the paragraph.	

38.	JCMVP		Draft Revised 4.8.4 Security Levels 3 and 4	E	“In addition to the requirements specified for Security Level 2” should be “In addition to the requirements specified for Security Level 1 and 2”.	
39.	JCMVP		Draft Revised 4.8.4, Security Levels 1 and 2	T	The following is said in Section 4.8.4 "Input and output of CSPs over unencrypted wireless connections is not allowed." This sentence states prohibition of CSP input/output over unencrypted wireless connections. However it is not used the word "shall". So we would like to know whether this sentence is a requirement or not. If so, please replace the word "is not" by "shall not be".	
40.	CMVP	Kim Schaffer	4.8	T	“Keys only used for self-tests specified in Section 4.9 are not considered SSPs.” This alleviates the case where the vendor may claim active keys are used for self-tests and do not have to be zeroized.	
41.	CMVP	Kim Schaffer	4.8	E	Should not need “Documentation shall specify all SSPs employed by a module.” since it should be in the security policy. Appendix B.	
42.	CMVP	Kim Schaffer	4.8.1	T	Since there is not a unified agreement as to entropy I would advise not demanding entropy considerations beyond some of the SP 800 series that already place requirements. Additionally entropy is most needed during the initialization of the module so if it is gathered externally it will be difficult to input encrypted.	
43.	CMVP	Kim Schaffer	4.8.3	T	Encrypted CSPs should not be required over a Trusted Channel unless they must also travel outside of the channel.	
44.	CMVP	Kim Schaffer	4.8.4 1st paragraph	T	Output via a visual display is not sufficient to determine manual entry.	

45.	CMVP	Kim Schaffer	4.8.4 Split knowledge		"Documentation shall demonstrate that if knowledge of n components is required to reconstruct the original CSP, then knowledge of any n-1 components provides no information about the original CSP other than the length." This seems unnecessarily restrictive. Is there sufficient weakness exposed if it is n-2 and greater than 3?	
46.	CMVP	Kim Schaffer	4.8.4 Security levels 1 & 2	T	Should wireless be expanded to broadcast?	
47.	CMVP	Kim Schaffer	4.8.5 Levels 3.& 4	T	Are each of the methods of input/output listed considered to be Trusted Channel or is this in addition?	
48.	CMVP	Kim Schaffer	4.8.5	T	If SSPs and CSPs and PSPs this appears to have a lot of redundancy.	
49.	CMVP	Kim Schaffer	4.8.6	T	Security level 2 & 3 appears to redefine zeroization from levels 1. This should be used the same way throughout the standard.	
50.	Cryptsoft	Tim Hudson	4.8.6	T	"authentication proxies" This term is introduced with no definition or context. More elaboration is required or the term should be removed. This is the only reference to proxies within FIPS140-3.	
51.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.8 Sensitive Security Parameter Manage-ment**, Paragraph 5	T	Why would hash values of passwords be considered CSPs since hash values are one way computations? Recommend not identifying hash values of passwords as CSPs.	

52.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.8**, **4.8.3 Sensitive Security Parameter Establish-ment**, SECURITY LEVELS 3 AND 4, Paragraph 1	T	Why would SSPs, especially public keys, need to be transported over a Trusted Channel? Suggest removing the requirement that all SSPs shall be transported over a Trusted Channel.	
53.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.8**, **4.8.4 Sensitive Security Parameter Entry and Output**, Paragraph 9	T	Why cannot secret or private keys be entered into or output from the module in plaintext form? This paragraph seems to state this since it covers all other SSPs. Suggest removing this paragraph.	
54.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.8**, **4.8.4 Sensitive Security Parameter Entry and Output**, SECURITY LEVELS 3 AND 4, Paragraph 1	T	Why would all SSPs necessarily need to be entered or output over a Trusted Channel? Suggest removing the first paragraph.	
55.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.8**, **4.8.4 Sensitive Security Parameter Zeroization** Paragraphs 1 to 5	T	Good specification of zeroization requirements -- None	
56.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.8**, **4.8.4 Sensitive Security Parameter Zeroization** SECURITY LEVEL 1, Paragraph 1	T	Zeroization of CSPs should be done by the cryptographic module. Suggest removing the paragraph.	

57.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.8**, **4.8.4 Sensitive Security Parameter Entry and Output**, SECURITY LEVELS 2 AND 3, Paragraph 1	T	Temporary PSPs should not need to be zeroized. Suggest changing “SSPs” to “CSPs” in the statement “Temporary SSPs shall be zeroized when they are no longer needed.”	
58.	IBM Research, Zurich	Visegrady, Tamas	**4.8.3**		While confidentiality requirements of SSPs differ based on their external transport form (4.8.3), one may question the differentiation between electronically and non electronically transported CSPs. While operational procedures may externally differentiate between the origin of CSPs, modules themselves are probably unable to recognize the difference. While we realize the difference between clear keyparts and electronically transported keys, we propose to mandate encrypted transport of _all_ CSPs, without special considerations for manually transported ones. Note that clearkey transport of even split-knowledge CSP transport may compromise the entire CSP, even if transport is compliant with section 4.8.3. As a practical example, host administrators can easily capture--therefore, reassemble--all clearkey CSPs just before the module boundary. (It is not a coincidence that the IBM split-key transport implementation encrypts CSP-parts in transit.)	
59.	IBM Research, Zurich	Visegrady, Tamas	**4.8.3**		We consider a _mandatory_ trusted channel requirement inadequate. While a direct physical connection through trusted channel is useful, there are end-to-end alternatives which may be implemented. We do not dispute the security based on physical control of the trusted channel. However, a hardware security module may establish end-to-end security between itself	

					and its controlling officers, and be managed through this channel. In such an environment, the module may be safely deployed and managed, with any "shortcuts" through a trusted channel. Note that IBM security modules feature locally connected ports which may implement trusted channels, but our main usage is assisted by end-to-end security, and works without requiring trusted channels.	
60.	InfoGard		Section 4.8.3, Paragraph 1	G	AES key wrapping (key transport form of key establishment) is listed as a Security Function in Annex B. The distinction between Security Functions in Annexes A and B and SSP Management Techniques in Annexes C and D could use clarification; maybe A and B refer to cryptographic primitives and C and D refer to higher level protocols.	
61.	InfoGard		Section 4.8.3, Paragraph 1	E	This paragraph requires clarification/rewording; in particular the third and fourth sentences. The first sentence states that SSP establishment consists of (1) SSP transport or (2) SSP agreement. This is again reiterated in the third sentence where it states the following: "SSP establishment may be performed by electronic SSP establishment methods (i.e., using SSP transport or SSP agreement schemes)." This seems like a redundant sentence. Suggested text: *"SSP establishment may consist of SSP transport followed by SSP entry or output, or it may consist of an SSP agreement process. The SSP transport process may be manual or electronic. All electronic SSP establishment methods employed in an Approved mode of operation shall be Approved or Allowed for use in an Approved mode listed in Annex C*	

					and D."	
62.	InfoGard		Section 4.8.3, Levels 3 & 4	E	The text surrounding Trusted Channel appears to be referring to the External Trusted Channel, but there are two Trusted Channel types (refer to Section 2.1). Suggest rewording the text of the 3rd and 4th sentences as follows: *"Other than when first establishing a Trusted Channel, SSPs shall be transported over the Trusted Channel, whether or not they are otherwise cryptographically protected. The External Trusted Channel shall use only Approved or Allowed security functions."*	
63.	InfoGard		Section 4.8.3, Levels 3 & 4	T	Are manually transported CSPs required to go through a Trusted Channel or is this only applicable to electronically transported CSPs? The way the paragraph is written, this is unclear. Suggest rewording the text as specified in Item 56.	
64.	InfoGard		Section 4.8.3	T	We consider a mandatory Trusted Channel requirement inadequate. While a direct physical connection through the Trusted Channel is useful, there are end-to-end alternatives which may be implemented and provide equivalent protection. We do not dispute the security based on physical control of the Trusted Channel; however, a hardware security module may establish end-to-end security between itself and its controlling officers, and be managed through this channel. In such an environment, the module may be safely deployed and managed, with any "shortcuts" through a Trusted Channel. An example: IBM security modules feature	

					locally connected ports which may implement Trusted Channels, but our main usage is assisted by end-to-end security, and works without requiring Trusted Channels. Require that a Trusted Channel be supported, or something equivalent; end-to-end protection that provides confidentiality, data integrity, and non-repudiation.	
65.	InfoGard		Section 4.8.4, Paragraph 6	T	"To prevent the inadvertent output of sensitive information, two independent internal actions shall be required in order to output any CSP." Where is this applicable (manual output, electronic output, plaintext, cipher, split knowledge)? Clarification is required.	
66.	InfoGard		Section 4.8.4, Paragraph 7	T	"PSPs and CSPs that are not secret or private keys…may be entered into or output from a module in plaintext form." Is this general requirement for all levels? If this was only meant for Levels 1 and 2, it should be categorized as such.	
67.	InfoGard		Section 4.8.4, Paragraph 8	T	"PSPs do not need to be cryptographically authenticated regardless of whether they are entered manually or electronically." What does this mean? Clarification is required.	
68.	InfoGard		Section 4.8.4, Levels 3 & 4, Paragraph 1	E	The requirement for using a Trusted Channel is redundant with the interface section. This section also does not specify whether it is referring to Internal or External Trusted Channels. The last sentence stating that the Trusted Channel "shall use only Approved or Allowed security functions" implies that this is referring to the External Trusted Channel. Suggest rewording the last sentence as follows: *"The External Trusted Channel shall use only Approved or Allowed security functions."*	

69.	InfoGard		Section 4.8.4, Levels 3 & 4, Paragraph 2	T	It's not clear how the second paragraph and the first paragraph complement each other. The second paragraph provides three options for entering secret and private keys. Regardless of which option is selected, the key must also go through a Trusted Channel. Suggest rewording the 2nd paragraph as follows: *"Secret and private keys shall be entered into or output from the module through a Trusted Channel using either one of the following methods:* • *Encrypted* • *Plaintext through an Internal Trusted Channel* • *Plaintext using split knowledge procedures (i.e., as two or more plaintext components)".*	
70.	InfoGard		Section 4.8.5	T	This section should be more specific about Approved/Allowed encryption (or any other restriction) for encrypted SSP storage. Suggest adding the following new sentence after the first sentence in the first paragraph: *"Encrypted SSPs shall use only Approved or Allowed security functions."*	
71.	InfoGard		Section 4.8.6, Levels 2 & 3	T	Should this section be clearer about what is acceptable zeroization practice? For example, zeroization by power cycle, if RAM is not actively overwritten. This section cites "overwriting", but this is a weak statement as is.	
72.	InfoGard		Section 4.8.6, Paragraph 1	E	"A module shall provide methods to zeroize all CSPs within the module." This statement doesn't appear accurate, as the requirement here is level dependent. Clarify; be explicit.	
73.	InfoGard		Section 4.8.6, Paragraph 2	E	Why is this paragraph referencing SSPs? Replace SSP with CSP.	

74.	InfoGard		Section 4.8.6, Paragraph 3	E	This statement is not entirely true, as Level 4 requires zeroization of encrypted CSPs. Delete encrypted CSPs.	
75.	InfoGard		Section 4.8.6, Paragraph 3	T	The Level 4 requirements under this section state that the module should go back to a factory state. So is it required that PSPs and CSPs stored in another validation module also be zeroized? Clarification is required.	
76.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.8.3	T	Requiring "Electronically transported CSPs shall be in encrypted form" may, as previously stated, prevent NIST endorsed product from being used to protect Type 2 information in a NSS. Rationale: Make sure that NIST certified products can be used to protect unclassified NSS.	
77.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.8.6	T	For Security Levels greater than 1add the following requirement, "The zeroization process shall be verified by reading the zeroized security parameter. If the zeroization verification fails, the cryptographic module shall provide the operator with a status indicator and prevent secure operation. Rationale: If the cryptographic memory containing a security parameter isn't zeroized, then the operator should be notified of the possible insecure state of the module.	
78.	Motorola	Jan Hintermeister	4.8.3	G	How is manually tranported defined? Manual entry is defined as keyboard entry. Does manual transport cover both entry when directly connected to the module as well as from keyboard entry over a network connection to the module? The glossary carefully distinguished between electronic entry and electronic transport. Is a similar distinction required for manual entry and transport, or are manual entry and	

					tranport considered the same?	
79.	Motorola	Jan Hintermeister	4.8, 5th paragraph	G	Hash values of passwords are identified as CSPs. Given that the hash value is a cryptographically protected form of the password, are the constraints in 4.8.4 (e.g. two independent actions etc.) necessary for hash values? This is a general question for all cryptographically protected CSPs. In a similar vein, encrypted CSPs were exempted from the zeroization requirement in Section 4.8.6. Does this section apply to hash values?	
80.	NSA	TWG	4.8.5	T	Suggest adding the following requirement: SSPs stored within a module should be stored in a section of memory or component dedicated to the storage of SSPs and any associated integrity or data tags.	
81.	NSA	TWG	4.8	T	We are concerned that the current description of what constitutes an SSP, together with the wording on the usage of an RBG in an Approved mode (Section 4.8) is unnecessarily restrictive and likely to place undue difficulties on vendors to meet the perceived requirements. Random Bit Generators are an essential piece of many cryptographic algorithms, providing the secret values upon which their security is based. Used in this role, their outputs must be regarded as Critical Security Parameters, as should their input ("seeds") in the case of a DRBG. There are other uses for RBGs in algorithms, however, where the protections afforded a CSP or even a PSP, are not required for security. Examples of these may include Initialization Vectors (IVs) for symmetric ciphers; "numbers used once" (nonce) values to prevent replay attacks or variability in derived keys; anti-clogging	

					tokens. In particular, we believe that RBG outputs that are visible across a transport network ought **not** to be considered SSPs**.** To provide some clarity on the distinction, we suggest wording similar to the following in Section 4.8: "An RBG used to produce CSPs shall be entirely contained within a cryptographic module boundary. Outputs of any RBG which will become visible on a transport network are not treated as SSPs once outside the cryptographic module. RBGs which are never used to provide CSPs are not required to be Approved". **Highlighted** (in green) statements in Section 4.8 below are affected by this interpretation of RBGs. **4.8 Sensitive Security Parameter Management** Sensitive Security Parameters (SSPs) consist of Critical Security Parameters (CSPs) and Public Security Parameters (PSPs). The security requirements for SSP management encompass the entire lifecycle of SSPs employed by the module. SSP management includes random bit generators (RBGs) **used to provide CSPs**, SSP generation, SSP establishment, SSP entry/output, SSP storage, and SSP zeroization. A module may contain one or more embedded modules each performing SSP management functions. Encrypted CSPs refer to CSPs that are encrypted using an Approved or Allowed security function. CSPs encrypted using non-Approved and non-Allowed security functions are considered unprotected plaintext within the scope of this standard. CSPs **shall** be protected within the module from unauthorized access, use, disclosure, modification, and substitution.	

					PSPs **shall** be protected within the module against unauthorized modification and substitution. Keys used for self-tests specified in Section 4.9 are not considered SSPs. Hash values of passwords, RBG state information and intermediate key generation values **shall** be considered CSPs. Documentation **shall** specify all SSPs employed by a module. **4.8.1 Random Bit Generators** A cryptographic module may contain RBGs, a chain of RBGs, or may be solely an RBG. All RBGs **used to provide CSPSs** and their usage **shall** be defined and documented. All RBGs **used to provide CSPs** in an Approved mode **shall** be Approved or Allowed and listed in Annexes A or B. If entropy is collected from outside the cryptographic boundary of the module, the datastream generated using this entropy input **shall** be considered a CSP, and the module documentation **shall** specify the minimum entropy required by the module for each entered entropy input parameter. If the entropy is collected from within the cryptographic boundary of the cryptographic module, the minimum entropy and the generation method of the claimed minimum entropy **shall** be documented. **4.8.2 Sensitive Security Parameter Generation** A module may generate SSPs internally or they may be entered into the module. Documentation **shall** specify each SSP generation method employed by a module. Any SSPs generated in the Approved mode of the module using an RBG **shall** be generated using an Approved or Allowed RBG meeting	

					the requirements specified in Section 4.8.1. Compromising the security of the SSP generation method (e.g., guessing the seed value to initialize the deterministic RBG) **shall** require as least as many operations as determining the value of the generated key. Documentation **shall** specify each SSP generation method that makes use of an RBG. SSPs generated by the module for use by an Approved or Allowed security function or key establishment technique **shall** be generated using an Approved or Allowed SSP generation method listed in Annexes C and D. If random values are required **for an SSP** in an Approved or Allowed security function(s), then an Approved or Allowed RBG **shall** be used to provide these values. Additionally, in section 2.1, initialization vectors as an example of security parameters should be removed from the definition of "Key Management".	
82.	NSA	TWG	4.8.1	T	The sentence "If entropy is collected from outside the cryptographic boundary of the module, the data stream generated using the entropy shall be considered a CSP…" is a little confusing at first glance. We're assuming that by the data stream, one means the stream that is then **input** into the RBG not output, correct?	
83.	NSA	TWG	4.8.6	E	Need an adverb: "…operator, and independent**tly** of the module's control…" under security level 1.	
84.	NSS Project	Wan-Teh Chang	Section 4.8.4, first paragraph of page 41.	Technical	"For software modules, CSPs may be entered into or output from the module in either encrypted or plaintext for under control of the module operating system provided that the CSPs are maintained within the operational environment." It's a common practice for software vendors to	

					isolate the cryptographic and key management functions of their products in a shared software crypto module and just validate the shared software module. If a software module allows plaintext secret and private keys to flow out of the module, the products using the module will be burdened with the proper handling of plaintext keys, and therefore the products will be subject to some of the OS access control and SSP management requirements of FIPS 140-3. So this relaxed requirement seems at odds with the common practice of validating a shared software crypto module instead of individual products. If a product uses a software crypto module that allows plaintext keys to be exported into the product, it seems that the product should also be validated for its access control and management of the plaintext keys.	
85.	Orion	MS	Section 4.8, last line	T	"Document shall specify all SSPs employed by the module." This may be difficult to do in detail since modification of all software and all parameters within the module might lead to a security compromise. More guidance is needed as to what needs to be specified as a PSP. Provide more guidance as to what constitutes a PSP.	
86.	Orion	MS	Section 4.8.1, last sentence	E	"If the entropy is collected from within the cryptographic boundary of the cryptographic module, the minimum entropy of the generation method of the claimed minimum entropy **shall** be documented". This seems awkward to me. Consider "If the entropy is generated within the cryptographic boundary of the module, then the minimum entropy produced by the generation method **shall** be documented."	

87.	Orion	MS	Section 4.8.2, third paragraph beginning with “SSPs generated by the module…”	T	Annexes C & D only cover key establishment techniques. Annexes A & B should be included to cover Approved and Allowed security functions. For example, the generation of a DSA key would not be covered in Annexes C & D. Change “Annexes C and D” to “Annexes A and B or Annexes C and D, respectively”. Alternatively break this up into two separate requirements; one for security functions and one for key establishment.	
88.	Orion	MS	Section 4.8.3, first sentence	E	Generally, SSP transport is thought of as including the output of the encrypted transported key from one module and the input of the encrypted transported key into the other module. Therefore, it is not necessary to mention the input and output as separate processes. Change to read: “SSP establishment may consist of either an SSP transport process or an SSP agreement process.”	
89.	Orion	MS	Section 4.8.3, Security Levels 1 and 2	E/T	CSP should be plural. Also, this requirement may be thought to imply that an encrypted CSP is a CSP. Encrypted CSPs can always be transported since the are not CSPs. Change to “CSPs may be manually transported.”	
90.	Orion	MS	Section 4.8.4, paragraph 7	T	“PSPs do not need to be cryptographically authentication regardless of whether they are entered manually or electronically.” Though true, this statement can give the false impression that PSPs do not need protection outside of the module. PSPs do require protection. For example, consider a public-key. The protection may be physical or cryptographic. Whether the key is entered or output electronically or manually is irrelevant. Change to read: “Upon entry and output, PSPs **shall** be protected from unauthorized	

					modification either cryptographically by an Approved keyed integrity mechanism or physically." Note that although the scope is only the module, we still have entry and output requirements on PSPs just as we do with CSPs.	
91.	Orion	MS	Section 4.8.5, "Documentation **shall** specify	T	"Documentation **shall** specify: …How the module associated a PSP stored in the module with the entity (operator, role, or process) to which the parameter is assigned." This requirement should apply to CSPs as well. Change "PSP" to "SSP".	
92.	Orion	MS	Section 4.8.6, first paragraph	T	This paragraph implies that temporarily stored values (e.g., entropy input, RBG states, and shared secrets) are not CSPs since they are separately mentioned with CSPs. Yet by the definition of CSP, they are all CSPs. Change text to just zeroize CSPs since these other values are also CSPs. The could be given as examples of CSPs.	
93.	Orion	MS	Section 4.8.6, fourth paragraph	E	Critical terms should be defined. Define "authentication proxies" and "module initialization key".	
94.	Orion	MS	Section 4.8.6, Security Levels 2 and 3, second sentence	T	"Zeroization **shall** exclude the overwriting of the CSP with another CSP." By placing this requirement at L2 and L3, it seems to imply that it is OK to overwrite with a CSP at L1. This seems to run counter to the point of zeroization. Move this requirement to Level 1.	

95.	Orion	MS	Section 4.8.6, Security Level 4.	T	"The zeroization **shall** be immediate and non-interruptible and **shall** occur in a sufficiently small time period …." This requirement seems to be at the wrong level. Certainly Level 3 modules with removable covers and doors should employ immediate and non-interruptible zeroization. Move this requirement to level 3.	
96.	Orion	MS	Section 4.8.6, Security Level 4, last sentence	T	"All CSPs **shall** be zeroized whether in plaintext or cryptographically protected…. This implies that encrypted CSPs are CSPs which should not be the case. Even if the desire is to be conservative by zeroizing encrypted CSPs the text should be revised. See suggested change. "All CSPs and encrypted CSPs **shall** be zeroized such that …"	
97.	Orion	MS	Section 4.8.6, Security Level 4, last sentence	T	"…such that the module is returned to the factory state." "factory state" is not defined. Either define "factory state", or better yet, write the text as follows: "Upon zeroization, all CSPs and Encrypted CSPs **shall** be zeroized.	
98.	Thales e-Security		4.2.3, 4.8.3, 4.8.4 Trusted Channel	T	The Trusted Channel does not allow for either the initial commissioning of a unit or the fact that not all data is required to be protected from disclosure (for example a Public Security Parameter or status outputs such as an LED interface.) Additionally it is hard to see how it would be applied to (i) physically protected point to point channel into the crypto module e.g. key fill interface for red key (ii) remote server distributing already encrypted and signed black key. i.e. Authentication and protection for Black Key packages is already provided	

					using strong encryption and signature and therefore does not need a 'trusted channel'. Regarding the requirement for the port to be dedicated: The use of a Trusted Channel renders the physical nature of the interface irrelevant. Therefore the interface can be shared for other activities.	
99.	Thales e-Security		4.4, 4.8.6	T	Verification keys (PSPs) are used to authenticate Software/Firmware/Keys, and these must be preserved through zeroisation to allow units to be updated. Operationally, however, specific examples exist where root keys should be maintained through zeroisation to protect against malicious modification of software or code by loading a rogue verification root key; the standard should not preclude this.	
100.	Thales e-Security		4.8.1	T	RNG - Hardware noise source How is the strength of the noise source measured? Does one bit of entropy count for each bit output from the rng? Clarification is required.	
101.	Thales e-Security		Glossary, 4.8.4, 4.8.5	T	There are inconsistent integrity requirements for PSPs in the publication. The Glossary defines PSP as any security-related public information whose modification can compromise the security of a cryptographic module. Therefore their integrity must be maintained. Section 4.8.4 states that PSPs may be entered or output from the module in plaintext form and that PSPs do not need to be cryptographically authenticated. By contrast: Security Levels 3 and 4 in this section state that a Trusted Channel should be used for all SSPs, and section 4.8.5 which covers SSP storage states that PSPs must be protected	

					from unauthorised modification and substitution. The apparent inconsistent requirements for PSPs in their lifecycle should be resolved.	
102.	NIST	Elaine Barker	4.8.1, second para		"If entropy input is collected from outside the cryptographic boundary of the module, the datastream generated using this entropy input **shall** be considered a CSP, and the module documentation **shall** specify the minimum entropy required by the module for each entered entropy input parameter. If the entropy is collected from within the cryptographic boundary of the cryptographic module, the minimum entropy and the generation method of the claimed minimum entropy **shall** be documented. " Change the text to: "If entropy input is collected from outside the cryptographic boundary of the module, the entropy input **shall** be considered a CSP, and the module documentation **shall** specify the minimum entropy required by the module for each entered entropy input parameter request (?). If the entropy input is collected from within the cryptographic boundary of the cryptographic module, the minimum entropy and the generation method of the claimed minimum entropy **shall** be documented. " Probably need to document the method for providing the entropy input to the module (e.g., using a trusted channel).	

					John Kelsey and the rest of the X9.82 team probably need to look at this section closely.	
103.	NISt	Elaine barker	4.8.3, first para		"SSP establishment may consist of SSP transport followed by SSP entry or output, or it may consist of a SSP agreement process. The SSP transport process may be manual or electronic. SSP establishment may be performed by electronic SSP establishment methods (i.e., using SSP transport or SSP agreement schemes). All electronic SSP establishment methods employed in an Approved mode of operation **shall** be Approved or Allowed for use in an Approved mode listed in Annexes C and D. " Replace the text above with: "SSP establishment may be the result of transport or agreement processes. The SSP transport process may be manual, electronic or automated. The manual and electronic transport of SSPs will result in the entry or output of SSPs in plaintext or encrypted form, depending on the Security Level and application requirements; during automated SSP transport, the SSPs are entered and output from the module in encrypted form. The SSP agreement process is automated; the entry and output values depend on the specific agreement technique. All automated SSP management techniques	

					employed in an Approved mode of operation **shall** be Approved or Allowed for use in an Approved mode listed in Annexes C or D. “ 1. A definition of “automated” might be necessary. 2.“Electronic” which is used in the original text has a different meaning – see next section	
104.	NIST	Elaine Barker	4.8.3, Para 4		“Electronically transported CSPs **shall** be in encrypted form. The integrity of all electronically transported SSPs **shall** be cryptographically protected (e.g., by an Approved or Allowed security function or an Approved or Allowed key establishment method). “ Change above text to : “CSPs transported using automated techniques **shall** be in encrypted form. The integrity of all SSPs transported using automated technoques **shall** be cryptographically protected (e.g., by an Approved or Allowed security function or an Approved or Allowed SSP management technique). “	
105.	NIST	Elaine Barker	4.8.3, LS 3&4		“Manually transported CSPs shall be either in encrypted form or split into components (see Split Knowledge). Electronically transported CSPs **shall** be encrypted. Other than when first establishing a Trusted Channel, SSPs **shall** be transported electronically over	

					the Trusted Channel, whether or not they are otherwise cryptographically protected. The Trusted Channel **shall** use only Approved or Allowed security functions." Change text to: "Manually transported CSPs **shall** be either in encrypted form or split into components (see Split Knowledge). Electronically transported CSPs and CSPs transported using automated techniques **shall** be encrypted. Other than when first establishing a Trusted Channel, SSPs **shall** be transported electronically over the Trusted Channel, whether or not they are otherwise cryptographically protected." And using automated techniques? I don't know if it's required. Need to think about this.	
106.	NIST	Elaine Barker	4.8.4, para 4		"All cryptographically protected SSPs, entered into or output from the module and used in an Approved mode of operation, **shall** be encrypted using an Approved or Allowed security function." Replace SSPs with CSPs	
107.	NIST	Elaine Barker	4.8.4, para 8th		"PSPs do not need to be cryptographically authenticated regardless of whether they are entered manually or electronically. " The integrity may need to be checked. What about entered or output using automated techniques?	

108.	NIST	Elaine Barker	4.8.4, (split knowledge)		"At least two components **shall** be required to reconstruct the original CSP." Do we need to say anything here about PSPs?	
109.					"Plaintext CSPs may be entered and output via physical port(s) and logical interface(s) shared with other physical ports and logical interfaces of the cryptographic module. Input and output of CSPs over unencrypted wireless connections is not allowed. " Automated techniques should be allowed.	
110.	NIST	Elaine Barker	4.8.4 (bullets)		• Encrypted • Plaintext using a dedicated physical port • Plaintext using split knowledge procedures (i.e. as two or more plaintext components) Include automated techniques in this list?	
111.	NIST	Elaine Barker			"A module **shall** provide methods to zeroize all CSPs within the module. Temporarily stored values (e.g. entropy input, RBG state, shared secret used in a key establishment mechanism, etc.), key components owned by the module and CSPs should be zeroized when they are no longer needed for future use" Replace "should" by "shall"? In the case of RBGs, I think this is already handled.	

112.	NIST	Elaine Barker	4.8.5, para 5		"SSPs need not meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key). " Don't understand.	
113.	NIST	Elaine Barker	4.8.6		Define "factory state".. This may not be desirable if the factory state is considered to be a default key, which shouldn't be used.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Fiona Pattinson	4.9 4th para	E	This paragraph seems to be mis-positioned within the section. It would more logically appear after the 7th paragraph.	
2.	atsec	Fiona Pattinson	4.9 5th para	T	It is not clear what an “algorithmic standard” might include. The term “security functions” is used elsewhere in the standard. Using the term “algorithmic standard” may mean that self tests for some security functions not strictly defined as “algorithms” to not be implemented.	
3.	atsec	Helmut Kurth	4.9.1.1	E	The first sentence gives the impression that Section 4.4 specifies the “Approved integrity techniques” that are allowed to be used for the pre-operational software/firmware integrity test. Instead Section 4.4 specifies in detail how an Approved integrity technique can be used for software/firmware integrity tests.	
4.	atsec	Helmut Kurth	4.9.2.3 first bullet	T	The requirement states: “When the applied Approved digital signature technique is used, requirements in clause 4.9.2.1 shall also be met.” The purpose of the reference to 4.9.2.1 (Conditional Cryptographic Algorithm Self-Test) is unclear. Does this require performing an algorithm self-test for the Approved digital signature function before verifying the signature of the code loaded? We would rather expect a reference to Section 4.3.3.2 (Software or Firmware Loading) Clarify the purpose of the reference to 4.9.2.1. Add a reference to Section 4.3.3.2.	
5.	atsec	Peter Kim	4.9.2.1	G	The type of test is not defined, which implies it does not need to be a Known Answer Test as traditionally required. Please clarify.	

6.	atsec	Peter Kim	4.9.2.2	G	The method by which to perform the pairwise consistency test is not defined. Please define how a pairwise consistency test is to be performed.	
7.	atsec	Peter Kim	4.9.2.3	G	The Software/Firmware Load Test identifies only an Approved digital signature technique as being appropriate for the test. This is in conflict with the fourth bullet of Section 4.3.3.2. Please clarify whether any Approved data authentication technique is permitted or if modules will not be restricted to digital signatures for software/firmware load tests.	
8.	brightsight	Lex Schoonen	4.9	T	It is worth noting that the self-test mechanisms mandated by these paragraphs should not be susceptible to any of the attacks in previous subsections. It is not uncommon that self-tests are programmed in a way that makes them very susceptible to fault injection or side channel attacks.	
9.	Cisco		4.9	T	Please confirm, are there any additional requirements around status output for a degraded mode of operation? Specifically, is a single status output when degraded mode of operation is enabled acceptable or does the output have to be ongoing? Please clarify the requirements.	
10.	Cisco		4.9.2.3	T	Will the Conditional Software/Firmware Load Test apply to interpreted software elements, such as, TCL Scripts? Please clarify if the requirement applies to interpreted software elements. Recommendation: No the test does not apply to interpreted software elements	
11.	Cisco		4.9.3	T	The following requirement: “At Security Levels 1 and 2, a cryptographic module shall permit operators to initiate the pre-conditional and conditional self-tests on	

					demand for periodic testing of the module" seems to indicate that the module is required to be able to perform conditional tests on demand. It is not clear how this would apply to tests such as the conditional load test that require an external input to be performed. Please clarify how this requirement applies to conditional load tests. Recommendation: the requirement for conditional tests should be removed.	
12.	CSEC	Claudia Popa	4.9	G	Page 42 "All self-tests identified in addition or lieu of those specified in the underlying algorithm standards (Annexes A through E) shall be implemented as specified in Annexes A through E for each cryptographic algorithm." None of these Annexes have any self-test requirements. These annexes only refer to an Implementation Guidance document that was not provided.	
13.	CSEC	Claudia Popa	4.9.	T	Page 43 "If a module does not output an error status upon failure of a module self-test, the operator of the module shall be able to determine if the module has entered an error state through a procedure documented in the Security Policy." This statement is very general and provides a way in which the vendors could go around without implementing a proper error status indicator.	
14.	CSEC	Claudia Popa	4.9.1.2	E	Page 43. Replace "verify" in the two bullets with "verifying".	
15.	CSEC	Claudia Popa	4.9.2	T	4.9.1.2 describes the pre-operational bypass test, and 4.9.2.5 describes the conditional bypass test. Does a module have to perform the bypass test before becoming operational and before a	

					bypass operation?	
16.	CSEC	Claudia Popa	4.9.2.1 and 4.9.2.2	G	Annexes A through E does not include any self-tests requirements.	
17.	CSEC	Claudia Popa	4.9.2.3	E	First sentence, first bullet, "… digital signature shall be applied to all the **validated** software or firmware…" Is the second sentence needed? The first sentence already requires that the code should be validated.	
18.	CSEC	Claudia Popa	4.9.2.3	G	Second bullet- "Loaded software or firmware shall not be used if the Software/Firmware Load Test fails". Is this requirement actually saying that the module shall enter an error state and it shall not be operational?	
19.	CSEC	Claudia Popa	4.9.3	G	Security Level 1 and 2. "Acceptable means for the on-demand initiation of periodic self-tests are: resetting, rebooting, and power." The way this is worded it suggests that these are the ONLY acceptable methods. If the sentence is changed, like provided below, the meaning is already different. Resetting, rebooting, and power up, are acceptable means for the on-demand initiation of the periodic self-tests.	
20.	CSEC	Jean Campbell	4.9.2	E	Why don't use a "bullet" form for the list?	
21.	CSEC	Jean Campbell	4.9.2.1	G	Do we want to keep the requirement: "If a cryptographic module includes two independent implementations of the same cryptographic algorithm, then the module	

					shall continuously compare the outputs of the two implementations, and, if the outputs of the two implementations are not equal, the cryptographic algorithm test **shall** fail."	
22.	CSEC	Jean Campbell	4.9	G	Page 42 "The module **shall** provide a status indication when it is operating in a degraded mode of operation. It is desirable for the module to indicate the conditional self-test(s) that failed". Why don't have this requirement in the section 4.1.3.2 Degraded Mode of Operation?	
23.	CSEC	Jean Campbell	4.9.2.5	G	Last paragraph of section 4.9.2.5 refers to "Approved integrity technique". Should a reference to a list of integrity techniques be provided?	
24.	CSEC	Jean Campbell	4.9.3	G	"At Security Levels 3 and 4, the module vendor **shall** specify a critical time period that identifies the maximum operational time before self-tests must be repeated and any conditions associated with repeating these self-tests." Shouldn't the module implement this self-test?	
25.	CMVP	Kim Schaffer	4.9	T	Depending on the module's use, it may or may not be "… desirable for the module to indicate the conditional self-test(s) that failed"	
26.	CMVP	Kim Schaffer	4.9.1.1	T	I believe that any code stored in non-reconfigurable memory must be firmware or I don't understand this exception.	
27.	CMVP	Kim Schaffer	4.9.1.2	T	This should be internally tested and outputs should be disconnected or similar.	
28.	CMVP	Kim Schaffer	4.9.2.2	E	This needs to be reworded for clarity, I am confused about public or private key pairs and is there a procedural difference for encryption/decryption and signing/verifying. Perhaps that is described elsewhere.	

29.	CMVP	Kim Schaffer	4.9.2.3, end of first bullet	E	"…requirements in clause 4.9.2.1 shall also be met." can be confusing, perhaps " requirements in clause 4.9.2.1 are also met."	
30.	CMVP	Kim Schaffer	4.9.2.4	T	Does 32 bit EDC provide enough confidence over 16 bit given that there is a greater likelyhood that manual entry has a significantly greater chance of mis-entry?	
31.	CMVP	Kim Schaffer	4.9.2.5	T	If the requirement is that self tests must be run each time a router table is changed, then this may provide an indication as to when the tables are changed for anyone monitoring the connections. In most cases this will not be significant, but in examples other than the router example provided, it may be more exposure.	
32.	Cryptsoft	Tim Hudson	4.9	T	"If a cryptographic module fails a self-test, the module shall enter an error state and shall output an error indicator as specified in Section 4.2.2. The cryptographic module shall not perform any cryptographic operations or output data via the data output interface while in an error state." The degraded mode of operation is not allowed for in this wording. Either it is acceptable for a self-test to fail and the module continue to operate if the algorithms for that self-test are not required (which is the degraded mode of operation) or it is not. The conflicting wording should be adjusted.	
33.	Cryptsoft	Tim Hudson	4.9.1.1	T	"non-reconfigurable memory" This is a new term being introduced and should be changed to match the existing usage elsewhere in FIPS140-3. Suggested resolution: replace with "non-modifiable storage"	
34.	Cryptsoft	Tim Hudson	4.9.2.1	T	"two independent" and "two implementations" unnecessarily limits the requirement to a two implementations when there may indeed be many more than two implementations	

					contained within a single cryptographic module. Suggested resolution: replace “two independent” with “multiple independent” This assumes the requirement remains comparison of any two if the multiple implementations rather than all of the implementations.	
35.	Cryptsoft	Tim Hudson	4.9.3	E	“rebooting, and power” Suggest resolution: “rebooting, and re-powering”. (matching the use of the term re-powering in section 4.9)	
36.	DOMUS		4.9, 4th paragraph, 2nd sentence	G	The requirements states: It is desirable for the module to indicate the conditional self-test(s) that failed“ Proposed resolution: Conditional tests are run while a specific function is called that requires a conditional test is required like generating a random number of generating an asymmetric key pair. The FIPS standard has always allowed the module to try and clear a conditional test error and if the conditional test could not be cleared, the module must enter an error state. The way the requirement reads, it implies that the module must return an error condition without trying to clear the error. I believe the CMVP must make a decision to either: 1) For each conditional self-test error, return an error message and module remains in an error state where all data is inhibited; or Allow the module to try and clear the error up to a maximum of 3 times for which if the error cannot be cleared, enter the error state where all data is inhibited.	

37.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9 Self-Tests**, Paragraph 1	T	The pre-operational self-tests need to be invoked for software. A clarifying statement should be added specifying that it is acceptable for the pre-operational self-tests to be invoked by an operator for a shared cryptographic module library.	
38.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9 Self-Tests**, Paragraph 7	E	There is an extra period (".") after "4.2.2." Suggest removing this period.	
39.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9 Self-Tests**, Paragraph 8, (Security Levels 3 and 4)	T	It is excessive to require a cryptographic module to maintain an error log. Suggest removing the requirement for an error log.	
40.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.1.2 Pre-Operational Bypass Test**	T	Verifying that data transferred through the bypass mechanism is or is not cryptographically protected is difficult. Suggest removing this self-test altogether.	
41.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.2.3 Conditional Software/ Firmware Load Test**, Bullet 1	T	It should be possible to use a MAC instead of a digital signature for the Conditional Software/Firmware Load Test since otherwise the vendor is required to implement an asymmetric algorithm which they may not need for anything else. Suggest specifying that keyed MACs are also allowed for the Conditional Software/Firmware Load Test.	
42.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.2.4 Conditional Manual Key Entry Test**, Bullet 2	T	A 32-bit EDC is excessive, especially for a 128-bit AES key. Suggest requiring that EDCs need only be 16 bits in length.	
43.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.2.5 Conditional Bypass Test**, Paragraph 2	T	It is difficult to test for the correct operation of cryptographic services for the exclusive bypass capability. Suggest removing this requirement	.

44.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.2 Conditional Self-Tests**	T	It is noticed that no Continuous Random Number Generator Test has been specified. It is understood that DRBGs have specified self-tests, but what about RNGs still useable and non-Approved RNGs used for entropy for Approved DRBGs or IVs? Suggest requiring a Continuous Random Number Generator Test for all DRBGs or RNGs implemented in the cryptographic module.	
45.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.3 Periodic Self-Tests**, SECURITY LEVELS 1 AND 2, Paragraph 1	E	It should be “pre-operational” not “pre-conditional” self-tests. Suggest changing “pre-conditional” to “pre-operational” in the first sentence.	
46.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.3 Periodic Self-Tests**, SECURITY LEVELS 1 AND 2, Paragraph 1	T	It makes no sense to test conditional self-tests on demand. Perhaps it is meant that it shall be possible to initiate Conditional Cryptographic Algorithm Self-Tests on demand. Suggest changing “conditional self-tests” to “conditional cryptographic algorithm self-tests” in the first sentence.	
47.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.9**, **4.9.3 Periodic Self-Tests**, SECURITY LEVELS 3 AND 4, Paragraph 1	G	What is preventing a vendor from specifying a critical time period of many years? Perhaps this should be a recommendation, not a requirement, or a maximum critical time period of a year could be specified. Suggest specifying a maximum critical time period.	
48.	IBM Research, Zurich	Visegrady, Tamas	**4.9.3**		We consider a mandatory requirement for periodic selftests overkill. Given enough error-checking coverage, a module may be sufficiently protected with on-demand selfchecks. As an example, request-driven stateless modules, which also perform continuous tests, would benefit little from an internally invoked	

					periodic test. In such environments, there is implicit checking on a per-request basis, and periodic selftests do not gain additional value, as hardware failures would be detected when a request is submitted. We propose to remove the unconditional periodic requirement, if comprehensive continuous testing (redundancy, or similar alternatives) protects against components failing.	
49.	InfoGard	Section	4.9.1.3	G	The definition or examples of critical functions have always been a little light; more specific scenarios should be provided (e.g., RSA used for key wrapping should have a test associated with it even if it's not a FIPS Approved algorithm and does not require an algorithm KAT).	
50.	InfoGard		Sections 4.9.1.3 & 4.9.2.6	E	"There may be other security functions critical to the secure operation of a cryptographic module that shall be tested …" This should be more strongly worded. Suggested text: "Other security functions defined by the vendor as critical to the secure operation of a cryptographic module shall be tested…"	
51.	InfoGard		Section 4.9.3	T	In some products, a mandatory requirement for periodic self-tests may not be acceptable; in particular, the cryptographic devices seen in the health industry (e.g., cryptographic transmitter for pacemakers). Given enough error-checking coverage, a module may be sufficiently protected with on-demand self-checks. We propose to remove the unconditional periodic requirement, if comprehensive continuous testing (redundancy or similar alternatives) protects against components failing.	

52.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.9	E	In the second line of the last paragraph on page 42 change “as specified in Section 4.2.2. .” to “as specified in Section 4.2.2. .”. Rationale: Correct typo	
53.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.9	T	The first three lines of the last paragraph state “If a cryptographic module fails a self-test, the module shall enter an error state and shall output an error indicator as specified in Section 4.2.2. . The cryptographic module shall not perform any cryptographic operations or output data via the data output interface while in an error state.” This should be changed to “If a cryptographic module fails a self-test, the module shall enter an error state and shall output an error indicator as specified in Section 4.2.2. . The cryptographic module shall not perform any cryptographic operations or output data via the data output interface that depends on the failed portion of the cryptographic device while in an error state.” Rationale: Cryptographic devices can be built to identify failed components and verify that one or more security functions may still be provided securely. For instance a cryptographic device that uses multiple FPGA based cryptographic engine physical interfaces to protect multiple physical interfaces, where one FPGA is dedicated to each physical interface, may be able to continue providing security services for physical interfaces supported by still “healthy” FPGAs and shut down the interface(s) for FPGAs that continuously fail their self-tests. In addition, NISTs responses to comments on the last FIPS 140-3 draft, contained in file CommentsFIPS140-3_draft1.pdf, ID# 94, Init J.C. accepted my comment on the previous draft that stated “Paragraph 4.1.4 allows the operation of cryptographic functions that have	

					passed their self-tests independent of another cryptographic function that has failed its self-test. The third requirement in second paragraph expressly prohibits any cryptographic operation when in an error state (self-test failure). These two paragraphs appear to contradict each other." accepted the comment and stated the text would be modified. Modern and complex SoC, multichip modules and other solutions can identify and isolate failing components from healthy components and these designs should be allowed to provide high quality/assurance security solutions for those portions of the system that are still securely operating!	
54.	Motorola	Ashot Andreasyan	4.9.2.4	G	The manual key entry tests do not include a check for minimum key length (e.g. for an authentication algorithm that uses HMAC). Should the module enforce the key length of manually entered keys or can this be done procedurally?	
55.	Motorola	Ashot Andreasyan	4.9.2.5, 2nd and 3rd paragraphs	G	It isn't clear what tests are required when a module switches between clear and secure processing (e.g. is it sufficient to verify that the output after crypto processing is different than the input?). Please clarify.	
56.	NSA	TWG	4.9.1	T	Suggest adding a zeroization self-test in the pre-operational tests.	
57.	NSA	TWG	4.9.1	T	Why was the Pre-Operational Self Test Cryptographic Algorithm Test section not carried forward from the 2007 draft?	
58.	NSA	TWG	4.9.2	T	Why was the Conditional Test Continuous RBG Test not carried forward from the 2007 draft?	
59.	NSA	TWG	4.9	E	Have an extra period in "Section 4.2.2..". Bad sentence construction: "The error log shall provide information, at a minimum, the most recent error event (i.e. which self-test	

					failed)". Need a period at end of 3rd bullet.	
60.	NSS Project	Wan-Teh Chang	Section 4.9, last paragraph of page 42.	Editorial	"If a cryptographic module fails a self-test, the module shall enter an error state and shall output an error indicator as specified in Section 4.2.2." Section 4.2.2 does not specify an error indicator. Is the error indicator a part of the status output interface?	
61.	OpenSSL Software Foundation		4.9	T	"If a cryptographic module fails a self test, the module shall enter an error state and shall output an error indicator as specified in Section 4.2.2. The cryptographic module shall not perform any cryptographic operations or output data via the data output interface while in an error state." Refer to comment on 4.1.3.2 – this should allow for degraded mode of operation but the current wording does not.	
62.	Oracle Solaris Security	Darren Moffat	4.4 / 4.9	T	Level 2: In the case of the cryptographic module consisting of multiple operating system binaries each of which provides one or more approved cryptographic algorithms and where some of the algorithms may be optionally installed does the verification failure of any one (optional but approved) algorithm binary signature require the whole cryptographic module to be in the error state or is it acceptable for just that optional algorithm to be disabled and the module not offer it? For example if the evaluated cryptographic module consists of multiple loadable kernel modules in a UNIX system say aes, des, rsa, dsa and one of them fails verification but the others pass can the module continue to provide services in an approved mode but not provide the functionality provided by the kernel module that failed verification ?	

					Section 4.9 seems to imply that operation without the optional components is acceptable.	
63.	Orion	MS	Section 4.9, paragraph 5, second sentence beginning with "All self-tests identified in addition or in lieu…."	E/T	I don't follow this requirement. If a self-test was identified in addition or in lieu of those specified in Annexes A through E, why would it necessarily be "implemented as specified in Annexes A through E? A self-test may have nothing to do with the self-tests of the Annexes. Rewrite to simplify and clarify the requirement.	
64.	Orion	MS	Section 4.9, paragraph 8 beginning with "At Security Levels 3 and 4…"	T	Since this security Level specific text was not proceeded with a heading "SECURITY LEVELS 3 AND 4", I assume that the documentation requirements that follow apply to all levels. Nevertheless, it would be better to move the Level 3 and Level 4 requirement to the end of the section and use an all cap heading. Use an all cap heading for Level 3 and Level 4 requirements at the end of the section.	
65.	Orion	MS	Section 4.9.3, first sentence	T/E	Is "pre-conditional" intended to be "pre-operational"? If not, please define "pre-conditional". Clarify	.
66.	Orion	MS	Section 4.9.3, Periodic Self-Tests, Levels 3 and 4.	T	It would be nice if a Level 4 module would enforce the periodic self-tests or at least provide a warning that they are due to be performed. Consider having a Level 4 module provide a warning that periodic self-tests are due to be performed	.
67.	RSA Security LLC	Kathy Kriese and Peter Robinson	Page 45 section 4.9.3	T	This section indicates pre-conditional and conditional self-tests can be run on demand, while section 4.3.3 (page 24) does not indicate these as available services.	

68.	RSA Security LLC	Kathy Kriese and Peter Robinson	Page 42, Section 4.9, paragraph 7	T	The action on failure of the various types of tests (pre-operational, conditional self-test) appears contradictory. Section 4.9 paragraph 7 indicates if any self test fails the module should enter an error state. This is in contradiction to the degraded mode of operation 4.1.3.2, which appears to allow a single algorithm conditional self-test failure to cause just the failing algorithm to be disabled.	
69.	RSA Security LLC	Kathy Kriese and Peter Robinson	Throughout the document	G	Action on failed pre-operational tests should be explicit.	
70.	SanDisk	Boris Dolgunov	**4.9.1.1 & 4.4**	G	Pre-Operational Software/Firmware Integrity Test mandatory requires “integrity technique as specified in Section 4.4”. Section 4.4 mandatory requires usage Approved digital signature for security levels 3 and 4 and does not allow keyed message authentication code. The security of message authentication functions is not lower than of digital signature functions while they require much less computational power than digital signature functions and therefore can be executed more frequently during run time. Also message authentication function can use different unique key in every device and therefore disable possibility of device cloning. The digital signature functions provide good solution for code distribution and uploading into secure boundary while message authentication functions fit better for the firmware or software code verification inside secure boundary. I suggest allowing message authentication function Pre-Operational Software/Firmware Integrity Test also for level 3 and 4.	
71.	Smart Card Alliance		4.9.1 paragraph 1, and Section	T	**4.9.1 Pre-Operational Software/Firmware Integrity Test states that "**All software and firmware components within the cryptographic	

			2.1		boundary **shall** be verified using an Approved *integrity technique* as specified in Section 4.4." The glossary (section 2.1) defines *Approved integrity technique* as "Approved hash, message authentication code or a digital signature algorithm." The approved integrity techniques as listed in the glossary -- namely “Approved hash, message authentication code or a digital signature algorithm” -- are not suitable for smart card architectures and will lead speed performance issues. Instead, a CRC16, as allowed by FIPS 140-2 standards, matches smart card architectures and should be listed as *Approved integrity technique*.	
72.	Thales e-Security		4.9	T	Self Tests Table 1 lists a requirement at level 3 for pairwise testing of key pairs entered into the module. However section 4.9 does not specify entry requirements. Before key entry the implementation will have been verified through: 1. CAVP Testing 2. Self Test Hence a KAT would be sufficient for this purpose and would be more efficient for low power devices.	
73.	Thales e-Security		4.9.1.2	T	The use of bypass mode to test cryptographic processing may itself create a vulnerability and is contrary to the good design principles of complete separation of these functions. There are other high level methods for achieving the requirement without merging the mechanisms.	

74.	Thales e-Security		4.9.2.1 Conditional Cryptographic Algorithm Self-Test	T	"*If a cryptographic module include two independent implementations of the same cryptographic algorithm, then the module shall continuously compare the outputs of the two implementations,* …" This requirement should not apply where the two implementations are used for different purposes. For example user data encryption and trusted channel encryption i.e. this is only a requirement when a second implementation is specifically designed to check the first implementation.	
75.	Thales e-Security		4.9.3	T	Is it the case that higher security levels are assumed to include all of the requirements from the lower security levels? This is normally the case for FIPS 140 but not specifically stated in the draft.	
76.	NIST	Elaine Barker	4.9 5th ara		All self-tests identified in underlying algorithmic standards (see Annexes A through E) **shall** be implemented as specified by that standard within the cryptographic module. All self-tests identified in addition to or in lieu of those specified in the underlying algorithmic standards (see Annexes A through E) **shall** be implemented as specified in Annexes A through E for each cryptographic algorithm. 1. I assume that this is a loose interpretation of "standard" that includes SPs. 2 This could be a problem, since a test in the underlying standard is probably important 3. Will the annexes identify the additional tests?	
77.	NIST	Elaine Barker	4.9.1.1		"All software and firmware components within the cryptographic boundary **shall** be verified using an Approved *integrity technique* as specified in Section 4.4." It's a little hard to pull the relevant information out of this section.	

78.	NIST	Elaine Barker	4.9.2.5		A cryptographic module **shall** test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service. What does "exclusive" mean here?	
79.	NIST	Elaine Barker	4.9.2.5		If a cryptographic module can automatically alternate between a bypass service and a cryptographic service, providing some services with cryptographic processing and some services without cryptographic processing, then the module **shall** test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified (e.g., an IP address source/destination table). Clarify. Provide an example?	
80.	NIST	Elaine Barker	4.9.3		"The time period and the policy regarding any conditions that may result in the interruption of the module's operations during the time to repeat the self-tests **shall** be specified (see Appendix B.) " Not clear.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Fiona Pattinson	4.10.1 1st bullet	E	A configuration management system does not develop software.	
2.	atsec	Fiona Pattinson	4.10.1 2nd bullet	E	Not all configuration management systems use a number to identify configuration items	
3.	atsec	Fiona Pattinson	4.10.1 3rd bullet	T	It is best practice that a CM system be used to track and maintain items during development and before the module is finally validated.	
4.	atsec	Fiona Pattinson	4.10.1 4th bullet	T	The definition of what standard of documentation is to be maintained is not described. It could therefore be as little as a reference to the name of the system used up to a full set of documentation per. Suggest that some indication of what is expected is added to this standard. Standards exist for both hardware and software configuration management that could be specified. E.g. ISO 10007:2003 Quality management systems - Guidelines for configuration management And ANSI/EIA-649-1998 National Consensus Standard for Configuration Management	

5.	atsec	Fiona Pattinson	4.10.2 SECURITY LEVEL 1	T	The level of detail of the correspondence is not provided by the standard. For example in a software module is it expected that the correspondence from source code to the security policy be specified or from architectural level design to the security policy? Clarify the level of detail expected.	
6.	atsec	Fiona Pattinson	4.10.1 4th bullet	T	The definition of what standard of documentation is to be maintained is not described. It could therefore be as little as a reference to the name of the system used up to a full set of documentation per. Suggest that some indication of what is expected is added to this standard. Standards exist for both hardware and software configuration management that could be specified. E.g. ISO 10007:2003 Quality management systems - Guidelines for configuration management And ANSI/EIA-649-1998 National Consensus Standard for Configuration Management	
7.	atsec	Fiona Pattinson	4.10.3 6th para List of other states	T	It is not clear if “degraded mode” should be depicted as an “Error state” or as an “Approved State”. Add a list item to para 4 giving the requirements for depicting degraded mode. OR Add some explanatory text to “Error State” in the preceding list of states (3rd para)	
8.	atsec	Fiona Pattinson	4.10.7 3rd para Administrator Guidance	T	The administrative guidance should also specify procedures on the decommissioning and secure disposal of the cryptographic module. Add a bullet giving the requirement : “Procedures on de-commissioning and the secure disposal of the cryptographic module.”	

9.	atsec	Fiona Pattinson	4.10.7 Administrator guidance	T	Since this standard is mandated for Federal use it would be appropriate if the Security Policy was consistent with other efforts in the Federal arena to improve security. It would be helpful to operators of cryptographic modules if they could check the configuration of the cryptographic module in a standard and consistent way. Add requirements to the specification of administration guidance to require that a configuration checklist be produced for the module using the eXtensible Configuration Checklist Description Format See http://scap.nist.gov/specifications/xccdf/	
10.	JCMVP		Draft Revised 4.9.1 1st paragraph	T	The following is said in Section 4.9.1: " The pre-operational tests shall be performed and passed successfully by a cryptographic module between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and transition to the operational state." However, the "operational state" is neither defined, nor mandatory in Section 4.10.3. Therefore, this sentence can be understood in many ways. So please revise the sentence in consistent with the similar requirement in FIPS 140-2, in the following: "The pre-operational tests shall be initiated automatically and shall not require operator intervention."	
11.	JCMVP		Draft Revised 4.10.4 Security Level 4	T	In this paragraph, the documentation only about "pre-conditions" and "post-conditions" is required, but we suggest to add "invariant conditions" as a part of documentation.	

12.	NSRI(National Security Research Institute)	Korea CMVP (Jihoon JEONG)	4.10.5(4th para) pp. 50		SL 3&4 : You have to **specify a sort of testing** of 'low-level testing' in the Security Level 3 & 4 more detail or specify the example like 'HDL Simulation Result' or something. (Do you have a plan to explain more detail in the DTR or IG later?)	
13.	NSRI(National Security Research Institute)	Korea CMVP (Jihoon JEONG)	4.10.7(3rd para) pp. 51		First Bullet : **The meaning of sentence is not clear.** 'Procedures required to keep independent operator administration mechanisms functionally independent.' **We would like to propose the new sentence. :** 'Procedures required to keep operator administration mechanisms functionally independent.'	
14.	CSD	Matthew Scholl/ Curt Barker	4.10.4	T	"The documentation **shall** also include the source code for the software or firmware, annotated with comments that depict the correspondence of the software or firmware to the design of the module." Modify to "The documentation **shall** include annotated comments that depict the correspondence of the software or firmware to the design of the module"	
15.	CMVP	Kim Schaffer	4.10.1	T	I do not understand the requirement for the last bullet under security levels 1 and 2.	
16.	CMVP	Kim Schaffer	4.10.3	T	" Each distinct cryptographic module service, security function use, error state, self-test, or operator authentication shall be depicted as a separate state." may be onerous for the lab and the reviewer for modules that provide many security functions such as cryptographic libraries.	

17.	Cryptsoft	Tim Hudson	4.10.1	T	Requiring specific individual component version tracking is a somewhat antiquated view of configuration management. A configuration management system may use other mechanisms than individual version or revision numbers for each component. e.g. distributed version control systems where the change set is allocated a change set identifier rather than a specific per-file version number. The requirements should be stated – not the mechanism for implementation. All items shall be under configuration management.	
18.	Cryptsoft	Tim Hudson	4.10.1	T	What is meant by “automated configuration management system”? If the intent is to preclude the use of a procedural based manual configuration management system then this should be stated. Suggested resolution: adjust text to be “the configuration management system shall not be by manual procedural methods”	
19.	Cryptsoft	Tim Hudson	4.10.3	T	The degraded operation state is missing from the list of optional states. Suggested resolution: add “Degraded State: a state in which not all services of a cryptographic module are available.”	
20.	Cryptsoft	Tim Hudson	4.10.4	T	“language reference” What is meant here? This term is not defined.	

21.	Cryptsoft	Tim Hudson	4.10.4	T	“using the configuration management system” It is unlikely that the same configuration management system used for the source and build environment for a cryptographic module will be used to contain a copy of vendor compilers, linkers, and operating system runtime libraries.	
22.	Cryptsoft	Tim Hudson	4.10.4	E	“All software or firmware within a cryptographic module shall be implemented using a high-level, non-proprietary language. Rationale shall be provided for the use of a low-level language …” The first requirement states shall and then provides a separate requirement if the first requirement is not followed. This should be reworded. It is also does not reflect the reality of embedded systems where assembly language is used for other than performance reasons.	
23.	Cryptsoft	Tim Hudson	4.10.5	T	“current automated security diagnostic tools” This is simply not stating any meaningful requirement as nothing specific is defined. Perhaps this was meant to be a reference to “industry best practice”?	
24.	Cryptsoft	Tim Hudson	4.10.6	E	“In addition to the requirement of Security Level 1, documentation shall specify the procedures required for maintaining security while distributing, installation and the initialization of versions of a cryptographic module to authorized operators. The procedures shall specify how to detect tamper during the delivery, installation and initialization of the module to the authorized operators.” This paragraph mixes tense and terms should be fixed.	

					Suggested resolution: replace with: "In addition to the requirement of Security Level 1, documentation shall specify the procedures required for maintaining security during the delivery, installation and initialization of the cryptographic module to authorized operators. The procedures shall specify how to detect tamper during the delivery, installation and initialization of the module to the authorized operators."	
25.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.1 Configura-tion Manage-ment**, SECURITY LEVELS 3 AND 4, Paragraph 1	G	Bills of Materials and documentation should not necessarily be managed by an automated configuration management system. Suggest specifying the use of an automated configuration management system for source code or HDL.	
26.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.2 Design**, SECURITY LEVEL 3, Bullet 1	G	Requiring a detailed design document is excessive. Recommend removing this requirement.	
27.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.3 Finite State Model**, Paragraph 1	E	What would be equivalent to a Finite State Model? Suggest giving an example of something equivalent to a Finite State Model.	
28.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.3 Finite State Model**, Paragraph 3, *Approved state*	G	Why would you need an Approved state when the Finite State Model only applies to the Approved mode(s) of operation? Suggest removing the requirement to specifically call out this state.	

29.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.3 Finite State Model**, Paragraph 4	G	A separate state for each cryptographic module service or security function may result in a Finite State Model that is much too busy to be of value. Suggest removing cryptographic module service and security function use as functions that require a separate state.	
30.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.3 Finite State Model**, Paragraph 6, *Bypass state*	G	Is the intention to require a Bypass state for only plaintext output or for all partial or non-cryptographic processing? Suggest being more specific as to what the Bypass state is to represent.	
31.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.4 Develop-ment**, SECURITY LEVEL 1, Bullet 2 of Bullet 4	G	Is a makefile sufficient to meet this requirement? Suggest specifying what would be needed beyond a makefile to meet this requirement.	
32.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.4 Develop-ment**, SECURITY LEVELS 2 AND 3, Bullet 3	T	This requirement cannot be verified and should be a recommendation, at most. Suggest removing this requirement.	
33.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.5 Vendor Testing**	G	FIPS 140 is a conformance testing. Specifying requirements for vendor testing make FIPS 140 more of an evaluation standard. Suggest removing this requirement section since this will be at the discretion of the CST laboratory what is sufficient low-level testing.	
34.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.7 Guidance Documents**, Paragraph 4	G	If there is no User role or similar roles, non-administrative guidance documentation may not be required. Suggest specifying that Non-administrator guidance document is not required if only Crypto Officer roles are supported.	

35.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**4.10**, **4.10.4 Develop-ment**, SECURITY LEVELS 2 AND 3, Bullet 3	T	This requirement cannot be verified and should be a recommendation, at most. Suggest removing this requirement.	
36.	IBM Research, Zurich	Visegrady, Tamas	**4.10.1**		The requirement of ``Automated CMS'' for higher security levels is underspecified (4.10.1). In an enterprise development environment, probably all CMS technologies would automatically qualify. One may probably reduce the explicit ``automation'' requirement without impacting design assurance.	
37.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.10.3	T	Crypto Officer State may be optional, based on cryptographic design. Rationale: See previous comment on the potential of a crypto being “Born” with all necessary CSPs.	
38.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.10.4	T	Under Security Levels 2 and 3 there is a requirement “Software cryptographic modules shall be designed and implemented in a manner that avoids the use of code, parameters or symbols not necessary for the module’s functionality and execution.” Is this requirement meant to preclude or prohibit precompiled software modules where the cryptographic module developer has no insight into the functionality of the entire software module? Is the requirement meant to preclude use of a software package, for instance a commercial IP stack in source code format, if the cryptographic product doesn’t require use of the entire IP stack? Likewise, commercially available software and FPGA libraries will likely contain “unneeded” functionality. Is the use of these products prohibited? Rationale: As hardware and software products become more complex, they can	

					contain unneeded functionality. I am attempting to clarify usability of these commercial products.	
39.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.10.4	T	Security Level 4 states "For each cryptographic module hardware and software component, the documentation shall be annotated with comments that specify (1) the pre-conditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the post-conditions expected to be true when the execution of the module component, function, or procedure is complete. The pre-conditions and post-conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the cryptographic module component, function, or procedure." Does this apply only to code developed by or explicitly for the cryptographic module or does it also apply to a commercial product, the source code of an IP stack? Rationale: If this applies to source code packages commercially developed, this may violate licensing agreements.	
40.	Motorola	Timothy Langham	4.10.6, Security Levels 2 & 3	G	Please provide more details about the tamper detection requirements for delivery.	
41.	NSA	TWG	4.10.6	E	Under security levels 2 and 3, should have tampering instead of tamper: "…how to detect tampe**ring** during .."	
42.	NSS Project	Wan-Teh Chang	Section 4.10.3, page 47.	Technical	Please allow the use of UML statecharts to specify the finite state model. Statecharts make it easy to specify complex modules. This doesn't need to be written into the standard. It suffices to just communicate this	

					to the testing labs.	
43.	Oberthur Technologies	Clement Capel & Christophe Goyet	§4.10.5	T	- §4.10.5 requires from level 1 that "vendors shall used current automated security diagnostical tools" to detect classical programming errors such as buffer overflow or division by 0. Although this is something we could do, there is for now nothing that is really designed for smartcard. Most of these errors are currently detected by compilers. It would be better to require an explanation on how vendor ensures that code is protected against those errors.	
44.	OpenSSL Software Foundation	Steve Marquess	4.10.3	T	The degraded operation state is missing from the list of optional states.	
45.	OpenSSL Software Foundation	Steve Marquess	4.10.4	T	"All software or firmware within a cryptographic module shall be implemented using a high-level, nonproprietary language. Rationale shall be provided for the use of a low-level language …" Assembly language is used for more than just performance reasons.	
46.	OpenSSL Software Foundation	Steve Marquess	4.10.5	T	T "current automated security diagnostic tools" This requirement is ambiguous.	
47.	Orion	MS	Section 4.10.4 Development, Level 1	T	"For software and firmware cryptographic modules…The result of the integrity and authentication technique mechanisms specified in Section 4.4 and 4.9 shall be calculated *and integrated into the software or firmware* module by the vendor during the module development."	

					It is not clear exactly what is to be integrated into the software or firmware module. In fact, the draft allows another module to perform the integrity test on the module. Clarify exactly what parts of the integrity need to be integrated into the module and what parts may be performed by another module.	
48.	Orion	MS	Section 4.I0.6, Security Level 4	T	This requirement should only apply when the module is initialized. It should not require that all operators must always be authenticated using authentication data provided by the vendor. For example, a vendor should not be required to set the passwords for all cryptographic officers and all users. A cryptographic officer should be allowed to set user passwords. Clarify that this only applies upon module initialization or delivery.	
49.	Defense Manpower Data Center (DMDC)	CTIS	4.10.5	T	The requirement that "shall used current automated security diagnostical tools" to detect classical programming errors is unclear in which specific tool(s) to use and may not apply to smartcard. DoD recommends further details on what acceptable tools may be used, and for requirements to fully specify programming errors expected to be caught.	
50.	Thales e-Security		4.10.3 Finite State Model	T	An FSM assumes that the module is only in one state at any one time. However some of the states provided are not mutually exclusive (For example the Crypto Officer State and the Approved State are not mutually exclusive. In fact these are roles rather than states). It will not be possible to specify an FSM for the Crypto Module using these states.	

51.	Thales e-Security		4.10.6		This section seeks to control the secure delivery and installation of the module. At Security Level 4 a procedure and technical controls are specified to ensure that the authorized user receives and installs the module. The requirements here are prescriptive, too solution orientated and onerous for both customer and vendor.	
52.	NIST	Elaine Barker	4.10 Para 1		*"Life-cycle assurance* refers to the use of best practices by the vendor of a cryptographic module during the design, development, and operation of a cryptographic module, providing assurance that the module is properly designed, developed, tested, configured, delivered, and installed, and that the proper operator guidance documentation is provided. Security requirements are specified for configuration management, design, finite state model, development, testing, delivery and operation, and guidance documentation" Replace with: "A configuration management system is intended to prevent accidental or unauthorized modifications to, and to provide change traceability for a cryptographic module and its related documentation. This section specifies the requirements for a configuration management system that **shall** be implemented by a cryptographic module vendor in order to provide assurance that the integrity of the cryptographic module is preserved during any refinement and modification of the cryptographic module	

					and related documentation. ”	
53.	NIST	Elaine Barker	4.10.2		“Cryptographic modules **shall** be designed to allow the testing of all provided security-related services. “ The “security-related services” refers to the approved security functions or SSP management techniques only? Or do non-approved things also need to be testable?	
54.	NIST	Elaine Barker	4.10.3		*“Bypass state*: a state in which a service, as a result of module configuration or operator intervention, causes the plaintext output of a particular data or status item that would normally be output in encrypted form. “ Could other cryptographic processes also be bypassed (e.g., digital signatures)?	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.11	T	In the responses to the last draft FIPS 140-3, NIST agreed that my comment regarding Simple Power Analysis shouldn't be applicable at Security Level 3. See CommentsFIPS140-3_draft1.pdf, ID# 93, Init J.C. . The requirement to prevent Simple Power Analysis doesn't appear to be included in the updated FIPS 140-3. Rationale: Modification accepted from earlier review and not incorporated in latest draft.	
2.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	4.11	T`	In the responses to the last draft FIPS 140-3, NIST agreed that my comment regarding Simple Power Analysis (SPA) and Differential Power Analysis (DPA) that Security Level 3 products should be required to protect against these attacks. See CommentsFIPS140-3_draft1.pdf ID# 63, Init J.C. . These agreed to requirements to protect against SPA and DPA at Security Level 3, the middle Security Level in the last round, have been moved to Security Level 4, the most extreme level, in this draft. Recommend that these requirement be applicable to Security Level 2 or 3 products. Security Level 2 is recommended since these techniques are being "productized" to the extent that technical expertise is not required to run/execute these techniques and obtain the CSPs or other security parameters of FIPS products. Rationale: NIST agreed that protection against these attacks should be provided by "middle of the road" NIST evaluated products.	

3.	Orion	MS	Section 4.11, Mitigation of other attacks	T	I think a Level 3 module should be required to specify the methods used to mitigate the attacks that are claimed to be mitigated. Change Security Levels 1,2, and 3 to Security Levels 1 and 2. Add a Level 3 that requires the vendor to specify the methods used to mitigate attacks but not the methods to test their effectiveness (as at Level 4).	
4.	Orion	MS	Section 4.11, Mitigation of other attacks	T	I think a Level 3 module should be required to specify the methods used to mitigate the attacks that are claimed to be mitigated. Change Security Levels 1,2, and 3 to Security Levels 1 and 2. Add a Level 3 that requires the vendor to specify the methods used to mitigate attacks but not the methods to test their effectiveness (as at Level 4).	
5.	SPYRUS, Inc.	WSM	4.11	G	In FIPS 140-2 an explicit list of attacks was provided to exemplify this area. This has apparently been replaced by Annex F. This section gives much less information on what is expected for a mitigated attack. For example, in the case of a module that is not a single chip (the latter being treated in 4.7), could Annex F attacks be claimed as Mitigated Other Attacks?	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	JCMVP		Draft Revised Appendix A, CRYPTOGRAPHIC MODULE SPECIFICATION	E	In this section, the word, "configuration items", seems to be used in the meaning of "components". We think that the usage of the two are different in the following: The term, "configuration items" is used in Section 4.10, and includes not only "cryptographic module components" but also documentations. So please replace "configuration items" with "components" in this section.	
2.	JCMVP		Draft Revised Appendix A, CRYPTOGRAPHIC MODULE PHYSICAL PORTS AND LOGICAL INTERFACES	E	The title “CRYTOGRAPHIC MODULE PHYSICAL PORTS AND LOGICAL INTERFACES” should be replaced by “CRYPTOGRAPHIC MODULE INTERFACES”	
3.	Cryptsoft	Tim Hudson	Appendix A	T	“Specification of the procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators. (Security Levels 2, 3 and 4)” This is inconsistent with the wording in 4.10.6. Suggested resolution: replace with “Specification of the procedures for maintaining security during the delivery, installation and initialization of a cryptographic module to authorized operators. (Security Levels 2, 3 and 4)”	

4.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX A**, **CRYPTO-GRAPHIC MODULE SPECIFIC-ATION**, Bullet 6	G	A block diagram is not required for software cryptographic modules. Recommend specifying that a block diagram is not required for software cryptographic modules.	
5.	NSS Project	Wan-Teh Chang	Appendix A, page 52	Editorial	Does a software module's vendor still need to provide documentation for "description of the physical configuration of the module" and "Block diagram depicting all of the major hardware components of a cryptographic module"?	
6.	Orion	MS	Appendix A, CRYPTOGRAPHIC MODULE PHYSICAL PORTS AND LOGICAL INTERFACES	E	It is confusing that this is similar to the old FIPS 140-2 Section 4.2 title but the new Section 4.2 title is just "Cryptographic Module Interfaces". While they are still present, physical ports have been de-emphasized. In any case, it would be nice for the titles in Appendix A to match the subsection titles in Section 4. Remove "PHYSICAL PORTS AND LOGICAL".	
7.	NIST	Elaine Barker			"A specification of each RBG (Approved RBGs Allowed RBGs, and entropy sources) employed by a cryptographic module. *(Security Levels 1, 2, 3 and 4) "* Only for seeding the old RNGs	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Fiona Pattinson	Appendix B	G	Since this standard is mandated for Federal use it would be appropriate if the Security Policy was consistent with other efforts in the Federal arena to improve security. For software modules and potentially other types of modules use appropriate SCAP methods for describing the module.	
2.	atsec	Fiona Pattinson	Appendix B 10. Life cycle Assurance	T	Secure disposal of the module is not discussed.	
3.	CSEC	Claudia Popa	Appendix B, 3. Roles, Services, and Authentication	T	Page 57 It is not enough if the strength of the authentication is specified in the Security Policy. This strength of the authentication has to meet the strength of authentication requirement. I did not find any requirements for the strength of authentication in the standard or annexes.	
4.	CSEC	Claudia Popa	Appendix B, 4. Software/Firmware Security	G	Page 57 The following information is required in the Security Policy: **"4. Software/Firmware Security** - Define the module's physical and cryptographic boundaries, contents, and logical security mechanisms. - How is the code protected from replacement? **- How is the code obfuscated?** - What are the tamper detection and response capabilities? " Is there any requirement in the standard that	

					requires that the code should be obfuscated?	
5.	CSEC	Claudia Popa	Appendix B, 9. Self-Tests	G	Third bullet “Describe all error states and status indicators”. I propose: “Describe all error states, status indicators and the action(s) required to exit the error state.”	
6.	CSEC	Jean Campbell	Appendix B	G	Page 57, Section 8. Add the text in bold Specify the SSP storage technique(s), **plaintext or encrypted** On the same page Specify the RBG entropy source(s). Do we need this information in the Security Policy or just in the test report?	
7.	JCMVP		Draft Revised Appendix B	E	Please start the section number by 1.	

8.	JCMVP		Draft Revised Appendix B 2. Cryptographic Module Ports and Interfaces	E	Please replace the title in consistent with that of Section 4.2, in the following: "Cryptographic Module Interfaces".	
9.	JCMVP		Draft Revised Appendix B, 3. Roles, Services, and Authentication	E	Please replace the title in consistent with that of Section 4.3, in the following: "Roles, Authentication and Services".	
10.	JCMVP		Draft Revised Appendix B, 9. Self-Test	E	Please add the documentation requirements about "critical function test" to the first bullet.	
11.	CMVP	Kim Schaffer	Appendix B, 3.	E	The order of Roles, Services and Authentication does not agree with section 4.	
12.	Cryptsoft	Tim Hudson	Appendix B Para 3.	E	“Specify each authentication method, whether the method is Identity or Role-based and the method is required.” Delete “is” from “is required”.	
13.	Cryptsoft	Tim Hudson	Appendix B Para 4.	T	“How is the code obfuscated?” There is no reference or requirement for code obfuscation elsewhere in FIPS140-3 and this section should not be introducing	

					requirements. Suggested resolution: delete bulleted item.	
14.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **2. Crypto-graphic Module Ports and Interfaces**	E	This section is now called “Cryptographic Module Interfaces”. Suggest renaming this subsection in this Appendix “Cryptographic Module Interfaces”.	
15.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **2. Crypto-graphic Module Ports and Interfaces**, Bullet 1	G	Is it really necessary to list all ports and interfaces in the non-proprietary Security Policy? Suggest removing this requirement.	
16.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **2. Crypto-graphic Module Ports and Interfaces**, Bullet 3	G	Is it really necessary to specify the data that passes over the physical ports in the non-proprietary Security Policy? Suggest removing this requirement.	
17.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **3. Roles, Services, and Authentica-tion**	E	This section is now called “Roles, Authentication and Services”. Suggest renaming this subsection in this Appendix “Roles, Authentication and Services”.	
18.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **3. Roles, Services, and Authentica-tion**, Bullet 2	G	Specifying all service commands with input and output is excessive in a non-proprietary Security Policy. This information should be in a manual. Suggest removing this requirement.	

19.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **3. Roles, Services, and Authentica-tion**, Bullet 8	G	This requirement may cause a significant amount of work for some vendors and is really not necessary. Suggest removing this requirement.	
20.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **3. Roles, Services, and Authentica-tion**, Bullet 9	G	The installation process should be described in a manual and not the non-proprietary Security Policy. Suggest removing this requirement.	
21.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **4.Software/Firmware Security**, Bullet 3	G	How the code is obfuscated should not be specified in the non-proprietary Security Policy. Suggest removing this requirement.	
22.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **4.Software/Firmware Security**, Bullet 4	G	The tamper detection and response capabilities are for Physical Security and not for Software/Firmware Security. Suggest removing this requirement.	
23.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **9. Self-Tests**, Bullet 1	G	Should not need to specify defined parameters for the self-tests. Suggest removing this requirement.	
24.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**APPEN-DIX B**, **10. Life-Cycle Assurance**	G	Procedures for secure installation, startup and operation of the module should be in a manual and not in the non-proprietary Security Policy. Suggest removing this requirement.	
25.	NSA	TWG	Appendix B	E	In #3, 4th bullet, need a “the” in “strength of **the** authentication …” In #5, need an article before applicable level in the last bullet, for example, “For an applicable level,….”	

					Section 9, 2nd bullet, need “periodic” instead of “period”	
26.	NSA	TWG	Appendix B	T	The bullets in section 4 don’t seem to be appropriate for the context discussed in that section; in particular, the two bullets “How is the code obfuscated” and “What are the tamper detection and response capabilities?”	
27.	NSS Project	Wan-Teh Chang	Appendix B, Section 1, page 56.	Editorial	The item “Approved and non-Approved modes of operations and how to enter/exit each mode” and the item “The security policy shall describe each Approved mode of operation implemented in the cryptographic module and how each mode is configured” are very similar.	
28.	Orion	MS	Appendix B, Cryptographic Module Ports and Interfaces	E	This title is the old FIPS 140-2 Section 4.2 title but not the new DFIPS 140-3 Section 4.2 title. Change to “Cryptographic Module Interfaces”.	
29.	NIST	Elaine Barker			“For Security Levels 1 and 2, the operation of the cryptographic module in an Approved mode **shall**, at a minimum, be by policy as specified in the security policy. “ Above statement doesn’t seem to fit here in Appendix B.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	CSEC	Jean Campbell	Appendix C	G	Include a statement that will allow these appendixes to be amended.	
2.	Cryptsoft	Tim Hudson	Appendix C	G	Reference to SP800-90 is inappropriate in this context. Only FIPS140-3 Annexes should be listed here. SP800-90 is already referenced in Annex A and does not warrant additional reference here.	
3.	Cryptsoft	Tim Hudson	Appendix C	G	All URLs should be references to the Annex document rather than general references to *PubsFIPS.html*.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	Athena	Athena Kerberos	Annex A		AES-CTS and SHA-96bit are mandatory for Kerberos Authetication, so AES-CTS and SHA-96bit should be listed in the FIPS140-3 approved crypto/hash list. AES-XCBC used in IPSec should also be listed in the list.	
2.	CSEC	Jan Rupar	Annex A: Approved Security Functions Symmetric Key Encryption	G	Why is Skipjack being recommended when it's slated to be discontinued by the end of 2010?	
3.	JCMVP		All annexes	E	In all the annexes, the phrase, "Operating Environment", is used. However the main document uses the phrase "Operational Environment". So please replace the phrase "Operating Environment" by "Operational Environment".	
4.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**Annexes A and B and Annexes C and D**	G	Too many Annexes. Recommend putting Approved and Allowed Security Functions in the same Annex and Approved and Allowed SSP Management Techniques in the same Annex.	

5.	InfoGard		Annex A	G	Remove Skipjack.	
6.	InfoGard		Annex A	G	Should SHA-1 be included under hashing, as it is Approved or Allowed in limited circumstances? If so, should there be qualifiers?	
7.	InfoGard		Annex A	G	Should SP 800-131 be referenced in this Annex, as a means of controlling the expiration of these functions?	
8.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Annexes	G	In general, the Annexes are a bit sparse, and seem to consist largely of references to the FIPS 140-3 Implementation Guidance (which is not available for review). It is not clear what the plan is for these Annexes and what information is intended to live here and what will be in the IG. To reduce confusion, it may be best to keep all this information in one document instead of spreading it across two places.	

9.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Annex A	T	It is not clear why Skipjack and SHA-1 are listed here, as the NIST transition plan requires them to be dropped from the Approved list after 2010.	
10.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Annex A	T	With the known security reductions with SHA-1, why hasn't the use of SHA-1 been precluded? Rationale: The effective security of SHA-1 has been reduced from 80 bits to the low 60 bits, or less. It is inappropriate for systems being designed in 2010+ to be able to use SHA-1.	
11.	Motorola	Ken Fuchs	Annex documents	G	Some of the Annex documents are grossly incomplete. What is the schedule to complete them?	
12.	NSA	TWG	Annex A	E	May want to remove SKIPJACK and Two-key Triple DES as options since it is unlikely that FIPS 140-3 will be published in 2010.	
13.	NSA	TWG	Annex A	E	The citation for the Digital Signature Standard (DSS) should be updated to FIPS 186-3.	

14.	NSA	TWG	Annex A	T	Under Asymmetric Key, reference 1 should be one for FIPS 186-3. Under Message Authentication, should #2 read instead "Recommendation for Block Cipher Modes of Operation: The CCM/**GCM Modes** for Authentication and Confidentiality"?	
15.	Oracle Security Evaluations	Shaun Lee	Annex A	T	Are additional algorithms, specifically ECC and Blowfish, being considered for inclusion as Approved Security Functions during this review period, or is such activity considered to be an independent exercise?	
16.	NIST	Elaine Barker	Annex A		Include a section for key wrapping, since it is included in Annex B, but indicate that there are currently no approved methods	
17.	NIST	Elaine Barker	Annex A 3. Skipjak		The transition SP (SP 800-131) addresses transitioning away from this at the end of 2010. If the item is retained in the annex, need to include 800-38A and maybe 800-38B.	
18.	NIST	Elaine Barker	Annex A Asymmetric Key - Signature 1. DSA, RSA and ECDSA		"National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2 with Change Notice 1, October 05, 2001. RSA Laboratories, *PKCS#1 v2.1: RSA Cryptography Standard*, June 14, 2002. Only the versions of the algorithms RSASSA-PKCS1-v1_5 and RSASSA-PSS contained within this document shall be used. " Modify these in accordance with the transition strategy and include FIPS 186-3.	

19.	NIST	Elaine Barker	Annex A 1. **Triple-DES**		"National Institute of Standards and Technology, *Computer Data Authentication*, Federal Information Processing Standards Publication 113, 30 May 1985. " Need to discuss how to deal with this. FIPS 113 needs to be withdrawn.	
20.	NIST	Elaine Barker	Annex A, 2. AES		SP 800-38E should be posted as final soon.	
21.	NIST	Elaine Barker	Annex A		**"Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512)** National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-3, October, 2008. " Include SP 800-106 and 107?	
22.	NIST	Elaine Barker	Annex A		"1. **Approved Random Bit Generators"** Need to discuss how to deal with the old generators here (see draft SP 800-131)	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	JCMVP		All annexes	E	In all the annexes, the phrase, "Operating Environment", is used. However the main document uses the phrase "Operational Environment". So please replace the phrase "Operating Environment" by "Operational Environment".	
2.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**Annexes A and B and Annexes C and D**	G	Too many Annexes. Recommend putting Approved and Allowed Security Functions in the same Annex and Approved and Allowed SSP Management Techniques in the same Annex.	
3.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Annexes	G	In general, the Annexes are a bit sparse, and seem to consist largely of references to the FIPS 140-3 Implementation Guidance (which is not available for review). It is not clear what the plan is for these Annexes and what information is intended to live here and what will be in the IG. To reduce confusion, it may be best to keep all this information in one document instead of spreading it across two places.	
4.	Motorola	Ken Fuchs	Annex documents	G	Some of the Annex documents are grossly incomplete. What is the schedule to complete them?	
5.	NSA	TWG	Annex B	E	May want to remove Two-key Triple DES for key wrapping as an option since it is unlikely that FIPS 140-3 will be published in 2010.	
6.	Oracle Security Evaluations	Shaun Lee	Annex B	T	What is the plan to modify this annex to align with the changes in NIAP/CCEVS policy and the generation of new standard profiles?	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	JCMVP		All annexes	E	In all the annexes, the phrase, "Operating Environment", is used. However the main document uses the phrase "Operational Environment". So please replace the phrase "Operating Environment" by "Operational Environment".	
2.	Cryptsoft	Tim Hudson	Annex C Annex D Annex F	T/G	Defining Annex's that simply point to Implementation Guidance sections is inappropriate. The details should be clearly contained within the Annex and updated as additional techniques/algorithms are approved or allowed for use in keeping with the approach used for FIPS140-1 and FIPS140-2. Implementation Guidance is defined as **guidance** and not **requirements**. Suggested resolution: replace with "None currently defined" and delete "Additional guidance can be found in FIPS140-3 Implementation Guidance, Section X" in each of the Annexes.	
3.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**Annexes A and B and Annexes C and D**	G	Too many Annexes. Recommend putting Approved and Allowed Security Functions in the same Annex and Approved and Allowed SSP Management Techniques in the same Annex.	
4.	InfoGard		Annex C	G	The meaning of Annex C and D is not clear. Rather than "SSP Management Techniques", NIST seems to mean "SSP Establishment Techniques" specifically.	

5.	InfoGard		Annexes C & D	G	Global Platform Secure Channel Protocol 03 is a Trusted Channel mechanism that specifies only NIST Approved primitives, methods and key sizes. Is it an Approved or Allowed security function or SSP management technique? Suggest including Global Platform SCP03 as an Allowed Security function.	
6.	InfoGard		Annexes C & D	G	Is OTAR an Approved or Allowed security function or technique? Suggest keeping and specifying OTAR as an Allowed Security function.	
7.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Annexes	G	In general, the Annexes are a bit sparse, and seem to consist largely of references to the FIPS 140-3 Implementation Guidance (which is not available for review). It is not clear what the plan is for these Annexes and what information is intended to live here and what will be in the IG. To reduce confusion, it may be best to keep all this information in one document instead of spreading it across two places.	
8.	Motorola	Ken Fuchs	Annex documents	G	Some of the Annex documents are grossly incomplete. What is the schedule to complete them?	
9.	NSA	TWG	Annex C	E	Suggest including “Recommendation for Pair-wise Key Establishment Schemes Using Integer Factorization Cryptography,” SP 800-56B, dated August 2009.	
10.	NSA	TWG	Annex C	T	Need additional reference for SP800-56B	

11.	OpenSSL Software Foundation	Steve Marquess	Annex C Annex D Annex F	T/G	Defining Annexes that simply point to Implementation Guidance sections is inappropriate. Implementation Guidance should not be providing requirements.	
12.	Orion	MS	Annex C	T	This Annex seems to be miss-named. Rather than “Approved SSP Management Techniques” it should be called “Approved SSP Establishment Techniques” since it only includes Approved SSP Establishment Techniques.	
13.	Orion	MS	Annex C	T	For symmetric key establishment guidance, this annex refers to Section 8 of FIPS 140-3 Implementation Guidance. I could not find implementation guidance for FIPS 140-3. Make referenced implementation guidance available.	
14.	Security Innovation	William Whyte	Annex C	Technical	The list of approved SSP management techniques is too restrictive. It should include Integer Factorization techniques. It should also consider including techniques based on mathematical problems that are not vulnerable to Shor’s algorithm, to enable agencies to move towards systems that will continue to be secure if quantum computers are developed Include RSA-OAEP encryption as specified in PKCS#1 Include NTRUEncrypt encryption as specified in IEEE 1363.1, X9.98	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	JCMVP		All annexes	E	In all the annexes, the phrase, "Operating Environment", is used. However the main document uses the phrase "Operational Environment". So please replace the phrase "Operating Environment" by "Operational Environment".	
2.	Cryptsoft	Tim Hudson	Annex C Annex D Annex F	T/G	Defining Annex's that simply point to Implementation Guidance sections is inappropriate. The details should be clearly contained within the Annex and updated as additional techniques/algorithms are approved or allowed for use in keeping with the approach used for FIPS140-1 and FIPS140-2. Implementation Guidance is defined as **guidance** and not **requirements**. Suggested resolution: replace with "None currently defined" and delete "Additional guidance can be found in FIPS140-3 Implementation Guidance, Section X" in each of the Annexes.	
3.	EWA-Canada IT Security Evaluation & Test Facility	Carol Cantlon	**Annexes A and B and Annexes C and D**	G	Too many Annexes. Recommend putting Approved and Allowed Security Functions in the same Annex and Approved and Allowed SSP Management Techniques in the same Annex.	

4.	InfoGard		Annexes C & D	G	Global Platform Secure Channel Protocol 03 is a Trusted Channel mechanism that specifies only NIST Approved primitives, methods and key sizes. Is it an Approved or Allowed security function or SSP management technique? Suggest including Global Platform SCP03 as an Allowed Security function.	
5.	InfoGard		Annexes C & D	G	Is OTAR an Approved or Allowed security function or technique? Suggest keeping and specifying OTAR as an Allowed Security function.	
6.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Annexes	G	In general, the Annexes are a bit sparse, and seem to consist largely of references to the FIPS 140-3 Implementation Guidance (which is not available for review). It is not clear what the plan is for these Annexes and what information is intended to live here and what will be in the IG. To reduce confusion, it may be best to keep all this information in one document instead of spreading it across two places.	
7.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Annexes	G	In general, the Annexes are a bit sparse, and seem to consist largely of references to the FIPS 140-3 Implementation Guidance (which is not available for review). It is not clear what the plan is for these Annexes and what information is intended to live here and what will be in the IG. To reduce confusion, it may be best to keep all this information in one document instead of spreading it across two places.	
8.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Annex D	G	The FIPS 140-3 Implementation Guidance, Section 8 is not available for this review with this draft specification. Provide this document as part of the review and comment cycle. Rationale: Annex D and other point to this document as forming part of the FIPS.	

					Without being able to review the content of this document, there could be errors and/or inconsistencies uncovered in the entirety. Also, what is defined in this document could change the understanding of requirements of portions of FIPS 140-3.	
9.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Annex D	G	The FIPS 140-3 Implementation Guidance, Section 8 is not available for this review with this draft specification. Provide this document as part of the review and comment cycle. Rationale: Annex D and other point to this document as forming part of the FIPS. Without being able to review the content of this document, there could be errors and/or inconsistencies uncovered in the entirety. Also, what is defined in this document could change the understanding of requirements of portions of FIPS 140-3.	
10.	Motorola	Ken Fuchs	Annex documents	G	Some of the Annex documents are grossly incomplete. What is the schedule to complete them?	
11.	OpenSSL Software Foundation	Steve Marquess	Annex C Annex D Annex F	T/G	Defining Annexes that simply point to Implementation Guidance sections is inappropriate. Implementation Guidance should not be providing requirements.	
12.	Orion	MS	Annex D	T	As before, it seems that Annex D should be “Allowed SSP Establishment Techniques”. Change Annex D title and text where “SSP Management Techniques” is used.	

13.	Orion	MS	Annex D	T	This Annex refers the reader to the Section 8 of the FIPS 140-3 Implementation Guidance. I could not find implementation guidance for FIPS 140-3. Make referenced implementation guidance available.	
14.	Security Innovation	William Whyte	Annex D	Technical	The Implementation Guidance document is not currently available so this section is difficult to comment on. SI encourages NIST to consider including techniques based on mathematical problems that are not vulnerable to Shor's algorithm, to enable agencies to move towards systems that will continue to be secure if quantum computers are developed In the Implementation Guidance document: Include RSA-OAEP encryption as specified in PKCS#1 Include NTRUEncrypt encryption as specified in IEEE 1363.1, X9.98	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	JCMVP		All annexes	E	In all the annexes, the phrase, "Operating Environment", is used. However the main document uses the phrase "Operational Environment". So please replace the phrase "Operating Environment" by "Operational Environment".	
2.	Microsoft Corporation	Vijay Bharadwaj <Vijay.Bharadwaj@microsoft.com>	Annexes	G	In general, the Annexes are a bit sparse, and seem to consist largely of references to the FIPS 140-3 Implementation Guidance (which is not available for review). It is not clear what the plan is for these Annexes and what information is intended to live here and what will be in the IG. To reduce confusion, it may be best to keep all this information in one document instead of spreading it across two places.	
3.	Motorola	Ken Fuchs	Annex documents	G	Some of the Annex documents are grossly incomplete. What is the schedule to complete them?	
4.	Orion	MS	Annex E	T	Since there are no Approved authentication mechanisms and (apparently) no Allowed authentication mechanisms, it is not clear how a level above Security Level 1 could be reached. The annex references FIPS 140-3 Implementation Guidance which is not provided. NIST needs to provide Approved or Allowed authentication mechanisms for each security level. This should be done before FIPS 140-3 is approved.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	atsec	Fiona Pattinson	Annex “F” Page (i)	E	The Title given on page (i) is not the same as the Title on the front page. Change the title on page (i) from “Test Metrics for FIPS PUB 140-3” to “Non-Invasive Attack Methods for FIPS PUB 140-3”	
2.	brightsight	Lex Schoonen	Annex F	E	Brightsight recommends mentioning that the class of timing attacks includes subtle extensions such as cache collision attacks.	
3.	brightsight	Lex Schoonen	Annex F, Table F.1	T	The table does not associate DPA and DEMA with asymmetric cryptographic algorithms. It is possible to apply this class of attacks on asymmetric algorithms. This has been well-established and mitigation is therefore mandated for certifications in the banking world and the common criteria, In FIPS 140-3, mitigation should also be required, and not optional.	
4.	JCMVP		All annexes	E	In all the annexes, the phrase, "Operating Environment", is used. However the main document uses the phrase "Operational Environment". So please replace the phrase "Operating Environment" by "Operational Environment".	

5.	CSEC	Eve St-Laurent	Annex F: Test Metrics Non-Invasive Attack Testing	T	*"For security Levels 4 all Approved asymmetric-key security functions **shall** pass both, the SPA and SEMA tests."* This is not sufficient: asymmetric-key security functions should also be tested against CPA (please refer to Japanese paper titled ***Comparative Power Analysis*** *of Modular Exponentiation Algorithms*). I have also seen other CPA attacks with chosen inputs acting like iterative SPA attacks - so easy to carry out, requiring fewer traces than DPA but more than SPA. **Suggestion:** Include CPA in *"For security Levels 4 all Approved asymmetric-key security functions **shall** pass the CPA, SPA and SEMA tests."* Also add a subsection titled: **Comparative Power Analysis (CPA)** **Level 4** To complete the CPA test at Level 4, the provided test tool **shall** collect x traces per iteration with predetermined input data […] The data collection and analysis time for x secret key bits **shall** be at least x days.	
6.	CSEC	Eve St-Laurent	Annex F: Test Metrics Non-Invasive Attack Testing	T	*"For security Levels 4 all Approved asymmetric-key security functions **shall** pass both, the SPA and SEMA tests."* This does not include DPA and DEMA tests for asymmetric keys although attacks are out there (please refer to papers such as - *A DPA Attack against Asymmetric Encryption*; - *A DPA Attack against the Modular Reduction within a CRT Implementation of RSA;* - *A DPA attack on RSA in CRT mode;* - *A refined power-analysis attack on Elliptic Curve Cryptosystems;* and, - *Protections against Differential Analysis for*	

					Elliptic Curve Cryptography). If a threat agent can carry out a DPA attack against a symmetric algorithm, he/she is probably able to do the same against an asymmetric one (maybe after trying SPA/SEMA and CPA). **Suggestion:** Include DPA and DEMA in "*For security Levels 4 all Approved asymmetric-key security functions **shall** pass the CPA, SPA and SEMA tests, as well as pass both, the DPA and DEMA tests.*	
7.	Cryptsoft	Tim Hudson	Annex C Annex D Annex F	T/G	Defining Annex's that simply point to Implementation Guidance sections is inappropriate. The details should be clearly contained within the Annex and updated as additional techniques/algorithms are approved or allowed for use in keeping with the approach used for FIPS140-1 and FIPS140-2. Implementation Guidance is defined as **guidance** and not **requirements**. Suggested resolution: replace with "None currently defined" and delete "Additional guidance can be found in FIPS140-3 Implementation Guidance, Section X" in each of the Annexes.	
8.	Cryptography Research, Inc.		Annex F	G,T	**Annex F is a positive structural enhancement of the standard.** We welcome the introduction of Annex F to provide listing of relevant attack methods applicable to the specification. The inclusion of Annex F allows for new and emerging attacks and threats to be brought within the scope of the specification in a timely manner, without requiring a full revision of FIPS 140.	

9.	The MITRE Corporation 202 Burlington Rd Bedford, MA 01730	James Cottrell jxc@mitre.org 781-271-7212	Annex F	T	Add entries for Cache, Predictive Branch and rf non-invasive attack methods. Rationale: These techniques are discussed and defined in the literature; see www.sidechannelattack.com and www.iarc.org for papers on these techniques. NIST evaluated product at Security Level 3 should be designed to prevent these attacks and those at Security Level 4 should protect against these attacks.	
10.	Motorola	Ken Fuchs	Annex documents	G	Some of the Annex documents are grossly incomplete. What is the schedule to complete them?	
11.	Motorola	Ken Fuchs	Annex F	G	Annex F involves non-invasive attacks. There is no measurement criteria listed to compare your module against.	
12.	OpenSSL Software Foundation	Steve Marquess	Annex C Annex D Annex F	T/G	Defining Annexes that simply point to Implementation Guidance sections is inappropriate. Implementation Guidance should not be providing requirements.	
13.	Riscure	Marc Witteman	Annex F	T	The annex only mentions side channel analysis attacks. Smart card issuing and certification schemes today regard fault injection as the most significant threat though. Include fault injection through voltage, electro-magnetic or optical manipulation. The test should verify that the module does not: 1) return corrupted signatures/cryptograms, 2) allow by-pass of access mechanisms, and 3) dump restricted data without authentication due to fault injection.	
14.	Riscure	Marc Witteman	Annex F, table F.1	T	The table suggests that SPA need not be performed on symmetric algorithms and DPA need not be performed on asymmetric algorithms. This is in contrast with significant vulnerabilities that have been found for these combinations. E.g. a DES implementation may be vulnerable to SPA due to parity	

					checking, and an RSA CRT implementation can be attacked with DPA during the recombination phase. Remove property “symmetric” and “asymmetric” from all table rows.	

	ORGANIZATION	AUTHOR	SECTION, SUBSECT & PARA.	TYPE	COMMENT	RESOLUTION
1.	JCMVP		All annexes	E	In all the annexes, the phrase, "Operating Environment", is used. However the main document uses the phrase "Operational Environment". So please replace the phrase "Operating Environment" by "Operational Environment".	
2.	InfoGard		Annex G, Section 2	E	Suggested change: Replace*: "… Approved SSP Management Techniques…" with "…Allowed Operating Environments…"*	
3.	Orion	MS	Annexes	G	The writers of this draft of FIPS 140-3 have moved the specification of Approved and Allowed SSP management techniques to Annexes. While this approach has significant advantages, NIST needs to complete the Annexes and the referenced implementation guidance. Complete the Annexes and referenced implementation guidance.	
4.	Orion	MS	Annex G	T	Annex G refers to FIPS 140-3 Implementation Guidance which was not provided. NIST needs to provide the cited FIPS 140-3 Implementation Guidance.	