ID	Init	Sub Sec	Para	Type	Comment	Author	**Resolution**
229	A.R.	4.1	General Comment		I would like to propose that any cryptographic module validated to FIPS 140-3 operates in FIPS mode only. This will eliminate many possible errors when using the validated crypto module. The review process and the documentation requirements will become more straightforward.	Allen Roginsky	**Rejected:** Vendors will be reluctant to split their production line and have separate modules just for US Gov. This will reduce number of modules available to US Gov. and drive the prices for US Gov. only modules higher.
657	W.C.	4.1	Sec. 4.1.5		The second sentence says "The security strength of the module shall be one of the recommended security strengths, .." Where are the recommended security strengths specified?	Wan-Teh Chang	**Accepted:** A reference is required. EX: NIST SP 800-57
121	Y.A.	4.1			Demands for machine readable data is increasing not only for data in business application but also for other information. In the Internet environment, if a software process uses a certain result which is sent from a remote site, it may need information about the security of the remote site, for example, the security level of the used hardware, software, and so on. If cryptographic technology is used in a remote site, there may be a need to know how trustworthy the implementation of the cryptographic module is. To give a solution to the above-mentioned issue in biometric verification in remote sites, a project named Authentication context for biometrics (ACBio) in ISO/IEC JTC 1/SC 27/WG 5 is standardizing the data format which enables the validator of a biometric verification process to tell the assureness of the result of the biometric verification. In addition to the security level of biometric device and other test results, ACBio is demanding machine readable test result of the cryptographic module used in biometric verification.	YAMADA Asahiko T	**Rejected:** This can be optionally engineered into a module as necessary. Not a minimum requirement of FIPS 140-3.
122	Y.A.	4.1			CryptographicModuleValidationProgramTestResult. It is important to be able to know who has done and reported the test. Because the result is thought to be trustworthy only if the test was done in a trusted evaluation organization. Therefore the Machine Readable Test Result shall be digitally singed by the evaluation organization. In order to use Machine Readable Test Result in ACBio, it is requested that it is described in ASN.1 notation since ACBio is specified in ASN.1 notation.	YAMADA Asahiko T	**Rejected:** This can be optionally engineered into a module as necessary. Not a minimum requirement of FIPS 140-3.

					This comment gives an example of ASN.1 module for Machine Readable Test Result as follows. Note that some values including OBECT IDENTIFIERs must be replaced with the suitable ones.		

123	Y.A.	4.1			3.ASN.1 module for Machine Readable Test Result
					
					CryptographicModuleValidationProgramTestResult {
					  iso(1) identified-organization(3) nist(5) cmvp(140) part3(3) module(1) rev(1)
					}
					
					DEFINITIONS AUTOMATIC TAGS ::= BEGIN
					
					IMPORTS
					
					  -- ISO/IEC 9594-8 Open Systems Interconnection -- The Directory: Authentication framework
					
					  AlgorithmIdentifier, Name
					  FROM AuthenticationFramework {
					  joint-iso-itu-t ds(5) module(1) authenticationFramework(7) 5}
					
					  -- RFC 3852 Cryptographic Message Syntax
					
					  CMSVersion, gestAlgorithmIdentifiers, CertificateSet, RevocationInfoChoices, SignerInfos
					  FROM CryptographicMessageSyntax2004 {
					  iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }
					
					ContentInfoCMVP ::= SEQUENCE {
					  contentType ContentTypeCMVP,
					  content [0] EXPLICIT ANY DEFINED BY contentType
					}
					
					ContentTypeCMVP OBJECT IDENTIFIER ::= id-signedDataCMVP
						YAMADA Asahiko T	**Rejected:** This can be optionally engineered into a module as necessary. Not a minimum requirement of FIPS 140-3.

```
SignedDataCMVP ::= SEQUENCE {
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo
EncapsulatedContentInfoCMVP,
    certificates [0] IMPLICIT CertificateSet
OPTIONAL,
    crls [1] IMPLICIT RevocationInfoChoices
OPTIONAL,
    signerInfos SignerInfos
}

EncapsulatedContentInfoCMVP ::= SEQUENCE {
    eContentType EContentTypeCMVP,
    eContent [0] EXPLICIT OCTET STRING
OPTIONAL
}

EContentTypeCMVP OBJECT IDENTIFIER ::= id-
cmvpContentInformation

CMVPContentInformation ::= SEQUENCE {
  version                Version DEFAULT v0 (0),
  productName            Name,
  overallLevelAchieved   Level,
  details                Details OPTIONAL,
  approvedAlgorithms     AlgorithmIDs,
  nonApprovedAlgorithms  AlgorithmIDs
OPTIONAL
}

Version ::= INTEGER { v0(0) } ( v0, ... )

Level ::= ENUMERATED {
  na      (0),
  level1  (1),
  level2  (2),
  level3  (3),
  level4  (4),
  level5  (5)
}

Details ::= SEQUENCE {
  moduleSpecification          LevelTypeA,
  modulePortsInterfaces        LevelTypeA,
```

```
  rolesServicesAuthentication       LevelTypeB,
  softwareSecurity                  Level,
  operationalEnvironment            LevelTypeB,
  physicalSecurity                  Level,
  nonInvasiveAttacks                LevelTypeC,
  sspManagement                     LevelTypeD,
  selfTest                          LevelTypeE,
  lifeCycleAssuranceCMS             LevelTypeA,
  lifeCycleAssuranceDesign          Level,
  lifeCycleAssuranceFSM             LevelTypeF,
  lifeCycleAssuranceDevelopment     LevelTypeG,
  lifeCycleAssuranceVendorTesting   LevelTypeA,
  lifeCycleAssuranceDeliveryOperator LevelTypeH,
  lifeCycleAssuranceGuidanceDocs    LevelTypeF,
  mitigation                        LevelTypeI
}

LevelTypeA ::= ENUMERATED {
  na          (0),
  level1And2  (1),
  level3And4And5 (2)
}

LevelTypeB ::= ENUMERATED {
  na      (0),
  level1  (1),
  level2  (2),
  level3  (3),
  level4And5 (4)
}

LevelTypeC ::= ENUMERATED {
  naAndLevel1And2  (0),
  level3And4And5   (1)
}

LevelTypeD ::= ENUMERATED {
  na      (0),
  level1And2 (1),
  level3And4 (2),
  level5  (3)
}

LevelTypeE ::= ENUMERATED {
  na              (0),
  level1          (1),
```

					level2And3And4And5 (2)
					}
					
					LevelTypeF ::= ENUMERATED {
					na (0),
					level1And2And3And4And5 (1)
					}
					
					LevelTypeG ::= ENUMERATED {
					na (0),
					level1 (1),
					level2And3 (2),
					level4And5 (3)
					}
					
					LevelTypeH ::= ENUMERATED {
					na (0),
					level1 (1),
					level2 (2),
					level3And4And5 (3)
					}
					
					LevelTypeI ::= ENUMERATED {
					na (0),
					level1And2And3 (1),
					level4And5 (2)
					}
					
					AlgorithmIDs ::= SET OF AlgorithmIdentifier
					
					-- contentType
					
					id-cmvp OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
					nist(5) cmvp(140) part3(3) }
					
					id-signedDataCMVP OBJECT IDENTIFIER ::= { id-cmvp 1 }
					
					id-cmvpContentInformation OBJECT IDENTIFIER ::= { id-cmvp 2 }
					
					END --
					CryptographicModuleValidationProgramTestResult		

215	M. W.	4.1			*"I would like to make use of the opportunity to provide you with feedback on the FIPS 140-3 standard. I work for Riscure, a security test laboratory based in the Netherlands. Riscure specialises in the security evaluation of smart card and embedded technology and has been offering its services since 2001. Examples of North-American customers that we work with are MasterCard International, Visa International, Microsoft, Aspect Labs, Cryptography Research Inc.,* *NSA NCSC, Unisys and the Communications Security Establishment in Canada. Besides offering security evaluation services, we develop and sell the Side Channel Test Platform called Inspector."*	Marc Witteman (Amanda van der Berg) - Riscure	**Rejected:** Incomplete
328		4.1			Demands for machine readable data is increasing not only for data in business application but also for other information. In the Internet environment, if a software process uses a certain result which is sent from a remote site, it may need information about the security of the remote site, for example, the security level of the used hardware, software, and so on. If cryptographic technology is used in a remote site, there may be a need to know how trustworthy the implementation of the cryptographic module is. To give a solution to the above-mentioned issue in biometric verification in remote sites, a project named Authentication context for biometrics (ACBio) in ISO/IEC JTC 1/SC 27/WG 5 is standardizing the data format which enables the validator of a biometric verification process to tell the assureness of the result of the biometric verification. In addition to the security level of biometric device and other test results, ACBio is demanding machine readable test result of the cryptographic module used in biometric verification.	YAMADA Asahiko T	**Rejected:** Duplicate of 121

329	Y.A.	4.1			CryptographicModuleValidationProgramTestResult 2.Requirements and request It is important to be able to know who has done and reported the test. Because the result is thought to be trustworthy only if the test was done in a trusted evaluation organization. Therefore the Machine Readable Test Result shall be digitally singed by the evaluation organization. In order to use Machine Readable Test Result in ACBio, it is requested that it is described in ASN.1 notation since ACBio is specified in ASN.1 notation. This comment gives an example of ASN.1 module for Machine Readable Test Result as follows. Note that some values including OBECT IDENTIFIERs must be replaced with the suitable ones.	YAMADA Asahiko T	**Rejected:** Duplicate of 122
351	Y.A.	4.1			CryptographicModuleValidationProgramTestResult {iso(1) identified-organization(3) nist(5) cmvp(140) part3(3) module(1) rev(1) }DEFINITIONS AUTOMATIC TAGS ::= BEGIN IMPORTS -- ISO/IEC 9594-8 Open Systems Interconnection -- The Directory: Authentication framework AlgorithmIdentifier, Name FROM AuthenticationFramework { joint-iso-itu-t ds(5) module(1) authenticationFramework(7) 5} -- RFC 3852 Cryptographic Message Syntax CMSVersion, gestAlgorithmIdentifiers, CertificateSet, RevocationInfoChoices, SignerInfos FROM CryptographicMessageSyntax2004 {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24) }ContentInfoCMVP ::= SEQUENCE {contentType ContentTypeCMVP, content [0] EXPLICIT ANY DEFINED BY contentType}ContentTypeCMVP OBJECT IDENTIFIER ::= id-signedDataCMVP SignedDataCMVP ::= SEQUENCE { version CMSVersion, digestAlgorithms DigestAlgorithmIdentifiers, encapContentInfo EncapsulatedContentInfoCMVP, certificates [0] IMPLICIT CertificateSet OPTIONAL, crls [1] IMPLICIT RevocationInfoChoices OPTIONAL, signerInfos SignerInfos} EncapsulatedContentInfoCMVP ::= SEQUENCE { eContentType EContentTypeCMVP,	YAMADA Asahiko T	**Rejected:** Duplicate of 123

					eContent [0] EXPLICIT OCTET STRING OPTIONAL}
					EContentTypeCMVP OBJECT IDENTIFIER ::= id-cmvpContentInformation CMVPContentInformation ::= SEQUENCE { version Version DEFAULT v0 (0), productName Name, overallLevelAchieved Level, details Details OPTIONAL, approvedAlgorithms AlgorithmIDs, nonApprovedAlgorithms AlgorithmIDs OPTIONAL}Version ::= INTEGER { v0(0) } (v0, ...)Level ::= ENUMERATED {na (0), level1 (1), level2 (2), level3 (3), level4 (4), level5 (5)}Details ::= SEQUENCE { moduleSpecification LevelTypeA, modulePortsInterfaces LevelTypeA, rolesServicesAuthentication LevelTypeB, softwareSecurity Level, operationalEnvironment LevelTypeB, physicalSecurity Level, nonInvasiveAttacks LevelTypeC, sspManagement LevelTypeD, selfTest LevelTypeE, lifeCycleAssuranceCMS LevelTypeA, lifeCycleAssuranceDesign Level, lifeCycleAssuranceFSM LevelTypeF, lifeCycleAssuranceDevelopment LevelTypeG, lifeCycleAssuranceVendorTesting LevelTypeA, lifeCycleAssuranceDeliveryOperator LevelTypeH, lifeCycleAssuranceGuidanceDocs LevelTypeF, mitigation LevelTypeI}
					LevelTypeA ::= ENUMERATED {na (0), level1And2 (1), level3And4And5 (2)}LevelTypeB ::= ENUMERATED {na (0), level1 (1), level2 (2), level3 (3),level4And5 (4)}LevelTypeC ::= ENUMERATED { naAndLevel1And2 (0), level3And4And5 (1)}LevelTypeD ::= ENUMERATED { na (0), level1And2 (1), level3And4 (2), level5 (3)LevelTypeE ::= ENUMERATED {na (0), level1 (1), level2And3And4And5 (2)}LevelTypeF ::= ENUMERATED {na (0), level1And2And3And4And5 (1)
					}
					
					LevelTypeG ::= ENUMERATED {
					na (0),
					level1 (1),		

					level2And3 (2),
					level4And5 (3)
					}
					
					LevelTypeH ::= ENUMERATED {
					na (0),
					level1 (1),
					level2 (2),
					level3And4And5 (3)
					}
					
					LevelTypeI ::= ENUMERATED {
					na (0),
					level1And2And3 (1),
					level4And5 (2)
					}
					
					AlgorithmIDs ::= SET OF AlgorithmIdentifier
					
					-- contentType
					
					id-cmvp OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
					nist(5) cmvp(140) part3(3) }
					
					id-signedDataCMVP OBJECT IDENTIFIER ::= { id-cmvp 1 }
					
					id-cmvpContentInformation OBJECT IDENTIFIER ::= { id-cmvp 2 }
					
					END -- CryptographicModuleValidationProgramTestResult		

353	B.M.	4.1	Sec. 4.1		The Security Levels do not seem to fit the case of the PIV Card as an identity token capable of authentication at graduated levels of assurance. In Draft FIPS 140-3, subject authentication requirements are set for each of the Security Levels (e.g., two factor for Security Level 4). However, the PIV Card is designed to support one or two factor authentication, and could be extended to three factor authentication with the addition of Secure Biometric Match-On-Card capability. What Security Level is appropriate for the PIV Card? (See following questions.) Is it possible for a module validated at Security Level N to be used in an operating mode less than N? Would you agree that there is a conflict between the Security Level model of Draft FIPS 140-2 and the PIV requirement for graduated levels of assurance?	Bill MacGregor NIST	**Rejected:** FIPS 140-3 sets minimum security requirements. Vendor can always design the module to meet the requirements for 2 factor authentication (RE: Level 4 Section 4.3)
480	P.G.	4.1	General		*Brightsight would like to use the opportunity to give some comments on the proposed FIPS 140-3 specification. Brightsight has a long history in security evaluations under multiple schemes. Currently, Brightsight is a certified lab under, amongst others, the PCI, EMVCo, VISA, MasterCard and Common Criteria scheme. Although Brightsight is not a FIPS accredited laboratory we often use the FIPS 140 standard as a reference in security evaluations of payment terminals.*	Pascal van Gimst	**Rejected:** Incomplete
486	R.V.	4.1			*The Smart Card Alliance is pleased to respond to NIST during this public comment period on DRAFT FIPS 140-3, Security Requirements for Cryptographic Modules.* *The significant increase in market usage of smart card technology for a wide variety of secure identification applications over the past ten years has shown a unique market demand and applicability for secure, microcontroller-based, portable cryptographic devices.* ***This includes key U.S. projects such as ePassport, CAC, PIV, TWIC, FRAC, and Registered Traveler.***	Randy Vanderhoof, Executive Director, Smart Card Alliance	**Rejected:** Incomplete

582	W. C.	4.1	Global	E	My comments include a lot of typo fixes and suggested changes to the prose. I marked the more substantive comments with "XXX" to make it easier to find them in this file. Throughout the standard, please change "**crypto officer**" and "**crypto-officer**" to the new term "**cryptographic officer**". I like the old term "crypto officer", but consistency is more important. *Is Security Level 2 still the highest overall security level that can be achieved by a software module?*	Wan-Teh Chang	**Accepted:** Consistency and typos will be addressed.
743	EW	4.1	Sec. 1.1		FIPS 140-3 adds an additional security level and incorporates extended and new security features that reflect recent advances in technology. In FIPS 140-3, each of the eleven requirement areas in redefined. Software requirements are given greater prominence in a new area dedicated to software security, and an area specifying requirements to protect against non-invasive attacks is provided. "…in redefined…" should read "…is (or have been) redefined…".	EWA	**Accepted:** As provided
53	H.F.	4.1	4. Second para	E	"The overall rating will indicate the minimum of the independent ratings received in the area". Consider rephrase to "The overall rating will be set to the lowest rating received in the independent security ratings.	Hildy Ferraido	**Accepted:** For review
55	H.F.	4.1	Section 4.1, second para		(Cryptographic Module Specification): states "Non-Approved functions can be performed if they are not used to provide security relevant functionality (e.g., a non-Approved algorithm may be used to encrypt data or keys but the result is considered plaintext and provides no security relevant functionality until encrypted with an Approved algorithm)." It is unclear which category of the non-approved security function (non-approved but allowed or non-approved and excluded from List B) can perform these security irrelevant functions. The statement is also unclear about the Mode to use for the function. Is it the intent for these security irrelevant functions to be performed in Approved Mode or Non-Approved Mode of operation?	Hildy Ferraido	**Accepted:** To be clarified and review

56	H.F.	4.1	Section 4.1.3		Please provide an example of Multiple Modes of Operations (similar to the example in 4.1.4).	Hildy Ferraido	**Rejected:** May be provided by CMVP guidance in the future.
66	J.C.	4.1	4.1		The first sentence would appear to rule out a FIPS compliant software product, WinZip, since it is only a software product. Is that the intent of the requirement? Or will the certification of WinZip like products be performed on a specified hardware platform, requiring multiple certifications for items like the current PC market (different processor manufactures, different feature levels in the processor, etc.)? Recommend changing "set of hardware and software that" to "set of hardware and/or software that".	James Cottrell-MITRE	**Accepted:** For review
67	J.C.	4.1	General		This applies to a number of paragraphs in this document. The content of the Annexes, in draft form, should be provided with the Standard, to ensure a complete review. Specifically details on "applicable requirements specified in Annex B" for Allowed security functions should be known to the reviewers of this standard for completeness.	James Cottrell-MITRE	**Accepted:** The 2nd draft published for review will contain drafts of the Annexes.
68	J.C.	4.1			This paragraph states "The hardware and software of a cryptographic module can be excluded from the requirements of this standard if the vendor can demonstrate that the excluded hardware and software does not affect the security of the module". What level of validation needs to be applied to a vendors claims that one or more component (hardware or software) does not affect the security of the module? Can NIST, or their testing laboratories, challenge a vendor's assumption/demonstration?	James Cottrell-MITRE	**Rejected:** Out-of-Scope. CMVP programmatic issue. **Suggestion**: change: the sentence to: "The hardware and software **associated with** a cryptographic module can be excluded from the requirements of this standard if the vendor can demonstrate that the excluded hardware and**/or** software does not affect the security of the module." If not changed it will imply that a subset of the "module included in the defined boundaries" is tested for compliance.
69	J.C.	4.1	General		For Security Levels 3, 4 and 5, how does the Cryptographic module have to provide an indication for all "Approved modes" and any "Non-Approved mode" if the Cryptographic module is capable of	James Cottrell-MITRE	**Accepted:** Clarification needed.

					simultaneously processing more than one request? Or is the indication the “ORing” of the use, or lack of use, for each simultaneous mode?		
70	J.C.	4.1			This paragraph states that “The requirements of this standard shall apply to all components within this boundary, including all hardware and software”. Paragraph 4.1 states “The hardware and software of a cryptographic module can be excluded from the requirements of this standard if the vendor can demonstrate that the excluded hardware and software does not affect the security of the module”. The statement in paragraph 4.1, while not a requirement, appears to conflict with this requirement. Recommended change: Either remove the quoted statement in paragraph 4.1 or add “(except those components that the vendor demonstrates do not affect the security of the module)” after “components” in the quoted statement of paragraph 4.1.2.	James Cottrell-MITRE	**Accepted:** Clarification needed
71	J.C.	4.1	4.13		Are there any special considerations if a Cryptographic module performs multiple Approved modes simultaneously? For example a Cryptographic module that is supporting secure email will be required to encrypt/decrypt email and/or sign/verify email. Is switching from email signature/verification to email encryption/decryption considered a change in Approved Modes of Operation?	James Cottrell-MITRE	**Accepted:** Clarification needed
72	J.C.	4.1	Sec. 4.1.3		The last bullet states “If re-configuration from one Approved mode of operation to another alters the physical security level of the module without changing the overall security level of the cryptographic module”. This standard does not define what is meant by physical security level. Is this trying to say if reconfiguring the Cryptographic Module from Approved Mode 1 to Approved Mode 2 requires physical modifications to the module, then all CSPs shall be zeroized in the Cryptographic Module during this reconfiguration? Recommendation: If this bullet is addressing “opening the box” to reconfigure the mode of operation, change “alters the physical security level of the module” to “violates (enters) the physical security	James Cottrell-MITRE	**Accepted:** Clarification needed

					enclosure of the module".		
73	J.C.	4.1	Sec. 4.1.3.2		Suggestion, the Cryptographic module be required to indicate that it is in a Degraded Functionality State. Recommend: Adding "The module shall indicate that at least one Approved mode of operation is degraded. It is desirable for the module to indicate the Approved mode(s) of operation that are degraded." After the fifth bulleted item.	James Cottrell-MITRE	**Rejected:** Not sure why this type of indicator is needed. Provide justification.
75	J.C.	4.1	Sec. 4.1.4		Suggestion, if the Cryptographic module performs "health tests" after an Approved mode of operation has begun (see Table 1 row 9), any detected failure from these health tests to an Approved mode of operation should declared non-operational. Recommend: Adding a bullet "If "operational health tests" (see Table 1 Row 9 for possible operational health tests) indicate that an Approved mode of operation is degraded, module shall indicate this Approved mode is non-operational, cease using this Approved mode of operation and isolate this Approved mode from the remaining security functions of the cryptographic module."	James Cottrell-MITRE	**Rejected:** Not sure why this type of indicator is needed. Provide justification.
76	J.C.	4.1	Sec. 4.1.5		Where are the "recommended security strengths" that are referenced in the second sentence defined?	James Cottrell-MITRE	**Accepted:** Add reference to the recommended security strengths
89	J.C.	4.1			Acronym MRI is used and not defined.	James Cottrell-MITRE	**Accepted:** To be edited.
131	J.R.	4.1	4.1.3		The overall security level of the module shall not be changed when configured for different Approved modes of operation. Comment: (Note) This tends to indicate that a module can have varying levels of security in each of	James Randall RSA	**Rejected:** Out of scope. The standard requires all approved modes of operation to provide the same security level. I do not see how "Each Approved mode of operation shall meet all the requirements of the security level of the

					the areas and a different overall security level. How is this meant to be handled from a module certificate point of view - currently only a single level is listed for the module itself and one level for each of the areas. Currently vendors which offer modules with multiple levels test each module as an independent submission - is this intended to allow a single module to be submitted for these sorts of situations? If so then it does not allow for the typical case of an overall level 2 and overall level 3 module. Perhaps a better way to handle this requirement is: Each Approved mode of operation shall met all the requirements of the security level of the module.		module." is making a difference.
132	J.R.	4.1	4.1		Approved security functions are listed in Annex A of this standard. Non-Approved security functions that are Allowed in an Approved mode, and the rules that govern their use, are listed in Annex B of this standard and in the FIPS 140-3 Implementation Guidance. Non-Approved functions can be performed if they are not used to provide security relevant functionality (e.g., a non-Approved algorithm may be used to encrypt data or keys but the result is considered plaintext and provides no security relevant functionality until encrypted with an Approved algorithm). Comments: These items should be covered in Annex B and clearly stated and not handled in IGs.	Janes Randall RSA	**Accepted:** Annex B should provide all necessary requirements for the listed Allowed security functions.
133	J.R.	4.1	4.1 Cryptographic Module Specification		In an Approved mode of operation a cryptographic module shall implement at least one Approved (listed in Annex A) or Allowed (listed in Annex B) security function. Certain non-Approved security functions are allowed for use in an Approved mode of operation. Allowed security functions used in an Approved mode of operation shall meet all of the applicable requirements specified in Annex B. Comments: The annexes in 140-2 list allowed algorithms and not requirements - is there a draft of the new Annex B?	James Randall RSA	**Accepted:** If a module only implements an Allowed security function, that module should not be identified as a cryptographic module. At a minimum a module shall implement at least one Approved security function that can be tested for compliance. Draft Annex B will be included in 2nd Draft

134	J.R.	4.1			A cryptographic module may be designed to support degraded functionality (e.g., a module may fail the self-test for one encryption algorithm and alternately use another encryption algorithm) within an Approved mode of operation. For a cryptographic module to implement a degraded functionality in an Approved mode of operation, the following shall apply: • Degraded operation shall be entered only upon the failure of pre-operational self-tests. Comments: it would make sense to include the continuous runtime tests in this wording. Basically if any of the required tests fail then that algorithm shall remain disabled until such time as the required tests succeed.	James Randall RSA	**Partially accepted:** Provide requirements for the case when degraded functionality is detected during operation (runtime) and not by pre-operational tests, rather than accepting the proposed rewording.
135	J.R.	4.1	4.1.3		If re-configuration from one Approved mode of operation to another alters the physical security level of the module without changing the overall security level of the cryptographic module, then the cryptographic module shall perform a zeroization of all CSPs within the module. Comment: (Note) What is the intent of this requirement? The overall level is the lowest level in each area and the overall level must not change **so all that is possible is an increase of the physical security level** to any values greater or equal to the overall security level. I think there is something intended here which isn't clearly stated.	James Randall RSA	**Partially accepted:** The standard shall be rephrased to state that the physical security of a module can not be changed (also remove bullet 6th) 4.1.3.1 - Resolved in Draft 2.

143	J.R.	4.1	4.1 para 3		The hardware and software of a cryptographic module can be excluded from the requirements of this standard if the vendor can demonstrate that the excluded hardware and software does not affect the security of the module. Comments: It is unclear what the intent of this statement is - given that there are existing requirements imposed on non-approved functions and other areas which are not linked to "the security of the module". A statement of this effect enables all requirements to be argued as non-relevant based on an argument of the merits of the approach from a security perspective. This is open to abuse.	James Randall RSA	**Accepted**: See also the other comments addressing the same paragraph.
149	J.R.	4.1	4.1 Cryptographic Module Specification		A cryptographic module shall be a set of hardware and software that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary. Comment: This wording precludes the current treatment of software modules. 140-2 makes it clear that it is a combination of hardware, firmware and/or software. Software based 140-2 cryptographic modules are validated and reviewed and although tested on hardware devices these are not part of the module as such - the IG's are very clear on this in terms of "porting" of software and running of software on GPCs which are not the same physical embodiment as the platform tested by the validation lab.	James Randall RSA	**Accepted**: See previous comments referring to this paragraph. **Solution**: change to match the definition: “A cryptographic module shall be a set of hardware and/or software that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.”
150	J.R.	4.1	4.1.4		The module shall remain in the degraded mode until failed test(s) have all been passed. Comments: (Insert) pre-operational self- (failed (pre-operational self-)test)	James Randall RSA	**Accepted**: to be edited to clarify how a degraded mode is detected/entered/terminated. See also comment 134

167	J.R.	4.1	4.1.2		A cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical boundary of a cryptographic module. The requirements of this standard shall apply to all components within this boundary, including all hardware and software. The cryptographic boundary shall include the processor(s) and other hardware components that provide for the operational environment of the module. Comment: (Note) These requirements do not handle the concept of a software based module which operates on a general purpose computer provided by the ultimate end-user. Which components provided by the end-user are part of the module itself? How are these components if specified as inside the cryptographic boundary meant to be tested?	James Randall RSA	**Accepted**: To be edited. **Suggestion**: change to: "A cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical and/or logical boundary of a cryptographic module."
183	J.C	4.1			Acronym CBC is used and not defined.	James Cottrell-MITRE	**Accepted**: To be edited.
184	J.B.	4.1	Sec. 4.1.5		The requirements in sec. 4.1.5 Security Strength of the Module are unclear as it is not apparent how this will be determined. The method of determining this for cryptographic mechanisms is well understood but not for a module as a whole. Therefore it is difficult to comment on this requirement without guidance as to how it will be assessed.	Jason Bennet-Thales e-Security	**Accepted**: To be edited.
199	J.H.	4.1	Sec. 4.1.5		"The security strength … shall be no larger than the minimum security strength of the Approved and Allowed security functions …"How does this apply in the case of a general-purpose module whose interface is provided by an API that has to support a range of algorithms and key lengths used in various customer applications? It seems that such a module may be penalized because, for example, it must support AES 128, 192 and 256 to satisfy different customer requirements and would, therefore, have a published security strength of 128 bits where a single purpose module that supports AES 256 only would have a security strength of 256 bits. To a potential customer, this would make the general-purpose module appear to be "weaker" than the	Johnn Hsiung - for - SafeNety	**Partially Accepted:** Security strength of a module will be redefined for now and then analyse the issue!! The reviewer is wrong in its assumption/understanding of section 4.1.5

					single-purpose module. More seriously, I could imagine Federal departments and agencies, for example, mandating modules of a specific security strength and a general-purpose module would be ruled out even though it can provide the appropriate algorithm(s) and key sizes to satisfy their security strength requirements.		
201	J.R.	4.1	4.1.3		Pre-operational self-tests shall be performed for all Approved and Allowed security functions used in the selected Approved mode of operation. Comments: (Note) The wording allows for delay of pre-operational self-tests as described in the glossary for "pre-operational test"; however the reader could easily overlook that here. It should be explicitly stated.	James Randall RSA	**Accepted**: to be edited.
249	J.K.	4.1	4.1.1		The meaning of “software” in hardware and hybrid module seems to be different from the one defined in section 2.1. “Hardware module is a module composed primarily of hardware, which may also contain some firmware.” “Hybrid module is a module whose cryptographic functionality is primarily contained in firmware,”	JCMVP6	**Partially accepted:** requires clarification. It also require inclusion of “firmware” as the term is used in the Appendix C. Alternatively, remove the term in appendix
250	J.K.	4.1	4.1		The contents in FIPS 140-2 IG 1.2 are not reflected. The contents should be reflected in FIPS 140-3. Add the following statement in 4.1 or in 4.8.6. “A cryptographic module shall zeroize CSPs when switching from an Approved mode of operation to a non-Approved mode of operation, and vice versa.”	JCMVP5 Junichi Kondo	**Accepted**: to be edited

251	J.K.	4.1	Sec. 4.1		What are the differences between “Allowed” and “Approved” security functions? The differences are not clear only from the definition in section 2.1. Does CAVS perform algorithm test for “Allowed” security function?	JCMVP4	**Rejected**:
265	J.R.	4.1	N/A		General Comment –FIPS 140-3 does not acknowledge the use of cryptography approved by the National Security Agency as an appropriate alternative for organizations. Comments: It should contain this information.	NSA/SETA/SAIC, Joe Ruth, 410-865-7960	**Rejected**:
291	J.L.	4.1	4.1		Third para - ”The hardware and software of ...” Suggest some guidance be added as to what is acceptable and does it vary per 'security level.' Adds clarity and makes the document more user friendly.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted**: Addressed by other comments above.
293	R.A.	4.1	4.1.3		A cryptographic module may be designed to support multiple Approved modes of operation. For a cryptographic module to implement more than one Approved mode of operation, the following shall apply: Comment: Can the module go from an unapproved mode of operation to an approved mode of operation?	NSA/SETA/ SPARTA Rowland Albert, 410-865-7992	**Answer:** Yes, see Draft 2 provides the requirements
294	J.W.	4.1	4.1.5		The security strength of the module shall be specified. The security strength of the module shall be one of the recommended security strengths, and shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation. Comments: Change “larger” to “smaller” / strength must be larger than or equal to “minimum”	BAH/NSA I181 SETA Jay White, 410-684-6675	**Rejected**: Don’t see the reason for the change. It is required the strength to be not larger than minimum – it can be equal or lower… **NOTE** Draft 2 redefines the security strength.

295	J.L.	4.1	4.1.5		This para needs a ref. to provide guidance on how to determine a security strength, and how to recommend them per security level. Required for clarity and to make the document user friendly. "4.1.5 Security Strength of the Module The security strength of the module shall be specified. The security strength of the module shall be one of the recommended security strengths, and shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation."	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted**: also addressed by previous comments
322	AN	4.1			"A cryptographic module shall be a set of hardware and software." Comment: This does not appear to be consistent with the definition of a software module in Section 4.1.1 which states that a software module is a module that is "composed solely of software."	Anonymous	**Accepted**: Addressed by other comments above
323	AN	4.1	Selection 4.1.1		Comment: Strongly suggest making the requirements for all module "types" the same, in order to provide a consistent level of assurance across all embodiments. Given a hostile global communication and network infrastructure, a more pragmatic solution might be to validate software modules to a maximum of Security Level 1.	Anonymous	**Rejected**: not justified
324	AN	4.1	Sec. 4.1.3		"If re-configuration from one Approved mode of operation to another alters the physical security level of the module without changing the overall security level of the cryptographic module, then the cryptographic module shall perform a zeroization of all CSPs within the module." Comment: Typo: Need to zeroize the PSPs too for Level 5?	Anonymous	**Obsolete:** See above comment – no change in physical security is allowed – see Draft 2
325	AN	4.1			The security strength of the module shall be one of the recommended security strengths, and shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation." Comment: Typo: Should be no less than the	Anonymous	**Obsolete:** Misunderstanding. Other comments show the same misunderstanding. See Draft 2 for redefinition of the Security Strength

					minimum.		
346	R.A.	4.1	Sec. 4 line 3		add "disposal of equipment"	NSA/SETA/ SPARTA; Rowland Albert, 410-865-7992	**Accepted**: to be edited – in paragraph :" The security requirements cover areas related to the design, implementation and operation of a cryptographic module. "
347	A.G.	4.1	All		Add a Table similar to Table 1 that maps FIPS 140-2 security requirements and levels to the new security levels and requirements for FIPS 140-3 or a table that highlights only the new requirements and changes from FIPS 140-2 to FIPS 140-3.	NSA (JHU APL); Anne Gugel	**Partially accepted :** A separate document will provide it
348	J.L.	4.1	Sec. 4.1		Third para - "The hardware and software of ..." Suggest some guidance be added as to what is acceptable and does it vary per 'security level.' Adds clarity and makes the document more user friendly.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted**: Addressed by other comments.
393	J.K.	4.1	4.1.5		Will it be able to implement the digital signature verification function with1024 bits modulus size (i.e. 80bit security strength) for the backward compatibility in an Approved mode of operation even after year 2011?	JCMVP8 Junichi Kondo	**Rejected:** out-of-scope of 140-3:
394	J.K.	4.1	4.1.3		What situation is intended by this requirement? Is it reasonable to alter the physical security level by re-configuration? It is preferable to disallow the change of the physical security level by configuration. The last requirements in section 4.1.3 should be deleted.	JCMVP7 Junichi Kondo	**Rejected**: Please provide justification
395	J.K.	4.1			"Hardware module is a module composed primarily of hardware, which may also contain some firmware." "Hybrid module is a module whose cryptographic functionality is primarily contained in firmware,"	JCMVP Junichi Kondo	**Partially accepted**: See above comments. **Draft 2 brings back the firmware notion**

444	R.A.	4.1			Add a section which will include all requirements that were in FIPS Pub 140-2 that are not in FIPS Pub 140-3	NSA/SETA/ SPARTA; Rowland Albert, 410-865-7992	**Partially accepted**: A separate document will be provided
445	J.R.	4.1	N/A		General Comment - NIST Special Pub 800-53 contains Cryptographic Module Verification information and is not referenced in this document.	NSA/SETA/SAIC, Joe Ruth, 410-865-7960	**Rejected:** SP 800-53 is an over arching doc that shall points to 140-3 for CMP – not the opposite**.**
454	J.L.	4.1	Sec. 4.1.5		This para needs a ref. to provide guidance on how to determine a security strength, and how to recommend them per security level. Required for clarity and to make the document user friendly.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted**: Addressed by previous comments
508	T.K.	4.1	Sec. 4.1		the first sentence in the section begins with: "A cryptographic module shall be a set of hardware and software…" Should that read "hardware or software" (or "hardware and/or software") vice "hardware and software"? In Appendix C, would it be possible to explicitly state (minimum) inspection requirements for TELs? A number of approved modules require daily inspection of TELs, still others are quite vague concerning the required periodicity.	Tim Kramer IA Analyst NETWARCOM Office of the ODAA	**Accepted**: addressed by previous comments
520	T.C.	4.1			MSI - New acronyms cause more confusion. API is a perfectly acceptable acronym in this case, and can even keep the same definition as MSI.	Tom Casar	**Rejected**
521	T.C.	4.1			Table 1 - No DAC in Level 2	Tom Casar	
522	T.C.	4.1	Sec. 4.1		See Comment 1. Also, should not mention the IG here	Tom Casar	**Accepted**: Addressed by other comments too
523	T.C.	4.1	Sec. 4.1.		Non-operational Approved security functions shall be isolated from the remaining Approved security functions of the cryptographic module. What do you mean by this requirement and what is the test for it?	Tom Casar	**Accepted**: Provide clarification
532	T.I.	4.1	Sec. 4.1.0		As an instance of a cryptographic module, there provides the software module constituted only by software in 4.1.1; however, the 4.1.2 describes that such processor implementing the software should also be included in that cryptographic boundary – this shows somewhat inconsistency. Since software module is constituted by hardware, OSs and software, it leads misunderstanding unless describing cryptographic boundary is set within physical boundary by configuring the physical boundary. Add "define a physical boundary and define a code	Toru Ito - Cryptrec & INSTAC	**Partially accepted:** Draft 2 rewords it

					boundary in it." on the 4.1.2.		
533	T.I.	4.1	Sec. 4.1.3		In the 5th paragraph, “If re-configuration from one Approved mode of operation to another alters the physical security level of the module without changing the overall security level of the cryptographic module, then the cryptographic module shall perform a zeroization of all CSPs within the module.”:	Toru Ito - Cryptrec & INSTAC	**Rejected:** No comment
534	T.I.	4.1	Sec. 4.1.3		About “the physical security level”;	Toru Ito - Cryptrec & INSTAC	**Rejected:** No comment
535	T.I.	4.1	Sec. 4.1.3		Does this mean the security level relevant to the requirements of Physical Security described in the 4.6 or the security level is also included/described in 4.7 or does this mean other than that. It needs to be clarified. (It refers the description of FIPS140-2IG.)	Toru Ito - Cryptrec & INSTAC	**Accepted**: To be clarified
536	T.I.	4.1	Sec. 4.1.3		About The parameters needs to be zeroization, is the timing adequate to define when “the physical security level” is changed (It won’t be a problem if “the overall security level” would not be changed?.	Toru Ito - Cryptrec & INSTAC	**Obsolete:** See the resolutions above (physical security can not change)
549	B. W.	4.1	Sec. 4.5.1		Is it possible to have a module that has different security strengths for different modes?	Bridgete Walsh - CSE	**Rejected:** out-of-scope
555	J.C.	4.1			The acronym CMS is generally used in cryptography as "crypto message syntax". Suggest not using the acronym at all in the standard and just using the long form since it is not used often.	Jean Campbell - CSE	**Accepted**: To be edited
557	J.C.	4.1			The concept of one-way function should be mentioned.	Jean Campbell - CSE	**Accepted**: To be edited
558	J.C.	4.1			Sentence should read: ... that determines operations including but not limited to:"	Jean Campbell - CSE	**Rejected:** Pease provide location
559	J.C.	4.1			DAC should also be defined.	Jean Campbell - CSE	**Accepted**: To be edited
560	J.C.	4.1			The term should be renamed to "compromising emanation" or "CE"	Jean Campbell - CSE	**Accepted**: To be edited
561	J.C.	4.1			The definition should be changed to "measure of uncertainty of a random variable relative to ... something..."	Jean Campbell - CSE	**Accepted**: To be edited

562	J.C.	4.1			Hardware: the physical equipment within the cryptographic boundary used to process programs and data (includes non-reprogrammable software). Comments: Isn't this firmware?	Jean Campbell - CSE	**Accepted:** Firmware re-introduced back in Draft 2
563	J.C.	4.1			Implementation guidance: a set of documents published during the lifetime of the standard which provides additional clarification, testing guidance and interpretations of the standard. (Implementation guidance cannot change or add requirements to the standard.) IGs should not be part of the standard. They are a programmatic entity, not a standard entity.	Jean Campbell - CSE	**Accepted**: To be edited
566	J.C.	4.1	Sec. 4.1.4		4.1.4 Degraded Functionality Comments: Title should be changed to Degraded Modes of Operation	Jean Campbell - CSE	**Rejected**: - I don't think is correct
567	J.C.	4.1			The module shall remain in the degraded mode until failed test(s) have all been passed Comments: New requirements: - remaining functionality must not degrade Security Strength of the module - the module shall have status indicator when in degrade mode of operation.	Jean Campbell - CSE	**Accepted**: To be edited
568	J.C.	4.1	Sec. 4.1.5		4.1.5 Security Strength of the Module The security strength of the module shall be specified. The security strength of the module shall be one of the recommended security strengths, and shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation. Comments: What does that mean for several implemented key strengths?	Jean Campbell - CSE	**Accepted**: To be clarified

639	T.K.	4.1	Sec. 4.1		Please consider the following as part of the Request for Public Comment for the draft FIPS 140-2. I have the following two questions/comments: In section 4.1, on page 16, the first sentence in the section begins with: "A cryptographic module shall be a set of hardware and software…" Should that read "hardware or software" (or "hardware and/or software") vice "hardware and software"? In Appendix C, would it be possible to explicitly state (minimum) inspection requirements for TELs? A number of approved modules require daily inspection of TELs, still others are quite vague concerning the required periodicity. Very respectfully,	Tim Kramer	**Accepted**: addressed by previous comments
650	W. C.	4.1			Consider defining PIN.	Wan-Teh Chang	**Accepted**: To be edited
654	W. C.	4.1	Sec. 4.1		There is some redundancy in the descriptions of Approved (Annex A) and Allowed (Annex B) security functions in this paragraph and the next paragraph. At the end of the last sentence "(see Appendix C.)", move the period outside the closing parenthesis. Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Accepted**: To be edited
655	W. C.	4.1	Sec 4.1.3		The first bullet item says "The overall security level of the module shall not be changed when configured for different Approved modes of operation." This means a module won't be able to have a Level 1 mode and a Level 2 mode. Is this restriction intentional? Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Accepted**: addressed above
656	W. C.	4.1	Sec. 4.1.4		1st paragraph of the section: Consider changing "alternately use another encryption algorithm" to use an alternative encryption algorithm.	Wan-Teh Chang	**Accepted**: To be edited

749	EW	4.1	Sec. 4.1		A cryptographic module shall be a set of hardware and software that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary. In an Approved mode of operation a cryptographic module shall implement at least one Approved (listed in Annex A) or Allowed (listed in Annex B) security function. Certain non-Approved security functions are allowed for use in an Approved mode of operation. Allowed security functions used in an Approved mode of operation shall meet all of the applicable requirements specified in Annex B. The operator shall be able to determine when an Approved mode of operation is selected. All Approved modes of operation shall be specified in the module Security Policy (see Appendix C.) "..a set of hardware and/or software… This statement is incomplete without Annex B. As it currently reads, the statement would seem to indicate that, as an example, a module could implement Diffie-Hellman without any approved security functions and still be validated. Approved security functions are listed in Annex A of this standard. Non-Approved security functions that are Allowed in an Approved mode, and the rules that govern their use, are listed in Annex B of this standard and in the FIPS 140-3 Implementation Guidance. Non-Approved functions can be performed if they are not used to provide security relevant functionality (e.g., a non-Approved algorithm may be used to encrypt data or keys but the result is considered plaintext and provides no security relevant functionality until encrypted with an Approved algorithm). Non-Approved security functions may also be used in non-Approved modes of operation. The IG document should not be referenced in the standard since it (the IG) isn't part of the FIPS 140-3 standard. Any updates to the list of Allowed security functions should be added to Annex B. The hardware and software of a cryptographic	EWA	**Accepted**: re: the IG reference.

					module can be excluded from the requirements of this standard if the vendor can demonstrate that the excluded hardware and software does not affect the security of the module. "The specific hardware and software of a cryptographic module…"		**Accepted:** To be edited
750		4.1	Sec. 4.1.1		Hybrid module is a module whose cryptographic functionality is primarily contained in software, which also includes some special purpose hardware within the cryptographic boundary of the module. Not well defined. A hybrid module is a vendor supplied software module that requires a specific hardware component on the platform on which it is loaded in order to function properly as a cryptographic module.	EWA	**Rejected**
751	EW	4.1	Sec. 4.1.3		The overall security level of the module shall not be changed when configured for different Approved modes of operation. In consideration of the 5th (last) bullet, why can't a configuration change result in a different overall security level? For example, connecting a console port for management purposes only could result in a security level 3 module being downgraded to a security level 2 module. Pre-operational self-tests shall be performed for all Approved and Allowed security functions used in the selected Approved mode of operation. How can this be enforced for non-FIPS approved algorithms?	EWA	**Rejected:** The standard states one security level for all allowed modes- there is one field in the certificate. Testing validation issue – changing of security level generates a new module that shall req. a new validation.

752	EW	4.1	Sec. 4.1.4		A cryptographic module may be designed to support degraded functionality (e.g., a module may fail the self-test for one encryption algorithm and alternately use another encryption algorithm) within an Approved mode of operation. For a cryptographic module to implement a degraded functionality in an Approved mode of operation, the following shall apply: Should there not be the choice to either continue in the degraded state (e.g. use Triple-DES instead of AES due to the failure of the AES KAT) or remain in an error state? Failure to an unexpected mode of operation should not be allowed.	EWA	**Accepted**: To be clarified. The transition from degraded / error to normal
753	EW	4.1	Sec, 4.1.4		Non-operational security functions shall be isolated from the remaining security functions of the cryptographic module. Not clear what is meant by isolated. Can't be called or utilized? If, for example, the module is a software library, how would the function be isolated?	EWA	**Accepted**: To be clarified
754	EW	4.1	Sec. 4.1.5		The security strength of the module shall be specified. The security strength of the module shall be one of the recommended security strengths, and shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation. An overall strength of the module is not relevant because it is attempting to assign a number to a module when the module may simply provide a range of options. Furthermore, if a degraded mode of operation is allowed, then the security strength of the module could only be the minimum strength of the degraded mode. Strength of function is dependent on the algorithm being used. Why mention Allowed security functions? As defined in section 4.1, Cryptographic Module Specification, Allowed functions provide "no security relevant functionality". The inclusion of MD5 as an Allowed function would result in the security strength of the module being undefined.	EWA	**Obsolete:** Draft 2 redefines the security strength of a module

759	EW	4.1	4.8.4 & 4.3.2		During manual SSP entry, the entered values may be temporarily displayed to allow visual verification to improve accuracy. Allowing display of passwords being entered is contradictory to 4.3.2, Operator Authentication	EWA	**Rejected: –** needs research – see section 4.8.4 – it allows it. 4.3.2 – req. password ONLY masked
790	IG	4.1	Sec. 4.1		Recommend changing the definition of the module as follows: A cryptographic module shall be a set of hardware and software that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, all of which is contained within a defined cryptographic boundary. Note: The purpose of this proposed change is to prevent a crypto boundary from being drawn which attempts to limit the scope of functionality to just the cryptographic primitives (purposefully keeping many FIPS-relevant features outside the boundary). FIPS should clarify when crypto primitives alone may be validated without referencing key management functions that use them; many products employ unevaluated key management mechanisms (particularly in software libraries).	Inforgard	Partially addressed previously
791	IG	4.1	Sec. 4.1		The note on exclusions should be clarified to mean that an excluded component is still within the purview of FIPS (meaning one cannot make changes to, or remove, the excluded component without incurring some measure of re-validation), though not required to conform to one or more FIPS requirements.	Inforgard	**Rejected:** Clarifications will be provided by DTR and IG
792	IG	4.1	Sec. 4.1		Last sentence: Recommend changing as follows: “In addition to the requirements of Security Level 2, for Security Levels 3, 4 and 5, a cryptographic module shall, after having been properly initialized per operator guidance, indicate when an Approved mode of operation is selected. Note: It should be better formalized what a module must do for itself after leaving control of the manufacturer. Some types of modules may require some user action, if only the smallest procedure, to bring it into a FIPS-Approved mode from that time forward.	Inforgard	**Accepted:** To be edited

793	IG	4.1	Section 4.1.1		The classification of 'hybrid module' seems superfluous. There is only one requirement in this standard that relates to a 'hybrid' module.	Inforgard	**Rejected:** Please provide additional information
794	IG	4.1	Sec. 4.1.3		There is no mention of the former IG requirements concerning how a module must transition between Approved and non-Approved modes, or what the requirements in general are for a non-Approved mode.	Inforgard	**Accepted**: To be edited (from IG)
795	IG	4.1	Sec. 4.1.4		Degraded Functionality: It's not clear under what circumstances a module may exit the error state (entered due to failure of the self test) – hence not be under the error state requirements – and enter the 'degraded mode.' May this error state be an infinitesimally short time, effectively negating such requirements as prohibition of data output, or will those error state requirements only apply to a 'channel' which was directly affected by the algorithm whose self test failed? Also, the 'pre-operational' integrity test needs to be excluded from the possibility of entering a degraded mode.	Inforgard	**Accepted**: To be clarified. Other comments addressed it
796	IG	4.1	Sec. 4.1.5		The 'security strength of the module' concept is an over-simplification of the numerous aspects of a module's security, many of which are outside the control of the module and better described in a larger system context. Perhaps we should define 3 different security strengths to be specified in the security policy: 1) encryption security strength, 2) cryptographic authentication strength, and 3) Role or Identity authentication strength.	Inforgard	**Rejected.** Please provide justification
833	IG	4.1	Sec. 4.1.4		It is not clear that this is also for 'Allowed Security Functions'.	Inforgard	See Draft 2 for clarifications

875	AT	4.1			•Add definition for Temporary Key Values (TKV). The definition would be “any temporary variables or memory locations used to store intermediate SSP components during cryptographic calculations. These values include, but are not limited too, memory locations or variables used to store key schedule values, intermediate values of modular exponentiation operations, and intermediate keyed digest values.” Defining this new term will allow for further expansion of the key zeroization requirements. Most vendors currently only zeroize the entire key component rather than the individual parts when the key is used. This would be a good Level 4+ requirement to add. “Critical Security Parameter” should be replaced with “Critical Security Parameter (CSP)” • Add definition for Temporary Key Values (TKV). The definition would be “any temporary variables or memory locations used to store intermediate SSP components during cryptographic calculations. These values include, but are not limited too, memory locations or variables used to store key schedule values, intermediate values of modular exponentiation operations, and intermediate keyed digest values.” Defining this new term will allow for further expansion of the key zeroization requirements. Most vendors currently only zeroize the entire key component rather than the individual parts when the key is used. This would be a good Level 4+ requirement to add. “Critical Security Parameter” should be replaced with “Critical Security Parameter (CSP)”	Atlan	**Accepted**: to be edited
882	AT	4.1	Sec. 4.1.3		•Section 4.1.3 – Multiple Approved Modes of Operations Recommend removing last bullet per earlier comment on physical security. Physical security level should not included when calculating overall security level.	Atlan	**Accepted:** See Draft 2

891	AT	4.1	Sec. 4.1.4		•Section 4.1.4 – Degraded Functionality, third bullet "Non-operational security functions shall be isolated from the…" What type of isolation is required? Is it simply that the non-operational function cannot be performed? Or does it also pertain to the cryptographic key that the non-operational function might use? For instance, assuming a module only has one AES key, if an AES ECB self-test fails, but the AES CBC self-test passed, can one still use the single AES in CBC mode?	Atlan	**Accepted:** See Draft 2
909	CL	4.1	Sec. 4.1.5		"The security strength of the module shall be specified." In addition to the minimum security strength of the module, should the minimum security strength of each Approved mode of operation also be listed?	CEAL	**Rejected.** Please provide justification.
910	CL	4.1	Sec. 4.1.2 para 1		Section 4.1.2 – Paragraph 1 "The requirements of this standard shall apply to all components within this boundary, including all hardware and software." Shouldn't it be stated that the requirement don't apply to excluded components?	CEAL	**Rejected:** No change needed
911	CL	4.1	Sec. 4.1.2 para 1		Section 4.1.2 – Paragraph 1 "A cryptographic boundary shall consist of an explicitly defined perimeter" Why was the requirement for a "contiguous" perimeter removed? For software and hybrid module, is a logical boundary required in addition to a physical boundary? If so the standard should be clear on that.	CEAL	**Partially accepted:** Rewrite for clarification
935	CL	4.1			"non-Approved modes of operation" Please clarify whether a non-Approved mode applies only to a module which can change modes via configuration after it has entered operation; or if it also applies to a module which can be installed in a non-Approved manner. .	CEAL	**Rejected.** Please provide justification
947	CL	4.1	Sec. 4.1.3		Should the requirement from FIPS 140-2 IG 1.2, prohibiting the sharing of CSPs between multiple Approved modes of operation, be incorporated into the FIPS 140-3 requirements for multiple Approved modes?	CEAL	**Obsolete**: Changes were made in Draft 2

978	IG	4.1	Sec. 4.1.5		The security strength of the module shall be one of the recommended security strengths, (...)" – Where are the recommended security strengths specified?	Utimaco/InforGard	**Partially accepted**: Draft 2 redefines security strength. Reference shall be included
1026	R.E.	4.1	4.1		A cryptographic module shall be a set of hardware and software that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary. In an Approved mode of operation a cryptographic module shall implement at least one Approved (listed in Annex A) or Allowed (listed in Annex B) security function. Certain non-Approved security functions are allowed for use in an Approved mode of operation. Allowed security functions used in an Approved mode of operation shall meet all of the applicable requirements specified in Annex B. The operator shall be able to determine when an Approved mode of operation is selected. All Approved modes of operation shall be specified in the module Security Policy (see Appendix C.)	Randy Easter - NIST	**Rejected.** Please provide justification**:** No comment
1039	R.E.	4.1	4.1.3		A cryptographic module may be designed to support multiple Approved modes of operation. For a cryptographic module to implement more than one Approved mode of operation, the following shall apply:	Randy Easter - NIST	**Rejected:** No comment provided
1042	R.E.	4.1	4.1.4		A cryptographic module may be designed to support degraded functionality (e.g., a module may fail the self-test for one encryption algorithm and alternately use another encryption algorithm) within an Approved mode of operation. For a cryptographic module to implement a degraded functionality in an Approved mode of operation, the following shall apply:	Randy Easter - NIST	**Not Accepted:** No comment provided
1046	R.E.	4.1	4.1.5		The security strength of the module shall be specified. The security strength of the module shall be one of the recommended security strengths, and shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation.	Randy Easter - NIST	**Rejected:** No comment provided

966	I.F.	4.1			The security strength shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation. If the module supports a number of algorithms, including the weaker FIPS-approved ones (for backward compatibility), does this result in a reduction in the security strength of the module to that of the weakest supported algorithm? How do you determine the strength of the module when the module implements a security protocol such as TLS?	Indra Fitzgerald	**Rejected:** Security strength removed.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
51	H.F.	4.2	4.2		(Cryptographic Module Physical Ports and Logical Interfaces) states: " The data output for a given communication channel, shall be disabled while performing key generation. A smart card (a single chip Cryptographic module) generates an asymmetric key-pair in the module and returns the public key material over a communication channel back to the administrator. Giving the quoted statement above, does FIPS 140-3 disallow the public key communication as output? Or is the output of the public key material considered an action after the generation period, in which case the communication channels is opened.	Hildy Ferraiolo	Text removed from the FIPS 140-2 Draft 2
77	J.C.	4.2	Sec. 4.2		The first sentence states “A cryptographic module shall restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module”. Is the cryptographic module’s power and ground considered a “physical access port”? Does this requirement mean that all cryptographic modules have to eliminate any RF signals that provide unintended “information flow” regarding information being processed (data, keys, etc.) by the cryptographic module?	James Cottrell- MITRE	**Accepted:** Text will be clarified. **NOTE:** Any port that allows an informational flow shall be identified. In this case the cryptographic module is assumed operating in a benign environment.
78	J.C.	4.2	Sec. 4.2		The second paragraph states “The data output, for a given communication channel, shall be disabled while performing key generation, manual key entry, self-tests, software loading and zeroization”. The process of loading software could affect ALL communications channels in the cryptographic module, or a software load might only affect a specific channel. The loading software process could be designed to be effective upon cryptographic module restart (power cycle). Is it necessary that any software loading must disable channel output?	James Cottrell- MITRE	Text removed from the FIPS 140-2 Draft 2

79	J.C.	4.2	Sec. 4.2		Recommend changing “All electrical power externally provided to a cryptographic module (including power from an external power source or batteries) shall enter via a power port” to “All electrical power externally provided to a cryptographic module (including power from an external power source or batteries) shall enter via one or more power port(s)”. It may not be possible to provide prime power for the cryptographic module and any battery backup on the same port. Another wording change to the original would be change “power port” to “power interface”, which would allow multiple power lines of different kinds.	James Cottrell- MITRE	**Accepted:** Text will be modified. **NOTE:** We will define “power interface” and replace here “power port” with “power interface”.
98	C.P.	4.2	Sec. 4.2		Standard: Data output Interface: “For a given communication channel, all data output via the “data output” interface shall be prohibited when an error state exists and prior to successfully passing the pre-operational Software Integrity Test.” Suggestion: “For a given communication channel, all data output via the “data output” interface shall be prohibited when an error state exists and prior to successfully passing the pre-operational self-tests.”	Claudia Popa - CSE	**Accepted:** Text will be changed as suggested
145	J.R.	4.2	Sec 1.2 para 3		1.2 Security Level 2 Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals, or for pick-resistant locks on removable covers or doors of the module. Comment: (This description is very hardware focused and should be generic - describing the concepts of tamper evidence using both hardware and software terminology. Software based modules are currently possible in FIPS140-2 at level 2 - and this description should reflect that.) Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the Critical Security Parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are	James Randall RSA	

					placed on covers or doors to protect against unauthorized physical access. Security Level 2 requires role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services. Security Level 2 allows the software components of a cryptographic module to be executed on a general purpose computing system using an operating system that • provides discretionary access controls that protect against unauthorized execution, modification, and reading of cryptographic software, and • provides audit mechanisms to record modifications, accesses, deletions, and additions of cryptographic data and sensitive security parameters. An operating system implementing these controls provides a level of trust (logical protection) so that cryptographic modules executing on general purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems. This description is very hardware focused and should be generic - describing the concepts of tamper evidence using both hardware and software terminology. Software based modules are currently possible in FIPS140-2 at level 2 - and this description should reflect that.		
185	J.B.	4.2	Sec. 4.2		The requirements in sec. 4.2 Cryptographic Module Ports and Interfaces for protection against leakage of sensitive data during defined operations have been changed from FIPS140-2 so as to mandate module behaviour that will be unacceptable to some end users. In FIPS 140-2 the requirement is only for the output data path to be logically disconnected when performing key generation, manual key entry or key zeroization. For FIPS 140-3 this has been changed to the data output for a given communication channel (although the term communication channel is not clearly defined) shall be disabled while performing key generation, manual key entry, self tests, software loading and zeroization. The operational requirements	Jason Bennet-Thales e-Security	Text removed from the FIPS 140-2 Draft 2

					of many modules require that the data output interface may not be interrupted either for performance or network integrity reasons. So for a module that generates local keys with peers over the data output interface, using a key exchange mechanism such as Diffie-Hellman, the performance will be severely limited as this interface must be disabled when performing the key generation part of this operation. With relation to network integrity some protocols, such as SONET, expect that a continuous data stream is received from connected equipment. Therefore disabling the data output interface will cause an error condition to be assumed and appropriate alarms will be raised. Thales e-Security believes that the requirement, as specified in FIPS 140-2, should remain unchanged in FIPS 140-3 due to operational reasons shown above. FIPS 140-3 should provide assurance against leakage of sensitive data using logical separation of circuitry and processes rather than disablement of the data output interface.		
244	J.K.	4.2			In Table 1, “Cryptographic Module Ports and Interfaces” should be “Cryptographic Physical Ports and Logical Interfaces”. Comments: Rewrite the field as follows: “Cryptographic Module Physical Ports and Logical Interfaces”.	JCMVP1 Junichi Kondo	**Accepted:** Table will be updated as suggested
248	J.K.	4.2	4.2		What is the definition for “security strength of the Trusted Channel”? Define the security strength of the Trusted Channel	JCMVP10 Junichi Kondo	Text removed from the FIPS 140-2 Draft 2
296	J.L.	4.2	4.2		The last para needs to be amplified to provide guidance on how to determine a security strength, and how to recommend them per security level. At the least, a reference to guidance on the method of determining security strength should be included. Required for clarity and to make the document user friendly;	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	Text removed from the FIPS 140-2 Draft 2
344	J.L.	4.2	Sec. 2.2		The acronym list is incomplete; terms are missing, for example, ECDSA, DSA; a person should search the document for all acronyms and modify the list as necessary. Makes the document more user friendly,	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Rejected:** ECDSA and DSA are not mentioned in the document

					complete and adds clarity		
361	J.K.	4.2	4.2		"Table listing of all ports and interfaces (physical and logical)." Rewrite in the following: Table listing of all physical ports and logical interfaces.	JCMVP43	**Accepted:** Change text as suggested.
392	J.K.	4.2	4.2		Do the self-tests include conditional self tests? If so, the data output from all threads shall be disabled when a thread is performing conditional self-tests. It is not good for multi-thread software. Rewrite self-test as pre-operational self-test.	JCMVP9 Junichi Kondo	**Accepted:** Text will be clarified in 4.2 and 4.9 sections
509	T.K.	4.2	Sec. 1.2		In Part 1.2 "Security Level 2", the first paragraph describes the addition of a requirement for tamper-evidence (over Level 1 requirements). In working in IA for the last decade, I've had numerous opportunities to read the various Security Profiles for various products and have noted that FIPS does not set a minimum periodicity for the inspection of tamper-evident protections. Instead, it appears that the manufacturers/vendors have set a number of differing inspection periods. My question is: would it be valuable to define a minimum periodicity for inspection, of tamper evident protections, within FIPS 140-3?	Timothy L Kramer	**Rejected** – out-of-scope of FIPS 140-3
525	T.C.	4.2	Sec. 4.2		you already have ports and interfaces. What is a communication channel? This term is not used anywhere else in the standard. What are you trying to say here, and can it be said without introducing another term, which is not even defined in the glossary. And what is a "given" channel?	Tom Casar	Text removed from the FIPS 140-2 Draft 2
527	T.C.	4.2			Note that the "Documentation shall" sentences are gone from Sections 4.1 and 4.2, but are present in other sections. Is the intent to put all of them into the DTR?	Tom Casar	**Accepted:** Text will be modify to have these sentences in the main body and a summary of all in the annex.
586	W.C.	4.2	Sec. 2.2		Consider defining CMVP.	Wan-Teh Chang	**Rejected –** term(s) not used in document

659	W.C.	4.2			consider changing "to allow visual verification to improve accuracy" to "to allow visual verification of accuracy".	Wan-Teh Chang	Text removed from the FIPS 140-2 Draft 2
748	EW	4.2	Sec. 2.2		In 2.2 Acronyms - "CSE and CMVP" are not specified .	EWA	**Rejected –** term(s) not used in document
755	EW	4.2	Sec. 4.2		A cryptographic module shall restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module. The cryptographic module interfaces shall be logically distinct from each other although they may share one physical port (e.g., input data may enter and output data may exit via the same port) or may be distributed over one or more physical ports (e.g., input data may enter via both a serial and a parallel port). Why mention Allowed security functions? As defined in section 4.1, Cryptographic Module Specification, Allowed functions provide “no security relevant functionality”. The inclusion of MD5 as an Allowed function would result in the security strength of the module being undefined.	EWA	**Rejected:** The reviewer misinterpreted the standard.
756	EW	4.2	Sec. 4.2		A cryptographic module may utilize multiple independent communication channels. The data output, for a given communication channel, shall be disabled while performing key generation, manual key entry, self-tests, software loading and zeroization. Do not agree that data output needs to be disabled while performing key generation, manual key entry and zeroization. Also, “communication channel” should be defined in the Glossary of Terms.	EWA	Text removed from the FIPS 140-2 Draft 2
757	EW	4.2	Sec. 4.2		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. How can status output be implicit? Status output, by definition, is output.	EWA	**Accepted:** More information can be found in the DTR. Some modules can, implicitly, indicate an error state (e.g. smartcards will not reply if an error occurs , and if no reply is received in x time, it is assumed an error occurred.

760	EW	4.2	Sec. 4.2		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. Good requirement!!!	EWA	**No action required**
761	EW	4.2	Sec. 4.2		The module shall utilize a separate, dedicated physical port for the input or output of CSP's, or a Trusted Channel shall be utilized to protect the CSPs entering and leaving the cryptographic module. If a Trusted Channel is used, the documentation shall specify the security strength of the Trusted Channel. How can you specify the security strength of a directly attached communication pathway as described in the definition of Trusted Channel in the Glossary of Terms?	EWA	Text removed from the FIPS 140-2 Draft 2
775	IG	4.2	Sec. 4.2		"A cryptographic module may utilize multiple independent communication channels. The data output, for a given communication channel, shall be disabled while performing key generation, manual key entry, self-tests, software loading and zeroization." The relationship between a specific channel, and each of the operations listed above needs to be characterized/specified for this requirement to be clear. Otherwise, the sentence is ambiguous and leads to questions such as: -What is the scope of channels that must have their output disabled for a given operation (e.g. key generation)? -The sentence implies that the there is some relationship between key generation (and other operations) and one specific channel, but not another. Does this mean, key generation for keys related to that channel? If so, what is a related key? -Some operations listed would seem to apply to all channels, whereas some could be interpreted as applying to specific channels - how should this be interpreted?	Inforgard Vendor	Text removed from the FIPS 140

797	IG	4.2	Sec. 4.2		"A cryptographic module may utilize multiple independent communication channels. "Note: Further explanation of what constitutes a 'communication channel' is in order. A network router, for example, might consider each Security Association (VPN) as a 'separate channel;' additionally, sockets and other logical 'channel' mechanisms. I would assume constitute channels. Perhaps this should be dealt with more in the glossary.	Inforgard	Text removed from the FIPS 140
798	IG	4.2	Sec. 4.2		Each reference to CSP, SSP, etc. needs to be clarified as to whether the requirement is for 'plaintext,' 'protected' or 'cryptographically protected' values.	Inforgard	Text removed from the FIPS 140-2 Draft 2
799	IG	4.2	Sec. 4.2		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. Note: This needs to clarify whether the requirement applies to plaintext, protected or 'cryptographically protected' values (and types….CSPs vs. SSPs, etc.)	Inforgard	Text removed from the FIPS 140-2 Draft 2
890	AT	4.2	Sec. 4.1.2		•Section 4.1.2 – Cryptographic Boundary oThe first sentence is very restrictive and does not fit well for validation of software modules. Recommend adding a separate definition for a software module such as "A software cryptographic boundary shall consist of an explicitly defined set of binary executables that are executed on a defined Operational Environment (e.g. – OS)."	Atlan	**Accepted:** Changed in FIPS 140-2 Draft 2
907	CL	4.2	Sec. 4.2 last para before Security level 1&2		"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." Is each independent internal action required to be triggered by an independent operator action? (Also applicable to the description in Section 4.3.3, bullet point 2).	CEAL	Text removed from the FIPS 140-2 Draft 2

908	CL	4.2	Sec. 4.2		“A cryptographic module may utilize multiple independent communication channels. The data output, for a given communication channel, shall be disabled while performing key generation, manual key entry, self-tests, software loading and zeroization.” Shouldn’t this requirement be rewritten to make it clear that any and all channels that might be affected by the key generation, etc, shall have their data output disabled? If an RSA key is being generated that will be later used in conjunction with one of the data channels, is the data channel required to be disabled during the entire (potentially lengthy) RSA key generation process?	CEAL	Text removed from the FIPS 140-2 Draft 2
930	CL	4.2	Sec. 4.2		“If a Trusted Channel is used, the documentation shall specify the security strength of the Trusted Channel.” How should the security strength be specified for a Trusted Channel implemented as “A communication pathway between the cryptographic module and endpoint that is entirely local, directly attached to the cryptographic module and has no intervening systems.”	CEAL	Text removed from the FIPS 140-2 Draft 2
1048	R.E.	4.2	4.2		A cryptographic module may utilize multiple independent communication channels. The data output, for a given communication channel, shall be disabled while performing key generation, manual key entry, self-tests, software loading and zeroization.	Randy Easter - NIST	Text removed from the FIPS 140-2 Draft 2
1125	D.W.	4.2	Sec. 4.2		In addition to disabling output during the conditions stated, suggest including a general condition prohibiting output of data by a process during any operation it performs on keys (and/or other CSPs) – to include internal transfers and updates – unless, e.g., output of those CSPs is intended.	Debbie Wallner-NSA	Text removed from the FIPS 140-2 Draft 2
1126	D.W.	4.2	Sec. 4.2		•Disagree with the following statement (on page 18); “During manual SSP entry, the entered values may be temporarily displayed to allow visual verification to improve accuracy.” Perhaps the intent was for Public Security Parameters (PSPs) to be displayed (but not Sensitive Security Parameters). Rationale: According to Section 2.1, Glossary of Terms, Sensitive Security Parameters (SSPs) includes	Debbie Wallner-NSA	Text removed from the FIPS 140-2 Draft 2

					Critical Security Parameters (CSPs), which are further defined as private cryptographic keys and authentication data such as passwords and PINs. Shoulder surfing is a concern and should be adequately protected against. Suggest that consideration be given to rewording the requirement such that during manual entry of SSP information the values being entered shall not be displayed. This is a common security protection feature that has been employed in many commercial systems.		
658	W.C.	4.2	Sec. 4.2		What's the significance of "independent" in "A cryptographic module may utilize multiple independent communication channels"? Does this mean if the data output for one communication channel is disabled (while performing key generation, etc.), the data output for the other communication channels can remain enabled?	Wan-Teh Chang	Text removed from the FIPS 140-2 Draft 2

tID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
3	IG	4.3	4.3.2	GE	Comments regarding password dictionary attacks --- This is quoted from section 4.3.2 (operator authentication) "If passwords are utilized as an authentication mechanism, then restrictions shall be enforced by the module on password selection to prevent the use of weak passwords that are more susceptible to attacks (e.g., dictionary attacks)." This is a vague requirement (unless it is intended this way and will be clarified in IG docs). What restrictions shall be enforced? This is very dependent on the dictionary, etc.	Inforgard Vendor	**Accepted:** Please have the author of this requirement provide an explanation how a module (hardware/software/firmware) can meet this requirement? If not, then suggest removal.
54	H.F.	4.3	Section 4 - Table 1		The “Roles, Services and Authentication” is set to “Role-based or identity-based authentication” for Security Level 2. However, Section 1.2 (security level 2) states “Level 2 requires role-based authentication in which a crypto module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services”. Is identity-based authentication allowed in Security Level 2?	Hildy Ferraiolo	**Accepted:** If the module only meets role based authentication, then it meets the Level 2 requirement. If it requires operator identity based authentication, then it meets the Level 3 requirement. Appears Table 1 needs correction.
57	H.F.	4.3	Section 4.3.2		For security levels 2 – 5 a cryptographic module shall support at least one of the following mechanisms to control access to a module.” The mechanisms are: Role-Based and Identity Based Authentication.” The statement implies that the module-designer can choose between the two methods, which is not the case. Please clarify.	Hildy Ferraiolo	**Not Accepted:** The module designer engineers the module to meet any particular assurance level.
58	H.F.	4.3	Section 4.3.2		For security level 2, role-based authentication is required. Table 1, however also lists identity based authentication. If higher level authentication (level 3) is allowed to be used in lower levels, then a statement needs to imply this. This is important for PIV.	Hildy Ferraiolo	**See comment 54.**
59	H.F.	4.3	Section 4.3.3		(services): states: “A cryptographic module may provide other services, both Approved and non-Approved” clarify non-Approved. Is it from the list in Appendix B or both appendix B and Appendix B excluded).	Hildy Ferraiolo	**Not Accepted:** Non-Approved is defined in Section 4.1.

60	H.F.	4.3	Section 4.3.3		(Services) Can a Bypass function be used to invoke a Allowed or Non-Approved cryptographic functions?	Hildy Ferraiolo	**Accepted:** Revisit text definition of bypass.
62	H.F.	4.3	4.3.2		Could an overall Security level 2 smart card-based cryptographic module use a self-defined identity based authentication for the optional User Role? The identity-base authentication; however would not comply with level 3 identity authentication, because it is out-side the scope of level 2 requirements. Under these conditions, can the user (role) invoke Approved security functions? - When only one authentication method is chosen for authentication (say biometric match), then the 10^8 FAR seems excessive and might negatively affect the FRR. - Device authentication can occur without user-action. For example, a smart card authenticates a reader. With FIPS 140-3 (level 2), all cryptographic function seem to be accessible only after the operator has authenticated to the cryptographic module. Could FIPS 140-3 include exceptions for non-authenticated cryptographic function such as Device authentication.?	Hildy Ferraiolo	**Accepted:** At Level 3, all operators of Approved services shall be identity based authentication. At Level 2, a role may be defined to a single operator which in a sense would be identity based. The authentication strength requirement will be removed. Instead only Approved authentication methods all allowed as specified in an Annex. If Approved methods can not be identified in the Annex, then one would be re-directed to guidance that will specify requirements, including strength. An operator need not be a human, but can be a device.
80	J.C.	4.3	Sec. 4.3.2		This paragraph states “When a cryptographic module is powered off and subsequently powered on, the results of previous authentications shall not be retained”. Table 1 row 5 state that audit mechanisms shall be used for Security Level 2 and above and Security Level 3 and above requires protection of audit data. One item typically captured in audit logs is the success or failure of login/authentication attempts. Does this requirement mean to remove authentication status from any audit log. Recommendation: Change “When a cryptographic module is powered off and subsequently powered on, the results of previous authentications shall not be retained and the module shall require the operator to be re-authenticated” to “When a cryptographic module is powered off and subsequently powered on, the module shall require the operator to be authenticated”.	James Cottrell- MITRE	**Accepted:** Status need not be removed from the log. However an operator will need to re-authenticate to a module after a power off event.

81	J.C.	4.3	Sec. 4.3.3		For the “Show Status” requirement, what level of status information is required to meet this requirement? If the module reported “Powered On” as its status, would this be sufficient to meet this requirement? Or is the module’s providing status on its ability to provide at least one approved mode of operation the intended “status” of this requirement?	James Cottrell- MITRE	**Accepted:** Depending on the status services a module implements, this interface shall be used to output such information. Certain status states are required in the standard.
82	J.C.	4.3	Sec. 4.3.3		For the “Show the Module’s Version Number” should this requirement include showing the software version number in addition to its hardware version number? Or should a separate “Show Module Software Version Number(s)” requirement be added. A module could have multiple versions of software installed. Since multiple software versions can be loaded, should an additional “Show Operational Software Version Number(s)” requirement be added? This would report the software version of all executable software modules within the cryptographic module.	James Cottrell- MITRE	**Accepted:** The versioning information found on a validation certificate shall be provided.
104	C.P.	4.3	Sec. 4.3.3 Services (page 22)		“Defining a limited or non-modifiable operational environment…” In the last paragraph there is a reference to limited operational environment, but in Section 4.5 we do not have anymore the concept of limited operational environment. In this version of the standard we use only non-modifiable and modifiable operational environment.	Claudia Popa - CSE	**Accepted:** To be corrected.
151	J.R.	4.3	4.3.3		Show the Module’s Version Number: Output the name and the version number of the cryptographic module. Comments: (Insert) The name and version number shall match the name and version number on the cryptographic module certificate.	James Randall RSA	**Accepted:** See comment #82
152	J.R.	4.3	4.3.3		The module shall support an Approved authentication technique to verify the validity of software that may be loaded. Defining a limited or non-modifiable operational environment by means of procedurally-enforced security rules prohibiting the use of the external software loading capability shall not be permitted. Comments: (Notes) It would be better to state that the	James Randall RSA	**Accepted:**

					authentication technique shall be enforced by the module's implementation - rather than stating shall not be handled by procedural controls.		
158	J.R.	4.3	4.3.2		If the module employs default authentication data to control access to the module for first-time authentication, then the default authentication data shall be unique per module unit delivered. Comments: (Notes) And shall not be displayed directly on the module's physical packaging. The intent here seems to be no "default password" - the logical alternative of using a module serial number etc displayed on the case of a module should also be precluded.	James Randall RSA	**Accepted:** To be clarified
163	J.R.	4.3	4.3.3		A cryptographic module shall provide the following services to operators: Show Status: Output the current status of the cryptographic module. This may include the output of status indicators in response to a service request. Comments: (Note) For software modules, the module shall also provide a service to display the digest of the modules software. There should be a mechanism for the end user of a module to verify that the code running in a module matches the code which was validated by a testing laboratory. Testing laboratories should provide the digest (or some MAC) of the modules software or firmware and these should be attached to the modules certificate and that information should be able to be compared against the output from this module service. There is no mechanism currently for end users to verify that the vendor has provided the same software implementation that was validated.	James Randall RSA	**Accepted:** text will be revisited

168	J.R.	4.3	4.3.2		In addition to the requirements of Security Level 3, Security Levels 4 and 5 shall also meet the following requirement. Comments: (Notes)This is instead of the requirements of the previous levels - i.e. two factor identity based is the requirement. Or reword to make it clear that the authentication mechanism requires two-factor approaches.	James Randall RSA	**Accepted:**
170	J.R.	4.3	4.3.2		Authentication strength requirements shall be met by the module's implementation and shall not rely on documented procedural controls or security rules (e.g., password size restrictions). Comments: It would be better to state that the authentication strength requirements shall be enforced by the module's implementation - rather than stating shall not be handled by procedural controls. i.e. follow the wording/style in the next section.	James Randall RSA	**Accepted:**
171	J.R.	4.3	4.3.2		The initialization of authentication mechanisms may warrant special treatment. If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorized methods (e.g., procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialize the authentication mechanisms. If default authentication data is used to control access to the module, then default authentication data shall be replaced upon first-time authentication. This default authentication data does not need to meet the zeroization requirements (see Section 4.8.) Comments: (Note) This implies some form of "factory reset" is possible which would re-use the authentication data - again covering this as per CSP handling fits the requirements.	James Randall RSA	**Accepted:**

172	J.R.	4.3	4.3.2		Various types of authentication data may be required by a cryptographic module to implement the supported authentication mechanisms, including (but not limited to) the knowledge or possession of a password, PIN, cryptographic key, or equivalent; possession of a physical key, token, or equivalent; or verification of personal characteristics (e.g., biometrics). Authentication data within a cryptographic module shall be protected against unauthorized disclosure, modification, and substitution. Comments: It would make sense for this data to be treated in the same manner as other CSPs and hence be covered by the same requirements rather than having a separate set of requirements for "authentication data" compared to other security critical information in the module.	James Randall RSA	**Accepted:**
173	J.R.	4.3	4.3.2		Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. For Security Levels 2-5, a cryptographic module shall support at least one of the following mechanisms to control access to the module: Role-Based Authentication: If role-based authentication mechanisms are supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator and shall authenticate the assumption of the selected role (or set of roles). The cryptographic module is not required to authenticate the individual identity of the operator. The selection of roles and the authentication of the assumption of selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module shall authenticate the assumption of any role that was not previously authenticated. Comments: for that operator. (or for the specified operator)	James Randall RSA	**Accepted:**

175	J.R.	4.3	Sec. 1.3 para 3 Security level 3		Security Level 3 requires mechanisms to protect CSPs against timing analysis attacks. If a module may operate in both an Approved and non-Approved mode, Security Level 3 requires an indication when the module is in the Approved mode. Security Level 3 allows the software components of a cryptographic module to be executed on a general purpose computing system using an operating system that Comment: This requirement should be across all security levels of modules - 140-2 required that the operator be able to determine the mode for all levels (section 4.1). It seems out of place to have this noted in this section - it should be left until later.	James Randall RSA	**Accepted:**
186	J.B.	4.3	Sec. 4.3.2		The use of two-factor authentication schemes to provide increased security with respect to authentication of entities is now widely recognised in industry and as such it is natural, that FIPS 140 should wish to address this issue. The security requirements as currently expressed in sec. 4.3.2 Operator Authentication for security levels 4 and 5 raises a number of issues with respect to how two factor authentication can be recognised and used within the current security requirements. Firstly, the explicit requirement for two factor authentication at security levels 4 and 5 limits the use of two factor authentication mechanisms as part of a complete system deployment that are not solely enforced within the module's crypto-graphic boundary. This contrasts with the overall requirement for strength of authentication mechanism that must be met. So for example this requirement currently prohibits the use of a single-sign on mechanism or a centralised management system, which use two-factor authentication, but will not fall within the crypto boundary. In the case where this type of authentication mechanism is mandated by the end user, the module is effectively limited to being validated to at most level 3 unless this external authentication mechanism is included	Jason Bennet--Thales e-Security	**Accepted:** TBD

					within the crypto-boundary. The definition of the crypto-boundary is also difficult to define where a 'local' two factor authentication mechanism is used in which one of the factors is something you have, such as a smart card. In this case does the validation also include the smart card, thereby limiting the possibility of using other smart cards, and if so how can a 'non-fixed' crypto-boundary be defined? Lastly the definition of the crypto boundary is particular problematic for embedded modules where the mechanisms for inputting authentication must be external to the module for accessibility. So for example a finger print reader attached to a PC will, (by definition), be outside what can be termed a fixed crypto-boundary for an embedded module. In conclusion Thales e-Security supports the use of two factor authentication mechanisms but is concerned that the requirement as currently stated will prohibit the validation of certain modules' configurations, as described above, at security levels 4 and 5.		
187	J.B.	4.3			This contrasts with the overall requirement for strength of authentication mechanism that must be met. So for example this requirement currently prohibits the use of a single-sign on mechanism or a centralised management system, which use two-factor authentication, but will not fall within the crypto boundary. In the case where this type of authentication mechanism is mandated by the end user, the module is effectively limited to being validated to at most level 3 unless this external authentication mechanism is included within the crypto-boundary. The definition of the crypto-boundary is also difficult to define where a 'local' two factor authentication mechanism is used in which one of the factors is something you have, such as a smart card. In this case does the validation also include the smart card, thereby limiting the possibility of using other smart cards, and if so how can a 'non-fixed' crypto-boundary be defined? Lastly the definition of the crypto boundary is particular problematic for embedded modules where the mechanisms for inputting	Jason Bennet- -Thales e-Security	**Accepted:** TBD

					authentication must be external to the module for accessibility. So for example a finger print reader attached to a PC will, (by definition), be outside what can be termed a fixed crypto-boundary for an embedded module. In conclusion Thales e-Security supports the use of two factor authentication mechanisms but is concerned that the requirement as currently stated will prohibit the validation of certain modules' configurations, as described above, at security levels 4 and 5.		
188	J.B.	4.3	4.3.2		Operator Authentication specifies that weak passwords shall be enforced by the module and that procedural controls or security rules cannot be relied upon, but no specification or guidance is given as to what properties strong or weak passwords should exhibit. It is felt that additional guidance should be made available to enable proper comment on this security requirement and allow vendors to determine the impact, if any, on current algorithms that they use to determine the 'strength' of passwords used by a module.	Jason Bennet-Thales e-Security	**Accepted:** See comment #3
196	J.F.	4.3	Sec. 4.3.2		The comments I have are in section 4.3.2 Operator Authentication and section 4.9.1 Pre-Operational Tests: In 4.3.2: "The authentication mechanism may be a group of mechanisms of different authentication properties that jointly meet the strength of authentication requirements of this section. The strength of the authentication mechanism shall conform to the following specifications: For each attempt to use the authentication mechanism, the probability shall be equal or less than one in 100,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods). For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 1,000,000 that a random	Jim Fox - NIST	**Accepted:** See comment #62

					attempt will succeed or a false acceptance will occur." In one case the probability is "equal or less than" and in the other the probability is "less than". Should this be consistent?		
231-1	J.H.	4.3	Sec. 4.3.2		1. Decreasing the probabilities of guessing authentication data by a factor of 100 seems extreme. Comments: Can you share with us the rationale for this change?	Johnn Hsiung - for - SafeNety	**Accepted:** See comment #62
231-2	J.H.	4.3	Sec. 4.3.2		2. Requiring default authentication data to be unique per module unit delivered might be reasonable in the case of a module used at the system level where an individual customer would normally order only a few modules typically order at most and a few tens of a module would represent a larger order. However, for a personal use device such as a smart card (PIV) or USB token, customers typically order thousands of the devices, with a large order being tens of thousands. In this case, requiring a separate default password for each device is simply not feasible. It is recommended that wording be added to the effect of: "In the case of modules that are typically delivered to customers in high volumes, this requirement may be met by providing initial default authentication data that is unique to an individual batch delivered to a single customer."	Johnn Hsiung - for - SafeNety	**Accepted:** See comment #62
245	J.K.	4.3	4.3		"3. Roles, Services, and Authentication" "Roles, Authentication, and Services" are correct. Rewrite "Roles, Authentication, and Services".	JCMVP44 Junichi Kondo	**Accepted:**

297	J.L.	4.3	4.3.1		The first para refers to a Crypto officer role. Are there any requirements on the qualifications of this individual (per security level) to perform this function. Needed for clarity and completeness. "4.3.1 Roles A cryptographic module shall support a Cryptographic Officer Role. The Cryptographic Officer Role shall be assumed to perform cryptographic initialization or management functions and general security services (e.g., module initialization, management of cryptographic keys, CSPs, and audit functions)."	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Not Accepted:** Any other unique qualifications would be out-of-scope.
299	J.L.	4.3	4.3.2		Fourth bullet - on passwords; you should add a reference on what constitutes a good password; for example, NIST SPEC Pub 800-12 (Chap 16), CSC-STD-002-85. Required to enhance security.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted:** See comment #3
326	AN	4.3			"Show the Module's Version Number: Output the name and the version number of the cryptographic module." Comment: Suggest adding the requirement that validation certificate numbers, algorithm certificate numbers, etc. be included in this type of required status service.	Anonymous	**Accepted:** See comment #82
359	J.K.	4.3	4.3		Roles, Services, and Authentication The contents in FIPS 140-2 IG 14.1 are not reflected.	JCMVP46 Junichi Kondo	**Accepted:**
360	J.K.	4.3	Sec. 4.3		Typo "Tables of Roles, with corresponding services commands with input and output" Rewrite "services commands" as "service commands"	JCMVP45 Junichi Kondo	**Accepted:**
387	J.K.	4.3	4.3.3		In FIPS 140-3, "a limited operational environment" is not defined. The following words should be deleted : "limited or".	JCMVP15 Junichi Kondo	**Accepted:**

388	J.K.	4.3	4.3.2		The “can” in the following sentence should be replaced with “may” : “the operating system can implement the authentication mechanism.” Rewrite as follows : “the operating system may implement the authentication mechanism.”	JCMVP14 Junichi Kondo	**Accepted:**
389	J.K.	4.3	4.3.1		In section 4.3.1 a Maintenance role is missing while a Maintenance role is referred in section 4.6.1. Define a Maintenance role in section 4.3.1 or delete the requirements in section 4.6.1.	JCMVP13 Junichi Kondo	**Accepted:**
390	J.K.	4.3			“An operator is not required to assume an authorized role to perform services where CSPs are not used, modified, disclosed, or substituted and PSPs are not used, modified or substituted (e.g., show status or other services that do not affect the security of the module).” This requirement is originally referred from FIPS 140-2 IG 3.1, but the exceptions in IG are not included.	JCMVP12 Junichi Kondo	**Accepted:**
391	J.K.	4.3	4.3.1		The following sentence is difficult to understand : “Authorized roles are applicable to all services utilizing Approved security functions or where the security of the module is affected.” The relative pronoun “where” is not clear to which noun is adorned.	JCMVP11 J unichi Kondo	**Accepted:**
407	D.W.	4.3	Sec 4.3.2		For security levels 4 and 5 under section 4.3.2 there is a statement that two-factor identity-based authentication is required. It might be beneficial to add a short statement about which factors are considered acceptable, elaborating on the possibilities listed in the paragraph on the top of page 20. In particular, it should be made clear that it is expected/required that the two factors will be chosen from different categories of authentication data (something you know, something you hold, and/or something you are). See, for example, the requirement below, which has a similar objective:	Debbie Wallner-NSA	**Accepted:**

408	D.W.	4.3			User's claimed identity should be verified using more than one of the three types of authenticators - passwords, tokens, or biometrics. The selection of the authentication techniques and the security strength of each technique must be designed to support the overall security requirements.	Debby Waller- NSA	**Accepted:**
456	J.L.	4.3	Sec. 4.3.1		The first para refers to a Crypto officer role. Are there any requirements on the qualifications of this individual (per security level) to perform this function. Needed for clarity and completeness.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Not Accepted:** See comment #297
459	J.L.	4.3	Sec. 4.3.3		Bypass capability - change the phrase 'but instead' to 'or.' Reads better	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted:**
505	T.V.	4.3			We propose to mandate for Security Levels 4 and 5, mirroring Level 3, optionally allowing 2FA for environments where source verification is feasible. On-chip integrated modules The current standard draft can not easily describe modules integrated below the single-chip level.	Tamas Visegrady - IBM	**Accepted:**
526	T.C.	4.3	Sec. 4.3.1		is a role required to use a public key, such as verify a signature?	Tom Casar	**Accepted:**
528	T.C.	4.3	Sec 4.3.2		Don't need a shall statement at the beginning because you have them further below.	Tom Casar	**Accepted:**
537	T.I.	4.3	Sec. 4.3.1 Roles		The description of Maintenance role which clearly stated in 140-2 is deleted. It seems that the description is included in the Other roles column; however in the 4.6.1, there clearly described about Maintenance role to be used for maintenance service/access: it should not be deleted.	Toru Ito - Cryptrec & INSTAC	**Accepted:**
538	T.I.	4.3	Sec. 4.3.2 Operator Authentication		In relation to the "password selection to prevent the use of weak passwords that are more susceptible to attacks": It should specifically present the requirements to be fulfilled by the passwords.	Toru Ito - Cryptrec & INSTAC	**Accepted:** See comment #3
539	T.I.	4.3	Sec. 4.3.3 Services		n relation to the description of "The logic performing the external software loading shall be logically disconnected from all data output.", it is hard to comprehend its major points. The scope of "loading logic" to be indicated should be clearly defined.	Toru Ito - Cryptrec & INSTAC	**Accepted:** To be clarified

550	B.W.	4.3	Sec 4.3.2		The first bullet indicates that the chance of a false acceptance for authentication should be no greater than 10-8. The second bullet indicates that when multiple attempts are made, the chance that a single attempt succeeds should be no greater than 10-7. If this is the case, and an attacker makes 10 attempts/min, the chance of success after 1 min will be 10*10-7=10-6, much greater than the success rate for single attempts given in the first bullet.	Bridgete Walsh - CSE	**Accepted:** See comment #62
569	J.C.	4.3	Sec. 4.3		SECURITY LEVELS 1 AND 2 For Security Levels 1 and 2, 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. Comments: Where did the requirements for the input and output of plaintext CSPs go?	Jean Campbell - CSE	**Accepted:**
570	J.C.	4.3	Sec. 4.3.2		If the module employs default authentication data to control access to the module for first-time authentication, then the default authentication data shall be unique per module unit delivered. Comments: Shouldn't this requirement be at a higher security level?	Jean Campbell - CSE	**Accepted:**
584	W.C.	4.3	Sec. 1.3		1.3. Security Level 3 Page 2, 1st paragraph of the section: Consider changing "attempts that provide direct physical access" to "attempts at direct physical access". Consider changing "use of or modification of" to "use or modification of".	Wan-Teh Chang	**Accepted:**
587	B.M.	4.3			First bullet. The Draft FIPS 140-2 requirement calls for a numerical PIN of at least 8 digits. For purposes of authentication to a smart card like the PIV Card, it might be appropriate to require an 8 digit PIN capability, but it is misleading to require a FAR of 1 in 10^8. In the real world, FAR rates are dominated by factors beyond the control of the PIV Card (e.g., theft, or inadvertent or intentional disclosure of PINs by the subject). Also, an 8 digit PIN would only meet this requirement if it had maximal entropy; in the real world, people will choose 4 digit PINS (by analogy with bank cards) unless they are prevented from doing so; and people will choose low-entropy PINs (like	Bill MacGregor NIST	**Accepted:** See comment #62

					9112001) unless they are prevented from doing so. It would make more sense to phrase this requirement in terms of a shared-secret authentication transaction between the module and an external system (which will typically not be the subject, directly). If this were done, it would make sense to retain the requirement for 1 in 10^8 FAR capability. Also, Draft FIPS 140-3 should acknowledge the importance of the FAR/FRR engineering tradeoff to usability, and specify reasonable bounds on both. Ideally, this should be based on human factors studies with password systems.		
588	B.M.	4.3			first bullet. The requirement for a FAR of 1 in 10^8 is orders of magnitude beyond the best achievable FARs of single sample biometric techniques. This requirement effectively rules out single sample biometrics. Even two sample biometrics (with different fingers, for example) are not likely to meet this requirement. In the case of the PIV Card, this requirement is excessive in the extreme, and could effectively prevent the use of well-known biometric techniques with FARs in the range of 1 in 10^2 to 1 in 10^4. FYI, the current authentication accuracy requirement for the PIV biometric is approximately 1 in 10^2 for FAR and FRR simultaneously, as documented in SP800-76-1. PIV Card users could use biometric Match-On-Card authentication with accuracy exceeding the requirements of SP800-76-1. Should Draft FIPS 140-3 prevent this?	Bill MacGregor NIST	**Accepted:** See comment #62
589	B.M.	4.3			fourth bullet. It is appropriate to state a requirement for password (or PIN?) structure. However, dictionary tests, the only example given, are impractical on smart cards today. A specific recommendation should be given, explicitly or by reference, for PIN and password policy.	Bill MacGregor NIST	**Accepted:** See comment #3
593	C.B.	4.3	Sec. 1.3		sentence: “Security Level 3 requires the entry or output of plaintext CSP’s…. .	Chris Brych - DOMUS	**Accepted:**

600	C.R.	4.3	Section 4.3.2		Please provide an example of password restriction logic in the standard. The inclusion of a dictionary file is not practical on resource constrained embedded systems with limited storage space. The effect of this requirement is that embedded systems may not be able to conform with FIPS 140-3. While this requirement may make sense for software modules that exist on an operating system platform, embedded systems do not have the space to store a large dictionary file.	Chris Romeo - Cisco	**Accepted:** See comment #3
601	C.R.	4.3	Section 4.3.2		In the case of a simple password system, the probability of guessing a password in a simple attempt is primarily a function of the strength of the password. Other requirements in this bullet list appropriately address the issue of weak passwords. Please consider removing the phrase "e.g., guessing a password" from this bullet.	Chris Romeo - Cisco	**Accepted:** See comment #3
662	W.C.	4.3	Sec. 4.3.2		Change "either be implicitly or explicitly" to "be either implicitly or explicitly". Make the same change in the next paragraph (Identity-Based Authentication).	Wan-Teh Chang	**Accepted:**
668	W.C.	4.3	Sec. 4.3.3		8th paragraph in this section: Use colon (:) instead of period (.) after "Bypass Capability". Page 21, 11th paragraph/2nd bullet item in this section: Lines 2-4 of this bullet item are not aligned with the first line on the left.	Wan-Teh Chang	**Accepted:**
762	EW	4.3	Sec. 4.3.1		A cryptographic module shall support a Cryptographic Officer Role. The Cryptographic Officer Role shall be assumed to perform cryptographic initialization or management functions and general security services (e.g., module initialization, management of cryptographic keys, CSPs, and audit functions). Criteria for the term “general security services” here, and under the next paragraph for User Role, would appear to be inconsistent. If only the Cryptographic Officer Role is available, then “general security services” would have to include “cryptographic operations and other Approved security functions” as is defined for the User Role.	EWA	**Accepted:**

763	EW	4.3	Sec. 4.3.1		Authorized roles are applicable to all callable services utilizing Approved security functions or where the security of the module is affected. An operator is not required to assume an authorized role to perform services where CSPs are not used, modified, disclosed, or substituted and PSPs are not used, modified or substituted (e.g., show status or other services that do not affect the security of the module). The 1st sentence specifies that authorized roles are applicable to all authorized services using Approved security function, whereas the 2nd sentence seems to allow the use of security hash algorithms being run without assuming an Authorized role. This needs to be clarified.	EWA	**Accepted:**
764	EW	4.3	Sec 4.3.2		For a software cryptographic module, the operating system can implement the authentication mechanism. If the operating system implements the authentication mechanism, then the authentication mechanism shall meet the requirements of this section. How can a module meet the requirements of section 4.8, Sensitive Security Parameter Management, if the authentication mechanism is implemented by the operating system? Authentication data cannot be protected unless it's within a cryptographic module.	EWA	**Accepted:** Authentication shall be implemented by the module and not the OS.
765	EW	4.3	Sec. 4.3.2		The initialization of authentication mechanisms may warrant special treatment. If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorized methods (e.g., procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialize the authentication mechanisms. If default authentication data is used to control access to the module, then default authentication data shall be replaced upon first-time authentication. This default authentication data does not need to meet the zeroization requirements (see Section 4.8.) It needs to be clear here that the module has to enforce this requirement.	EWA	**Accepted:**

766	EW	4.3	Sec. 4.3.2		The authentication mechanism may be a group of mechanisms of different authentication properties that jointly meet the strength of authentication requirements of this section. If the cryptographic module uses cryptographic functions to authenticate the operator, then those cryptographic functions shall be Approved or Allowed cryptographic functions. The combined strength of the authentication mechanism shall conform to the following specifications: From a mathematical perspective, this statement does not appear to consider the effect of one authentication mechanism on another and it's corresponding reduction of probability.	EWA	**Accepted:**
767	EW	4.3	Sec. 4.3.2		If passwords are utilized as an authentication mechanism, then restrictions shall be enforced by the module on password selection to prevent the use of weak passwords that are more susceptible to attacks (e.g., dictionary attacks). If restrictions are placed on the password quality, then is the increased probability warranted?	EWA	**Accepted:** See comment #3
768	EW	4.3			Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism beyond the required authentication strength. This requirement isn't needed as feedback of authentication data is already discussed in the preceding bullet.	EWA	**Accepted:**
769	EW	4.3	SEC. 4.3.2		If the module employs default authentication data to control access to the module for first-time authentication, then the default authentication data shall be unique per module unit delivered. This requirement puts an unnecessary burden on the vendor since there is a requirement to change the authentication data upon first use of the default authentication data.	EWA	**Accepted:**

770	EW	4.3	Sec. 4.3.2		The cryptographic module shall enforce two-factor identity-based authentication. Comment [EWA-C33]: This requirement will prohibit remote access for, as an example, wireless cryptographic modules.	EWA	**Accepted:**
771	EW	4.3	Sec. 4.3.2		The cryptographic module shall enforce two-factor identity-based authentication. This requirement will prohibit remote access for, as an example, wireless cryptographic modules. This requirement will prohibit remote access for, as an example, wireless cryptographic modules.	EWA	**Accepted:**
776	IG	4.3	Sec. 1.3		Section 1.3: Security Level 3 "Security Level 3 requires that the entry or output of CSPs (including the entry or output of CSPs using split knowledge procedures) be performed using ports that are physically separated from other ports, or interfaces that are logically separated using a trusted channel from other interfaces. CSPs may either be entered into or output from the cryptographic module in encrypted form or using a split knowledge procedure." Table 1: "Input and output of critical security parameters either physically separated or logically separated using trusted channel from other ports and interfaces."	Inforgard Vendor	**Accepted:**
782	IG	4.3	Glossary - Sec 4.3.3		Bypass definition in glossary is not the same as that in Section 4.3.3	Inforgard	**Accepted:**
802	IG	4.3	Section 4.3		Recommend changing as follows: A cryptographic module shall support a Cryptographic Officer Role. A Cryptographic Officer Role shall be responsible for performing cryptographic initialization or management functions and general security services (e.g., module initialization, management of cryptographic keys, CSPs, and audit functions). Note: '…shall be assumed' could be misinterpreted as not being a requirement, but rather a statement that "I assume the CO will do this or that…." Also, it should be clarified that both the CO and User are classes of roles and not necessarily	Inforgard	**Accepted:**

					discrete.		
803	IG	4.3	Sec. 4.3.1		This requirement needs to be augmented with the latest IGs dealing with use of a particular RNG or hash function without prior authentication. Also, we may want to clarify here that the unauthenticated use of the Approved security functions is allowed if the call to the Approved function is part of the 'act of authenticating' the operator.	Inforgard	**Accepted:**
804	IG	4.3	Sec. 4.3.2		It should be clarified that the different types of authentication data may be protected differently. If it is a CSP or secret or private key, then the authentication data shall be protected from unauthorized 'disclosure, modification and substitution.' If the authentication data is in the form of a PSP (public key), then the protections must be against 'modification and substitution' only. Note: The other option here would be to define exactly what 'Authentication Data' is in the glossary. For example, is a public key used to verify a digital signature considered authentication data and thus subject to protection against unauthorized disclosure?	Inforgard	**Accepted:**
805	IG	4.3	Sec. 4.3.2		Recommend changing the sentence to read, "The default authentication data is not subject to the zeroization requirements (see Section 4.8.)" • Section 4.3.2: If the module employs default authentication data to control access to the module for first-time authentication, then the default authentication data shall be unique per module unit delivered. Note: This should only be required at Levels 4 and 5. This completely prohibits normal distribution mechanisms for many types of modules, especially software.	Inforgard	**Accepted:**

806	IG	4.3	Sec. 4.3.2		Recommend changing the following bullet as follows: "Authentication strength requirements shall be met by the module's implementation and shall not rely on documented procedural controls or security rules (e.g., password size restrictions) unless such controls or rules are restricted by the design of the module to being performed only during the first-time initialization of the module. Note: The above change would be recommended only for Level 1 and 2 modules, not Levels 3 and up which should have hard-coded minimum strengths which the module must meet.	Inforgard	**Accepted:** See comment #62
807	IG	4.3	Sec. 4.3.2		Recommend changing the following bullet as follows: "Authentication strength requirements shall be met by the module's implementation and shall not rely on documented procedural controls or security rules (e.g., password size restrictions) unless such controls or rules are restricted by the design of the module to being performed only during the first-time initialization of the module. Note: The above change would be recommended only for Level 1 and 2 modules, not Levels 3 and up which should have hard-coded minimum strengths which the module must meet.	Inforgard	**Accepted:** See comment #62
808	IG	4.3	Sec. 4.3.2		If passwords are utilized as an authentication mechanism, then restrictions shall be enforced by the module on password selection to prevent the use of weak passwords that are more susceptible to attacks (e.g., dictionary attacks). Note: Module enforcement of this requirement is not a possibility. For example, how can all types of modules store every dictionary for every language in the world? This is something that is a definite concern, but unfortunately cannot be enforced by all types of modules and must be procedural to some extent.	Inforgard	**Accepted:** See comment #3

809	IG	4.3	Sec. 4.3.2		Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password). Non-significant characters may be displayed in place of the actual authentication data. Note: This would seem to contradict Section 4.2 that states the following: "During manual SSP entry, the entered values may be temporarily displayed to allow visual verification to improve accuracy." Is there an exception when entering SSPs for authentication?	Inforgard	**Accepted:**
810	IG	4.3	4.3.2		Recommend striking the words, "…beyond the required authentication strength."	Inforgard	**Accepted:**
811	IG	4.3	4.3.2		Security Level 2: It states that the module shall employ role-based authentication. This contradicts Table 1 that allows identity-based at Level 2 (p. 15, beginning of Section 4).	Inforgard	**Accepted:**
812	IG	4.3	4.3.2		Should read that 'at least 2 factors' be used…one may want to use more than 'two.'	Inforgard	**Accepted:**
813	IG	4.3	4.3.3		What is a 'non-approved Service' as described in paragraph 7?	Inforgard	**Accepted:**
814	IG	4.3	4.3.3		Should read, "…dedicated to mediating the bypass."	Inforgard	**Accepted:**
815	IG	4.3	4.3.3		Rephrase as follows: "The cryptographic module shall not execute any Approved security functions in the newly loaded executable code until after the Cryptographic Algorithm self-tests specified in Section 4.9.1 have been successfully executed."	Inforgard	**Accepted:**
816	IG	4.3	4.3.3		"The module shall support an Approved authentication technique to verify the validity of software that may be loaded. Defining a limited or non-modifiable operational environment by means of procedurally-enforced security rules prohibiting the use of the external software loading capability shall not be permitted. Note: Recommend removing 'limited operational environment' because this doesn't exist anymore.	Inforgard	**Accepted:**

834	IG	4.3	Sec. 4.3.2		Please further define what a 'weak' password is.	Inforgard	**Accepted:** See comment #3
835	IG	4.3	Sec. 4.3.3		Is this required for pure HW devices?	Inforgard	**Accepted:**
873	IG	4.3	Sec. 4.3.2		Password strength - We consider the requirement on password strength (4.3.2) difficult to enforce in practice. Practical experience shows that static password-enforcement schemes are routinely bypassed by user (administrator) ingenuity. One could include password-security verification as a special "Mitigations of other attacks" scenario, but probably not as a generic requirement applicable to all modules.	Inforgard	**Accepted:** See comment #62
885	AT	4.3			•Under Services, Bypass Capability. This new definition of bypass seems to increase the scope by which the bypass capability is applicable. Traditionally, the bypass service was only applicable to when encryption was turned off. This new definition seems to require that if data is protected with only HMAC (e.g. – no encryption), and then this functionality is disabled, then this is a form of bypass. Is this truly the intent of this statement? This could greatly increase of the impact/scope of this requirement to many other applications such as digital signatures, etc. We recommend keeping it as is and only applicable to turning off the confidentiality service.	Atlan	**Accepted:**
886	AT	4.3	Sec. 4.3.3		"Show the Module's Version Number" service should state "Output the name and the all version numbers of the cryptographic module as identified on the validation certificate." Wording may not be good but we want to clearly identify that all version numbers (HW, SW, etc.) are identified so that operators can easily see if they are using a validated version.	Atlan	**Accepted:** See comment #82
887-1	AT	4.3	Sec. 4.3.2		•This draft seems to only require one role to be defined (Crypto officer). This still seems to relatively arbitrary. Why not simply state that at least one role must be supported? The vendor can define the name of that role and identify their responsibilities and services.	Atlan	**Accepted:**

887-2	AT	4.3	Sec. 4.3.2		•Section 4.3.2 – Operator Authentication "weak passwords" needs to be defined. Modules with limited space/resources will have a tough time, if not impossible, preventing use of weak passwords.	Atlan	**Accepted:** See comment #3
887-3	AT	4.3	Sec. 4.3.2		"If the module employs default authentication data to control access to the module for first-time authentication, then the default authentication data shall be unique per module unit delivered." This is an extremely restrictive requirement for vendors who delivery high volume products. Having unique passwords requires vendors to have backend support to store these default values. This requirement will affect the manufacturing process of vendors greatly.	Atlan	**Accepted:**
889-4	AT	4.3	Specific Comments		•"Critical Security Parameter" should be replaced with "Critical Security Parameter (CSP)" •"Public Security Parameter" should be replaced with "Public Security Parameter (PSP)" •"Sensitive Security Parameter" should be replaced with "Sensitive Security Parameter (SSP)"	Atlan	**Accepted:**
889-5	AT	4.3	Specific Comments		•Generally speaking, some acronyms are properly definition within the Glossary (e.g. – TA, SPA, RBG, etc.) but in the above three examples, and possible others, the acronym isn't defined. Recommend making this consistent (one way or the other).	Atlan	**Accepted:**
889-6	AT	4.3	Specific Comments		•Definition of "Strong" is just too vague. It's not objective when dealing with physical security protection.	Atlan	**Accepted:**
905	CL	4.3	Sec. 4.3.1 para 3		"Authorized roles are applicable to all callable services utilizing Approved security functions or where the security of the module is affected." Is this intended to remove the exception currently listed in the June '07 update of FIPS 140-2 IG 3.1 which allows non-authorized roles access to callable hashing and RNG security functions? If not this should be made clearer.	CEAL	**Accepted:**

906	CL	4.3	Sec. 4.3.1 para 2		Section 4.3.1 – Paragraph 2 Should this mention the optional Maintenance Role, referred to in section 4.6.1.	CEAL	**Accepted:**
916	CL	4.3	Sec. 4.3.2		"If the cryptographic module uses cryptographic functions to authenticate the operator, then those cryptographic functions shall be Approved or Allowed cryptographic functions" What exactly is meant by "uses cryptographic functions"? Do passwords which are hashed by the module prior to comparison count? How about a password that is hashed outside the module and only the hash of the password is sent? (If password hashes are considered to be authentication using cryptographic functions then Windows or most Unix based systems couldn't be used because they use non-Approved hashing functions)	CEAL	**Accepted:**
931	CL	4.3	Sec. 4.3.2		"For a software cryptographic module, the operating system can implement the authentication mechanism" How much of the OS would need to be tested to determine it met the requirements? Would the source code of the authentication mechanism need to be examined? (If so Microsoft Windows and Mac OS would likely be impossible to test) Or is the operation system assumed to meet the requirement, requiring no testing?	CEAL	**Accepted:**
933	CL	4.3	Sec. 4.3.3		"The module shall show its status to indicate whether: the module is providing services without the use of cryptographic functions (the bypass capability is activated), or the module is providing services with the use of a cryptographic function (the bypass capability is not activated)." This is potentially confusing as to what the module should indicate if (out of the services which can use cryptographic functions) it is providing some services using the functions and some without. The first bullet point seems to say that it must show bypass is activated, but the second bullet point seems to say that it must show bypass is not activated. How shall the module show that an alternating bypass is occurring, such as happens in a VPN which has some routes configured for bypass and some	CEAL	**Accepted:**

					configured for encryption. Should the module have an alternating bypass indicator, or should it just cycle the normal bypass indicator on and off as it automatically alternates between bypass and non-bypass traffic?		
934	CL	4.3	Sec. 4.3.1		“If passwords are utilized as an authentication mechanism, then restrictions shall be enforced by the module on password selection to prevent the use of weak passwords that are more susceptible to attacks (e.g., dictionary attacks).”	CEAL	Incomplete comment
949	CL	4.3	Sec. 4.3.3		The definition of bypass used here differs from the definition in the section 2.1 glossary.	CEAL	**Accepted:**
950	CL	4.3	Sec. 1.3 Para 3		Section 1.3 - Paragraph 3 “performed using ports that a physically separated from other ports”. Please add the word “dedicated” between “using” and “ports”. This will make the overview consistent with the requirement in section 4.2 Security level 3, 4, and 5.	CEAL	**Accepted:**
1054	R.E.	4.3	4.3.1		4.3.1 Roles A cryptographic module shall support a Cryptographic Officer Role. The Cryptographic Officer Role shall be assumed to perform cryptographic initialization or management functions and general security services (e.g., module initialization, management of cryptographic keys, CSPs, and audit functions).	Randy Easter - NIST	**Accepted:**
1063	R.E.	4.3	4.3.2		For a software cryptographic module, the operating system can implement the authentication mechanism. If the operating system implements the authentication mechanism, then the authentication mechanism shall meet the requirements of this section.	Randy Easter - NIST	**Accepted:**
1065	R.E.	4.3			• If passwords are utilized as an authentication mechanism, then restrictions shall be enforced by the module on password selection to prevent the use of weak passwords that are more susceptible to attacks (e.g., dictionary attacks). Comments: Clueless on how a module shall meet this requirement. Does the standard define "weak passwords"? If not, then this requirement should be	Randy Easter - NIST	**Accepted:**

					removed.		
1071	R.E.	4.3	4.3.3		Show the Module's Version Number: Output the name and the version number of the cryptographic module. Comments: Why name? Name is arbitrary and subject to marketing changes. Only version P/N information should be required.	Randy Easter - NIST	**Accepted:**
1128	D.W.	4.3	Sec. 4.3.2		Suggest that additional guidance be included to further define the criteria for weak verses strong passwords. Either state what constitutes a strong password (minimum number of characters, requirements for use of upper case, lower case, special symbols, etc.) or provide a pointer to another document where this type of information exists.	Debbie Wallner-NSA	**Accepted:**
1270	F.R.	4.3	Sec. 4.3.2		SECURITY LEVELS 4 AND 5 In addition to the requirements of Security Level 3, Security Levels 4 and 5 shall also meet the following requirement. The cryptographic module shall enforce two-factor identity-based authentication. Pitney Bowes agrees with this requirement for human operators of a cryptographic module. However, there are instances when one cryptographic module, A, requests services from another cryptographic module, B. In these cases cryptographic module A may assume a user (or cryptographic officer) role as an operator of module B. While cryptographic module A could provide two-factor authentication it is more likely that module A would use cryptographic authentication techniques (e.g., a digital signature or message authentication code). The ability of a cryptographic module to engage is a cryptographic challenge response protocol provides stronger authentication than the two factor authentication as required in the current FIPS 104-3 draft. Therefore, Pitney Bowes requests that the requirement be extended to include	F.Ryan Pitney Bowes, Inc	**Accepted:**

					cryptographic authentication techniques: The cryptographic module shall enforce two-factor identity-based authentication or The cryptographic module shall enforce identity-based authentication with security strength greater than or equal to the security strength of the module.		
216	M.W. .	4.3, 4.7			*"As a specialised laboratory, we have limited involvement in formal evaluation schemes and our laboratory does not provide Common Criteria or FIPS evaluations. At the same time, we follow these standards with great interest and support their application. We further participate in security certification schemes of MasterCard (CAST, Mobile Payment Certification) and Visa (Mobile Payment Certification) and we are a member of the JIL Hardware Attacks Subgroup (JHAS) in Europe."* *Our feedback on FIPS 140-3 is centred around the proposed security classification. FIPS 140-3 specifies five security levels for cryptographic modules. We note the following aspects:* "Security Level 3 aims to offer resistance against attacks that require physical access to the module. Level 3 requires protection against timing analysis attacks and it mandates identity-based authentication mechanisms." "Security Level 4 increases security by requiring resistance against **power analysis attacks**. Further, Level 4 requires **two-factor authentication**." "Security level 5 is the highest level and amongst other things, it requires protection from electromagnetic emanation attacks." ***We would like to comment on two-factor authentication and side channel attacks.*** "Many smart card applications on the market do not require two-factor authentication. This would simply that Level 4 goes beyond the level supported by commonly used smart card applications for mobile	Marc Witteman (Amanda van der Berg) - Riscure	**TBD:** FIPS 140-3 addresses only the attacks for which CMVP can develop conformance testing (i.e. SPA, DPA and EME) –Additionally, section 4.11 addresses all the other non-invasive attacks.

					communication, finance and conditional access. At the same time these smart card products are generally perceived and can be considered as highly secure devices that can safely operate in a hostile environment. **We would therefore like to recommend that the requirement for two-factor authentication be revisited. We propose to require this for the highest level only**." "Side channel analysis is a dangerous class of attack for cryptographic devices to which an attacker has physical access. **We therefore support that protection against side channel analysis has been introduced to the security levels of the FIPS 140 scheme**. However, we believe that the current division between Level 3, 4 and 5 is not the optimal representation of the threat that these techniques pose to cryptographic devices."		
129	D.F.	4.3	Sec. 4.3.3		"The cryptographic module shall not execute the loaded code until after the Software Load Test specified in Section 4.9.2 has successfully verified the validity of the externally loaded code." Does the definition of External Software include all DLLs used by our crypto modules that do not contain crypto functionality? If so, does this mean the crypto module must verify the integrity of these DLLs, or can it rely on OS services external to the crypto module for integrity verification? Proposed Disposition: No change necessary.	David Friant Microsoft, Redmond, WA.	**Rejected:** The integrity test only applies to code which is loaded or identified within the defined boundary of the crypto module.
130	DD	4.3	Sec. 4.3.3		Does the definition of External Software include all DLLs used by our crypto modules that do not contain crypto functionality? If so, does this mean the crypto module must verify the integrity of these DLLs, or can it rely on OS services external to the crypto module for integrity verification? Proposed Disposition: No change necessary.	David Friant Microsoft, Redmond, WA.	**Rejected:** RE: comment 129

436	D.F.	4.3	Sec 4 - 4.4.3		Section 4 – Software Security: 4.3.3) Is a UI module required to provide feedback to the operator? How should this be done? Do we need to provide status on everything?	David Friant Microsoft, Redmond, WA.	
963	I.F.	4.3			The module shall enforce restrictions on password selection to prevent the use of weak passwords (e.g. the module shall prevent against dictionary attacks).This needs to be clarified. How should the module enforce this? In particular, what if the password is a PIN? What is considered to be a bad PIN? Excluding PINs from all possible PIN values just reduces the search space for an attacker.	Indra Fitzgerald	**Accepted: text will be revisited**

tID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
1	AN	4.4		GE	"All cryptographic code within the module shall be in executable form." Comment/Question: Does this suggest that a secure cryptographic compiler should not be validated?	Anonymous	**Rejected:** Yes. If the software is in an executable form, then such a compiler would not need to be validated. No change required Bullet and Sub bullet seep to contradict themselves
2	AN	4.4		GE	"The symmetric key shall not be retained within the module when the module is transported to the customer. When the software is loaded into the module, the Cryptographic Officer(s) shall enter the symmetric key or key components (Section 4.8.4) to decrypt the encrypted portions." Comment: Confusing, suggest reword.	Anonymous	**Rejected:** This text is no longer included in the standard since encrypted software for distribution has been removed. No change required.
23	CR	4.4		GE	Summary and Conclusions Cryptography Research welcomes the introduction of requirements for the mitigation of non-invasive attacks in the FIPS 140-3 specification. The addition of these requirements is an appropriate evolution of the specifications and is important for FIPS 140 to keep up-to-date with modem threats that cryptographic modules must address. We believe that defenses to classes of non-invasive attacks should be validated at lower security levels than currently proposed in the FIPS 140-3 draft. These attacks are relatively easy for malicious adversaries to perform, are widely known, and risk potentially devastating consequences if left unaddressed. We also recognize that the introduction of these new requirements into the specification may require some education and training for the testing laboratories. Cryptography Research currently offers such training, as do other technology vendors around the world. We would be pleased to work with NIST and the testing laboratories to help develop any additional training materials appropriate for FIPS 140-3. If you have any questions or would like to discuss any	Cryptography Research Inc.	**Rejected:** Not applicable to Section 4.4. This comment should be moved to Section 4.7. No change required to this Section.

					of the issues addressed in these comments, please contact us. Paul Kocher President & Chief Scientist Benjamin Jun VP of Technology Josh Jaffe Research Scientist		
52	H.F.	4.4	4.2		To prevent the inadvertent output of sensitive information, two independent internal actions shall be required to output CSPs. Comments: Please exemplify independent internal actions	Hildy Ferraiolo	**Rejected:** This comment is not applicable to Section 4.4. Move to Section 4.2. No change required for this section.
63	J.C.	4.4	Sec. 1.4		With the advances in Differential Power Analysis (DPA) demonstrated and documented by Cryptography Research Inc., http://www.cryptography.com/resources/whitepapers/DPA_Attacks.pdf, against AES in Counter Mode recommend that Simple Power Analysis (SPA) and DPA protections be required for cryptographic modules evaluated at Security Level 3 using AES in Counter Mode.	James Cottrell- MITRE	**Rejected:** This comment should be addressed in Section 4.7 comments No change required for this section.
83	J.C.	4.4	Sec. 4.4		In the sixth bulleted item under “Security Level 1”, what checks must be done on complete reloads of module software?	James Cottrell- MITRE	**Rejected:** Pre-Operational Tests. No change required
84	J.C.	4.4	Sec. 4.4		In the bulleted item under “Security Level 2”, it is unclear who “The entity requesting validation” is. Is this entity the developer/integrator of the software for the module? Is the “Software Integrity Test” different than the “Software Load Test, specified in 4.9.2?	James Cottrell- MITRE	**Rejected:** “Entity requesting validation” has been removed, but signature key is still required. The intent is that the vendor would provide this key. Don’t think additional text is now necessary .
86	J.C.	4.4	Sec. 4.4		In the second bulleted item under “Security Level 3”, what is the rationale for zeroization of the hash value computed in the “Software Integrity Test”? If there is no requirement to zeroize the software code on a tamper condition, the tampering party can re-compute	James Cottrell- MITRE	Text has been modified but new text could lead to a denial of service attack.

					the hash of the software upon opening the device. I can understand why the hash value would be zeroized in a Security Level 4, and above, cryptographic module.		
99	C.P.	4.4	Sec. 4.4		Standard: Security Level 1"Any modifications to the module software other than a complete reload shall pass the Software Load Test as specified in Section 4.9.2 "If a specific format for externally provided data is expected, then the module shall verify the format." Security Level 3, page 23 "The MSI command shall return an indication as to whether the Software Integrity Test was successful and a newly computed hash value". "The hash value of the module's software shall be zeroized from the module upon completion of the MSI command which initiate the Software Integrity Test." "The Software Integrity Test, including the symmetric key (as data), shall then be performed as part of the pre-operational tests." Suggestion: Why a complete software reload is considered an exception? Why is this different than the requirement in 4.9.2 "Software Load Test. If software can be externally loaded into a cryptographic module, then …". Do we really need this? Is this not supposed to happen by default? The software has to verify the format of the externally provided data before parsing and using this data. "The MSI command shall return an indication as to whether the Software Integrity Test was successful and the computed hash value". "The hash value of the module's software, calculated and returned by the Software Integrity Test, shall be zeroized from the module upon completion of the MSI command which initiate the Software Integrity Test." Why do we need to mention the "symmetric key"? Is: "The Software Integrity Test shall then be performed as part of the pre-operational tests." not good enough?	Claudia Popa - CSE	**Rejected:** No longer in latest draft

124	D.F.	4.4			Microsoft is very concerned about the new requirements around running self-tests on resume from standby / hibernate and periodical re-test. We do not understand how this will make products more secure. MES: FIPS 140-2 states: “Power-up tests shall be performed by a cryptographic module when the module is powered up (after being powered off, reset, rebooted, etc.).” FIPS 140-3 states: “The pre-operational tests shall be performed by a cryptographic module between the time a cryptographic module is powered on, either from a power-off state or a quiescent state (e.g., low power, suspend or hibernate) and the time that the cryptographic module uses a function or provides a service using the function to be tested.” FIPS 140-3 would require pre-operational test after low power, suspend or hibernate. The more often a test is performed, the sooner it might detect an error, thus improving security. However, the question seems to be whether the efficiency impact of this testing is worth the security benefit. Proposed Disposition: Change the requirement to state “The pre-operational Tests shall be performed by a cryptographic module between the time a cryptographic module is powered on and the time that the cryptographic module uses a function or provides a service using the function to be tested.”	David Friant Microsoft, Redmond, WA.	**Rejected:** May belong in 4.9.1 Need to discuss the hibernate power up testing requirements
126	D.F.	4.4			The consensus at Microsoft is that this requirement is not appropriate for software modules. “The operating system shall prevent operators and external executing processes from reading cryptographic software stored within the cryptographic boundary.”	David Friant Microsoft, Redmond, WA.	**Accepted:**Move to 4.5 However read access to code is no longer prevented.
128	D.F.	4.4			Since we must grant execute but don’t want to grant read and execute is ~” read + run the code”, this requirement is rather strange. By default, we grant users read and execute across almost all of the system. The crypto modules are not secret. What is needed is to prevent tampering?	David Friant Microsoft, Redmond, WA.	Same as above

129	D.F.	4.4	Sec. 4.3.3		“The cryptographic module shall not execute the loaded code until after the Software Load Test specified in Section 4.9.2 has successfully verified the validity of the externally loaded code.” Does the definition of External Software include all DLLs used by our crypto modules that do not contain crypto functionality? If so, does this mean the crypto module must verify the integrity of these DLLs, or can it rely on OS services external to the crypto module for integrity verification? Proposed Disposition: No change necessary.	David Friant Microsoft, Redmond, WA.	**Accepted:** Move to 4.4.3
130	DD	4.4	Sec. 4.3.3		Does the definition of External Software include all DLLs used by our crypto modules that do not contain crypto functionality? If so, does this mean the crypto module must verify the integrity of these DLLs, or can it rely on OS services external to the crypto module for integrity verification? Proposed Disposition: No change necessary.	David Friant Microsoft, Redmond, WA.	**Accepted:** Move to 4.3.3
148-1	J.R.	4.4			5. Operational Environment SL 1: Single user OS or discretionary access control. Comment: This was "Single Operator" in 140-2 which is more appropriate TODO - check later sections for this.	James Randall RSA	**Accepted:** Move to 4.5.1 Table in section 4 needs to be fixed
148-2	J.R.	4.4			8. SSP Management : Zeroization of PSPs. Comment: zeroization is covered in the physical security section - and zeroisation of CSPs is required for security level 3 and 4 and not listed h	James Randall RSA	**Accepted:** Belongs in Key management section 4.8.

148-3	J.R.	4.4			10. Life-Cycle Assurance (CMS) Automated CMS. Comment: What is meant by "automated"? TODO - check later sections for this. 10. Life-Cycle Assurance (CMS) Low-level Testing. Comments: What is meant by "low-level" here? TODO - check later sections for this.	James Randall RSA	**Accepted:** Belongs in section 4.10
153	J.R.	4.4	4.4		SECURITY LEVEL 1 The following requirements shall apply to software contained within a cryptographic module for Security Level 1. • All cryptographic code within the module shall be in executable form. Comments: (Notes) And not in human readable source code. Interpreting java byte codes isn't really executable form for the CPUs on which the interpreter is running - but it is for the "platform" formed by the Java Virtual Machine. The requirement needs to be clear what is meant here for these different situations.	James Randall RSA	**Accepted:** Consider what to require on executable/non-executable code.
154	J.R.	4.4	4.4		The MSI shall not permit the operator of the service to read the software. Comment: (note) What is the intent here? For software based modules the module is by definition readable outside the module so this requirement does not make sense. There are no controls as such which prevent reading. For hardware based modules this seems to indicate that the module should not allow reading out the software and/or firmware directly.	James Randall RSA	**Rejected:** No longer required

155	J.R.	4.4	4.4		The MSI shall not permit the operator to modify module software without invoking the Software Load Test as specified in Section 4.9.2. Comments: (note) Software modules on GPC have access controls outside the MSI - so this seems to not apply. The software load test is for code which is loaded into the module - should this requirement be stated in those terms?	James Randall RSA	**Rejected:** No longer a requirement
157	J.R.	4.4	4.4		• If a specific format for externally provided data is expected, then the module shall verify the format. Comments: (strikeout) If the module is performing a Software Load Test then this additional requirement is redundant in that the module must be approved for loading hence there should be no "format" issues.	James Randall RSA	**Rejected:** No longer required
159	J.R.	4.4	4.4		The Approved integrity technique used in the Software Integrity Test shall consist of the generation of a digital signature using an Approved digital signature algorithm. The entity requesting validation shall generate the private key used to sign the code and the public key used to verify the code. The private signing key shall not reside within the module. The public verification key may reside with the module code. Comments: (Insert)vendor "The entity requesting validation shall (Insert)generate"	James Randall RSA	**Accepted:** See new text
162	J.R.	4.4	1.4		Level 4 modules that contain software must provide for the encryption and authentication of CSPs and integrity test code when the module is not in use. This provides for the strong protection of CSPs from unauthorized disclosure and modification when the module is inactive. Comment: (not in use) What is meant by "not in use" here? TODO - check the later text on this.	James Randall RSA	**Rejected:** No longer in text

165	J.R.	4.4	4.4		The module shall have the capability to decrypt portions of the software that is encrypted when the module is first loaded. All CSPs as well as the Software Integrity Test software (including the public verification key and digital signature) shall be encrypted by the vendor using a symmetric key. The symmetric key, or key components, shall initially be generated by the vendor (Section 4.8.2) and transported to the module site (Sections 4.8.3 and 4.8.4). The symmetric key shall not be retained within the module when the module is transported to the customer. When the software is loaded into the module, the Cryptographic Officer(s) shall enter the symmetric key or key components (Section 4.8.4) to decrypt the encrypted portions. The Software Integrity Test, including the symmetric key (as data), shall then be performed as part of the pre-operational tests. Comments: (notes) What is the intent for "portions" of the software only? What portions should be encrypted and what portions should not be encrypted?	James Randall RSA	**Rejected:** No longer in text
166	J.R.	4.4	4.4		An MSI command (i.e., callable service) permitting a cryptographic officer to initiate the Software Integrity Test without instituting a power-down of the module shall be incorporated. The MSI command shall return an indication as to whether the Software Integrity Test was successful and a newly computed hash value. Comments: (note) As noted earlier - this requirement should apply to all modules at all security levels to enable end-user verification that the software running is the correct (and tested) version.	James Randall RSA	**Rejected:** No longer in text

174	J.R.	4.4	1.4 Security level 4		1.4 Security Level 4 At Security Level 4, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Comment 1: (AT) Missing the "in addition to the requirements of Security Level 3" ... Comment 2: (physical) This wording tends to preclude a software based module - it would be better to see this worded generically and then in the details for each of the areas outline the specific requirements. The later part of the description in this section indicates that software on a GPC can be used and how this interacts with the physical requirements is unclear.	James Randall RSA	**Accepted:** Move to 1.4
189	J.B.	4.4	Sec. 4.4		No introduction is given to the high level aims of sec. 4.4 Software Security and it has been difficult to review the requirements without the context of what the overall security aims are, particularly as this section is new to FIPS 140-3. The requirements stated at security levels 4 and 5 seem to aim to ensure the integrity of the module's software during transit and operation i.e. to provide assurance that the software has not been tampered with. This is obviously vital to the security of the module but the requirements are expressed in terms of a single solution and do not provide for equally valid solutions to this overall goal. An equally valid solution would protect the integrity of the software through the use of physical protection measures, to prevent access to the internal circuitry, and use cryptographic mechanisms to ensure that only authenticated software may be loaded onto the module. It is believed that the requirements should be augmented to allow for use of alternative software integrity protection mechanisms which still achieve the overall aim such as the example given above of using physical protection and external download of	Jason Bennet --Thales e-Security	**Rejected:** No longer in text

					cryptographically signed software. In addition, the overall security aims should be stated as these will give valuable guidance to vendors when complying with the security requirements of FIPS 140-3.		
190	J.B.	4.4	Sec. 4.4		In sec. 4.4 Software Security, a requirement is specified that all cryptographic code within the module shall be in executable form. The exact meaning of this term is not clear, but if taken in its strictest form, the cryptographic code may only exist in machine code (or other native processor forms) and specifically, not compressed, encrypted, Java bytecode or Python etc., all of which must be transformed in some manner before being executed by the processor. This seems to contradict the requirement in sec. 4.4 Software Security for the software integrity test at security levels 4 and 5 to be encrypted. Thales e-Security believes that the requirement as stated should be changed so that cryptographic code may exist in non-executable form only if the transformation code is part of the module and will therefore itself have been validated against the FIPS 140 security requirements. So for example, cryptographic code that is decompressed using code that is implemented in the module should be allowed but cryptographic code that is decompressed using code that did not form part of the validation, say WinZip, should not be allowed.	ThaleJason Bennet- - Thales e-Security	**Accepted:** Review executing code issue.
212	J.R	4.4	4.8.4		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. PSPs may be entered into or output from a module in plaintext form. Comments:(note) Security levels 3 and above require encrypted - so this sentence should be reworked to allow for that.	James Randall RSA	**Accepted:** Move to 4.8.4

226	R.E.	4.4			FIPS 140-3 adds an additional security level and incorporates extended and new security features that reflect recent advances in technology. In FIPS 140-3, each of the eleven requirement areas in redefined. Software requirements are given greater prominence in a new area dedicated to software security, and an area specifying requirements to protect against non-invasive attacks is provided. Where all eleven sections redefined? It appears some of the sections are identical to FIPS 140-2 Rather than given greater prominence, isn't it simply that software modules are further defined with better clarity over FIPS 140-2. Software should not be perceived as a better solution than hardware or mixed solutions. The standard provides mechanisms for assurance to mitigate against access to security parameters. "Protect" appears to be too great a claim.	Randy Easter - NIST	**Accepted:** Does not apply to software section 4.4 This belongs in introductory material
227	R.E.	4.4	Sec. 1.1 & 4.4		Security Level 1 provides the lowest level of assurance. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved security function must be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. Lowest implies something of marginal value. Maybe instead use the term "base line" level of assurance. How does "production-grade" relate to a software module? Is this legacy text from FIPS 140-1 which is hardware centric?	Randy Easter - NIST	**Accepted:** Move to Section 1.1

228	R.E.	4.4	Para 2		Security Level 1 allows the software components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system. Such implementations may be appropriate for security applications where controls, such as physical security, network security, and administrative procedures are provided outside of the module. The implementation of Level 1 cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements. Correct with: software cryptographic Correct with: FIPS 140-3 no longer requires an evaluated OS ... but simply meeting Level 1 requirements. Suggest a change in text. "Suggest starting this as a new paragraph since this is a broad Level 1 statement. " Crossed out : "The implementation of Level 1 cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements."	Randy Easter - NIST	**Accepted:** Looks like 1.1 material
232-1	J.H.	4.4	Sec. 4.4		1. The Level 1 requirements refer to the Software Load Test, as specified in section 4.9.2. The Level 2 and higher requirements refer to the Software Integrity Test without mentioning where it is specified (section 4.9.1). Is this intentional or should the various Levels all refer to the same test?	Johnn Hsiung - for - SafeNety	**Accepted:** Be consistent on referencing

232-2	J.H.	4.4	Sec. 4.4		2. The wording of the Level 2 requirement does not seem to be consistent with the Level 3 requirement or the requirements of section 4.9.1. In particular, the Level 2 requirement calls for a digital signature on the software image to be performed using a key pair generated by the entity requesting the Software Integrity Test. In the Level 3 requirement, the crypto officer is able to initiate the Software Integrity Test as a callable service and the return is specified as a hash value as opposed to a digital signature to be verified by the crypto officer.	Johnn Hsiung - for - SafeNety	**Rejected:** Text has been removed.
232-3	J.H.	4.4	Sec. 4.4		3. Section 4.9.1 defines the Software Integrity Test as a power-up self-test. How does the entity requesting validation specify a key pair to be used for signature and verification before the module is powered on?	Johnn Hsiung - for - SafeNety	**Accepted:** Text has been rewritten
235	J.H.	4.4	Sec. 4.8		This section states: “For a software module, the Software Integrity Test key is a CSP. For a hardware module that contains software components, the Software Integrity Test key is a PSP.” Referring back to section 4.4, how can the key used to perform the test be a SSP at all, for Level 2 and above, when the Level 2 requirement in 4.4 states that the entity requesting the validation generates the key pair used to carry out the test? In other words the key pair is not under the control of the module.	Johnn Hsiung - for - SafeNety	**Accepted:** Clarify whether software integrity test key is just a PSP or SSP
241	J.H.	4.4	Sec. 4.9.1		The “Software Integrity Test” description contains some wording whose meaning is unclear. It says, “The Software Integrity Test is not required for any software excluded from the security requirements of this standard or for any executable code stored in non-reconfigurable memory.” Does this mean, for example, that the firmware loaded into a hardware crypto module would not be subject to the SIT since it is loaded in memory that is reconfigurable only via the approved software load operation? This would make sense since the firmware code would be properly verified using the Software Load Test and then cannot be changed, except by a subsequent software load. However, the wording of section 4.9.2	Johnn Hsiung - for - SafeNety	**Accepted:** Move to 4.9.1

					appears to say that the SIT has to pass after the Software Load test has been completed, which would indicate that consideration for the Software Load Test is not being given with respect to applying the SIT. (See the comment on section 4.9.2 also).		
252	J.K.	4.4	4.4 , 4.9.2, Appendix A		"Approved Integrity technique" is not defined in section 2.1. Define "Approved Integrity technique".	JCMVP3 Junichi Kondo	**Accepted:** Defined by EG in text.
253	J.K.	4.4	4.4		In section 4.4, there is no requirements for the code obfuscation. Remove the following sentence. "How is the code obfuscated?"	JCMVP10	**Rejected:** Yes there is no such requirement. Could not find obfuscated in text
254	J.K.	4.4	4.4		"What are the tamper detection and response capability?" How can software detect tampering? What attacks are considerable against software?	JCMVP49 Junichi Kondo	**Rejected:** Tampering is addressed in hardware section.
261	R.E.	4.4	Sec. 1.4 Security Level 4		Security Level 4 introduces the two-factor authentication requirement for operator authentication. This requires two of the following three attributes: Would 2-factor authentication also allow the agreement of two or more operator passwords? As written, it implies all Level 4 modules shall have as an input a token or biometric.	Randy Easter - NIST	**Accepted:** Move to other section.
262	R.E.	4.4	1.4		"Entire line is highlighted : Level 4 modules that contain software must provide for the encryption and authentication of CSPs and integrity test code when the module is not in use. This provides for the strong protection of CSPs from unauthorized disclosure and modification when the module is inactive." Would 2-factor authentication also allow the agreement of two or more operator passwords? As written, it implies all Level 4 modules shall have as an input a token or biometric.	Randy Easter - NIST	**Accepted:** Move to 1.4

273	R	4.4	1.4		Security levels 1, 2, 3, 4, 5 often are not independent. A higher security level (i.e. level 5) often depends on the lower level (i.e. level 4). Level 5 description states "Level 5 provides the highest level of security in the standard. This level includes all of the appropriate security features of the lower levels, as well as extended features." Security level 3 and security level 4 should also contain the statement "This level includes all of the appropriate security features of the lower levels, as well as extended features". This makes the description of levels 3 and 4 consistent with the description of level 5.	NSA/SETA/ SPARTA Rowland Albert, 410-865-7992	**Accepted:** Move to 1.4
301	J.L.	4.4	4.4		SECURITY LEVEL 4 In addition to the requirements of Security Level 3, the following requirements shall106 apply to software contained within a cryptographic module for Security Level 4. • The module shall107 have the capability to decrypt portions of the software that is encrypted when the module is first loaded. All CSPs as well as the Software Integrity Test software (including the public verification key and digital signature) shall108 be encrypted by the vendor using a symmetric key. The symmetric key, or key components, shall109 initially be generated by the vendor (Section 4.8.2) and transported to the module site (Sections 4.8.3 and 4.8.4). The symmetric key shall not110 be retained within the module when the module is transported to the customer. When the software is loaded into the module, the Cryptographic Officer(s) shall111 enter the symmetric key or key components (Section 4.8.4) to decrypt the encrypted portions. The Software Integrity Test, including the symmetric key (as data), shall112 then be performed as part of the pre-operational tests. **Comments**: Ref to first bullet in security level 4 - refers to use of symmetric key; are there any requirements on this key; suggest adding a ref or standard on key. Needed for clarity, completeness and to ensure security	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Rejected:** No longer in text

302	J.L.	4.4	4.4		**Comments**: 2nd bullet in security level 4 - suggest the term 'may supply' be changed to 'shall'; this wording change would insure that the vendor no longer has the capability to modify the code after transfer to the gov't. Needed for clarity, completeness and to ensure security. • Before the module subsequently transitions to the pre-operational state, the Cryptographic Officer(s) may supply a new symmetric key, or key components (otherwise the current symmetric key shall113 be used). The CSPs, and Software Integrity Test software (including the public verification key and digital signature) shall114 be encrypted and all plaintext copies of these values within the module shall115 be automatically zeroized.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	Removed from text
305	J.B.	4.4	4.4		In sec. 4.4 Software Security, a requirement is specified that all cryptographic code within the module shall be in executable form. The exact meaning of this term is not clear, but if taken in its strictest form, the cryptographic code may only exist in machine code (or other native processor forms) and specifically, not compressed, encrypted, Java bytecode or Python etc., all of which must be transformed in some manner before being executed by the processor. This seems to contradict the requirement in sec. 4.4 Software Security for the software integrity test at security levels 4 and 5 to be encrypted. Thales e-Security believes that the requirement as stated should be changed so that cryptographic code may exist in non-executable form only if the transformation code is part of the module and will therefore itself have been validated against the FIPS 140 security requirements. So for example, cryptographic code that is decompressed using code that is implemented in the module should be allowed but cryptographic code that is decompressed using code that did not form part of the validation, say WinZip, should not be allowed.	Jason Bennet-Thales e-Security	See previous executable resolution.

327	AN	4.4			"Initially, the hash value on the module software may be transmitted to the cryptographic officer independently of the module. The cryptographic officer may manually compare the newly computed hash value to the one provided by the module vendor. If the hash values do not match or the digital signature does not validate, the cryptographic officer should assume that the module software is not valid." Comment: This does suggest adequate security even at Level 1.	Anonymous	**Rejected:** Text has been removed.
357	J.K.	4.4			Please review the requirements from the conformability to multi-thread software module.	JCMVP53 Junichi Kondo	**Rejected:** Commenter needs to point out issues.
386	J.K.	4.4	4.4		If the definition of "hardware module" and "hybrid module" is correct, they include some software inside so that the requirements in this section shall apply to these modules.	JCMVP16 Junichi Kondo	**Accepted:**
420	D.F.	4.4			This requirement will likely require significant re-engineering for software only crypto modules. The draft should provide a set of security threats this requirement was designed to mitigate to help justify the engineering investments.	David Friant Microsoft, Redmond, WA.	**Rejected:** What requirement. Please provide explanation.
421	D.F.	4.4			Windows may suspend or hibernate during a cryptographic operation. It may be very difficult to temporarily stop cryptographic operations to perform self-tests when the computer powers up again. Moreover, this requirement will result all cryptographic process to re-run self-tests at the same time. It will be difficult to justify the performance degradation to a majority of Windows users who do not need FIPS certified crypto.	David Friant Microsoft, Redmond, WA.	**Accepted:** Consider what to do on hibernation. Move to Section 4.9

422	D.F.	4.4			Windows notifies applications when the machine resumes from low power, suspend, or hibernate states by broadcasting the WM_POWERBROADCAST message to all applications with visible windows. The current mechanism is not appropriate for applications such as command line tools or background services that do not have visible windows. Microsoft needs to perform a more thorough study to determine if there is an appropriate mechanism to communicate power events to crypto modules that are loaded into the application's process. Proposed Disposition: The requirement will be changed to eliminate the quiescent, low power, suspend or hibernate states.	David Friant Microsoft, Redmond, WA.	Same as previous.
424	D.F.	4.4			"The vendor shall specify a critical time period that specifies the maximum operational time before pre-operational tests must be repeated." A periodic self-test requirement adds a lot of complexity to crypto modules, especially for those that run in kernel mode. Moreover, running periodic self-tests may have an unpredictable side effect on real-time scenarios such as media playback.	David Friant Microsoft, Redmond, WA.	**Accepted:** Move to 4.9 Text has been removed
428	D.F.	4.4			"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" A continuous test is incompatible with pre-operational testing. If a module chooses this option, when should they consider the pre-operational test complete? Perhaps this should be in a different section. Proposed Disposition: No change is necessary. The continuous comparison of outputs is in lieu of KAT tests.	David Friant Microsoft, Redmond, WA.	**Rejected:** Move to 4.9.1. No change is necessary.

433	D.F.	4.4			The draft refers to annex documents that do not seem to be publicly available. When will they be available for review? We cannot fully understand the set of new requirements without the Annexes. Proposed Disposition: Add annexes in next draft.	David Friant Microsoft, Redmond, WA.	**Accepted:** Move to annexes To be addressed
434	D.F.	4.4			What role does SP800-22 play (if any) in future FIPS certifications? Will it add new self-test requirements to the our general purpose RNG?	David Friant Microsoft, Redmond, WA.	**Rejected:** SP800-22 is NA
436	D.F.	4.4	Sec 4 - 4.4.3		Section 4 – Software Security: 4.3.3) Is a UI module required to provide feedback to the operator? How should this be done? Do we need to provide status on everything?	David Friant Microsoft, Redmond, WA.	**Accepted:** Move to Section 4.3
460	J.L.	4.4	Sec. 4.4		Ref to first bullet in security level 4 - refers to use of symmetric key; are there any requirements on this key; suggest adding a ref or standard on key. Needed for clarity, completeness and to ensure security	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted:** Removed
503	T.V.	4.4			Two-factor authentication We consider two-factor authentication to be indistinguishable from other authentication at the module level. We think this requirement may not be properly enforced by modules.	Tamas Visegrady - IBM	**Accepted:** Removed
504	T.V.	4.4			In our opinion, in the typical restricted environment of HSMs or libraries, two-factor authentication (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 and verify this representation (hash, signature from a token, usw.). The standard already provides 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.	Tamas Visegrady - IBM	**Accepted:** Removed

531	T.C.	4.4	Sec. 4.4		"the input and output interfaces of the cryptographic module shall be directed through a defined API."	Tom Casar	There is no comment
556	J.C.	4.4			The input and output of the module shall be directed through a defined MSI. Comments: Use API instead of MSI. This is an already understood term.	Jean Campbell - CSE	**Rejected:** Currently SMI or HMI is the terminology
571	J.C.	4.4	4.4		All cryptographic code within the module shall be in executable form. Comments: Could "code" be construed as "source code"? We should have precise terminology.	Jean Campbell - CSE	**Accepted:** revised
572	J.C.	4.4			In addition to the requirements of Security Level 3, the following requirements shall apply to software contained within a cryptographic module for Security Level 4. Comments: This whole section is difficult to understand.	Jean Campbell - CSE	**Accepted:** Removed
590	B.M.	4.4	Sec. 4.4		Has the time required to perform the Approved authentication technique to verify the validity of software been estimated or measured for the case of a smart card like the PIV Card? Since a PIV Card is often "started" immediately before a crypto operation, users are extremely sensitive to any delays in startup. Can this verification be done in 200 ms or less?	Bill MacGregor NIST	Don't know the answer – it depends on the card's capabilities.
594	C.B.	4.4	Section 4.4		Software Security, Security Level 3 Requirements: Consider adding an additional requirement for Key Management that will require that if a module supports key management functionality at Level 3 that all CSP's be encrypted using a FIPS recommended or Approved method. The reason is that DOMUS has seen the emergence of Key Management applications for which vendors can define a cryptographic boundary that allows keys to be stored in plaintext. It is my belief that if a vendor is marketing a key management product that all keys and CSP's within the cryptographic module boundary must be stored in encrypted form.	Chris Brych - DOMUS	**Accepted:**

636	T .V.	4.4	Sec.4.4		Software integrity checks (4.4) The explicit requirement for a cryptographically strong integrity check on software contained within the module is redundant. Assuming the module controls software load into internal, trusted storage, one only needs to protect 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 (and subsequent management etc. of this key material). Similar observations are applicable for Security Level 2 and higher. Note that protecting internal storage does not gain addition security from switching to digital signatures (i.e., asymmetric techniques). We obviously do not question strong integrity checks on software loaded externally. We also think changing the requirement from simple EDC schemes, such as checksums, to cryptographic hash functions (for example) may be reasonable, but requiring keyed mechanisms is not.	Visegrady, Tamas	**Accepted:** Discuss whether keyed integrity check is needed :
670	W.C.	4.4	Sec 4.4		2nd bullet item of the section "A cryptographic mechanism using an Approved integrity technique ... shall be applied to all software within the cryptographic module.": Please clarify "all software". Does this requirement apply to the operating system or other non-crypto software? XXX Page 22, 1st bullet item under SECURITY LEVEL 2: Please define "The entity requesting validation". Is it the vendor of the module? The user/operator of the module?	Wan-Teh Chang	**Rejected:** Operating system is not in the module Text removed.
820	IG	4.4	Sec. 4.4		Level 1, 2nd bullet: Probably needs to say ‘approved data authentication technique’ instead of approved	InfoGard	**Accepted:** revisited

					'integrity technique.'		
821	IG	4.4	Sec. 4.4		Level 1, bullets 5 and 6: These seem to be restating the same requirement. Level 1, last bullet: Either the 'format' for externally provided data needs to be clarified to state that it applies only to data that is relevant to the security of the module. Otherwise, this requirement should be removed altogether. It's not clear that the module is generating the digital signature or if the vendor is generating the signature outside of the module. Should simply state that it will verify a digital signature and the public key will be inside the module (and the private key outside the module). Levels 4 and 5: These are not reasonable requirements for software (whether in a hardware module or purely software) as currently defined (meaning 'any module containing software'). Either these requirements should be removed or it should be asserted that there will be no Level 4 or 5 modules that 'contain software.'	Inforgard	**Accepted:** Addressed Removed Clarify in text A module may be validated by another external cryptographic module. The first loaded module must validate itself. Text removed
825	IG	4.4	Sec. 4.4		The explicit requirement for a cryptographically strong integrity check on software contained within the module is redundant. Assuming the module controls software load into internal, trusted storage, one only needs to protect 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 (and subsequent management etc. of this key material). Similar observations are applicable for Security Level 2 and higher. Note that protecting internal storage does not gain addition security from switching to digital signatures (i.e., asymmetric techniques). We obviously do not question strong integrity checks on software loaded externally.	InfoGard	Consider as before

901	CL	4.4	Sec. 4.4		Is it intended that the Software Integrity Test Decryption Key be provided to the module on each power-up? This seems to be implied, but isn't clearly stated. Also, assigning a common name to this key would make it easier to refer to.	CEAL	**Accepted:** See revised Text
902	CL	4.4	Sec. 4.4		This requirement has an implied race condition because it doesn't have a requirement that the encrypted CSPs and Integrity Test code only be decrypted to volatile memory. If they are decrypted in place on non-volatile memory, and the module loses power before it can re-encrypt them, then this protection is lost.	CEAL	**Accepted:** Text removed.
904	CL	4.4	Sec. 4.4		"The MSI command shall return an indication as to whether the Software Integrity Test was successful and a newly computed hash value." Is this requirement intended to force a module to provide a single digital signature (and underlying hash) for the entire module software? Or is it acceptable to have multiple digital signatures as long as all the module software is covered by at least one digital signature? (Also consider a hybrid module, which may have software in the hardware half, as well as the software portion) How should a module with loaded software handle this requirement? After the software is loaded should it overwrite the modules stored digital signature, replacing it with a new digital signature which covers the module + loaded software? (Note: this may be affected by the discretionary access control requirements) Or should the module ignore the loaded software while running this integrity test and only return a hash on the original software? Or should it return a hash on the original software and a second hash for the loaded software? Should this hash be the same one used internally by the digital signature algorithm or should it (or can it) be an additional hash?	CEAL	**Accepted:** Text Removed
951	CL	4.4	Sec. 4.4		"The MSI shall not permit the operator to modify module software without invoking the Software Load Test" Does this requirement apply to the operating system? If not please clarify.	CEAL	**Accepted:** Text Removed

952	CL	4.4	Security Level 4, Bullet Point 1		“shall be encrypted by the vendor” To be consistent with the security level 2 description, should “vendor” be “entity requesting validation” instead?	CEAL	**Accepted:** Text Removed
963	I.F.	4.4			The module shall enforce restrictions on password selection to prevent the use of weak passwords (e.g. the module shall prevent against dictionary attacks).This needs to be clarified. How should the module enforce this? In particular, what if the password is a PIN? What is considered to be a bad PIN? Excluding PINs from all possible PIN values just reduces the search space for an attacker.	Indra Fitzgerald	**Accepted:** Move to 4.3.2
964	I.F.	4.4			This whole section (in particular the first three bullet points) needs to be clarified, as it is very confusing. The draft standard states that all CSPs as well as the Software Integrity Test software shall be encrypted by the vendor using an Approved encryption with an authentication mode. This appears to be on top of the digital signature that shall be performed as part of the Software Integrity Test. It seems unnecessary to have an encryption algorithm with an authentication mode when you are already signing the software. When exactly should the CSPs and Software Integrity Test software be encrypted? What about the code that performs the decryption? How should that be protected?	Indra Fitzgerald	**Accepted:** Move to 4.3.2 Text Removed Text Removed
965	I.F.	4.4			When exactly should the CSPs and Software Integrity Test software be encrypted? What about the code that performs the decryption? How should that be protected?	Indra Fitzgerald	**Accepted:** Text Removed
966	I.F.	4.4			The security strength shall be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation. If the module supports a number of algorithms, including the weaker FIPS-approved ones (for backward compatibility), does this result in a reduction in the security strength of the module to that of the	Indra Fitzgerald	**Accepted:** Wrong Section see Section 4.1.5

					weakest supported algorithm? How do you determine the strength of the module when the module implements a security protocol such as TLS?		
967	I.F.	4.4			Does this only apply for the crypto officer? What if the user of the module is not a human, but a process? Do passwords coupled with certificates meet the two-factor requirement?	Indra Fitzgerald	See above
1023	R.E.	4.4			Replace document with : relevant documentation	Randy Easter - NIST	**Rejected:** Please provide additional information
1024	R.E.	4.4			Omit: including copies of the user and installation manuals	Randy Easter - NIST	**Rejected:** Please provide additional information
1081	R.E.	4.4	4.4		The requirements of this section apply to modules containing software. Comments: Does this include software only modules?	Randy Easter - NIST	YES
1153	R.E.	4.4	4.5		The operational environment of a cryptographic module is the set of all software and hardware required for the module to operate securely. For example, the operational environment of a software module includes the module itself,	Randy Easter - NIST	**Accepted:** Move to 4.5
1154	R.E.	4.4			What is the relationship to operational environment and module boundary? Unclear.	Randy Easter - NIST	**Rejected:** Please provide additional information
1156	R.E.	4.4			authenticated? A non-modifiable operational environment is designed to contain only validated software.	Randy Easter - NIST	**Rejected:** Please provide additional information
1157	R.E.	4.4			A non-modifiable operational environment is designed to contain only validated software. This environment may be software operating in a non-programmable computer (e.g., a non-programmable card or non-programmable smartcard), or software whose update is controlled using Approved data authentication processes (i.e., through the Software Load Test specified in Section 4.9.2). If the open environment is non-modifiable, then the operational en modifiability shall be bound to the software module.	Randy Easter - NIST	**Rejected:** Please provide additional information

1158	R.E.	4.4			So the OS/Platform can enforce this for a software module? Is that a hybrid module?	Randy Easter - NIST	**Rejected:** Please provide additional information
1165	R.E.	4.4			Software on a processor that allows the input of non-validated executable code. Comment: Modifiable?	Randy Easter - NIST	**Rejected:** Please provide additional information
1255	R.E.	4.4	4. Software Security		Define the module boundary, contents, and logical security mechanisms.• Separately list the security and non-security services.• How is the code protected from replacement?• How is the code obfuscated?• What are the tamper detection and response capabilities?	Randy Easter - NIST	**Rejected:** Please provide additional information
8	D.F.	4.4		GE	Section 4 – Software Security: 4.3.3) Is a UI module required to provide feedback to the operator? How should this be done? Do we need to provide status on everything?	David Friant - Microsoft	**Accepted:** Move to 4.3.3

tID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
5	D.F.	4.5	4.5.1		"The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not." On the face of it, this appears to disallow most/all debuggers. Perhaps it needs an exception for maintenance mode?	David Friant - Microsoft	**Accepted:** This comment might still apply to bullet 2 in Section 4.5.1. Should an exception be made for the maintenance mode? We modified text to make the maintenance mode and exception.
61	H.F.	4.5	4.5		According to table 2 (Examples of Operational Environment), the PIV smart card would be categorized as non-modifiable operational environment, if only validated software is loaded. Under these condition the audit trail requirements do not apply for level 2. Is this assumption correct? Due to very limited memory, a smart card (modifiable OE) might not be able to adhere to the audit requirements. Have limited-memory cryptographic module been considered with this requirement? Consider quantifying how for long the audits need to be maintained.	Hildy Ferraiolo	.**Accepted:** Yes Yes at level 2 and above. This is not necessary since audit data may be output from the module/operational environment? The application and policy determine how long data needs to be retained.
87	J.C.	4.5	Sec. 4.5		The term "non-modifiable operational environment" appears to be confusing and inaccurate, since this environment can be updated "or software whose update is controlled using Approved data authentication process". Recommend changing "non-modifiable operational environment" to "configuration controlled operational environment" or "validated operational environment", since only validated software is resident.	James Cottrell- MITRE	**Accepted:** Does the group wish to change at this point? No but add definition of non-modifiable environment

100	C.P.	4.5	4.5.		Standard: Table 2. Example of Operational Environments Example of Operational Environments Row 4 in the table, “Software on a processor that allows the input of non-validated executable code.” Suggestion: Not clear for me what non-validated code means, in this context.	Claudia Popa - CSE	**Accepted:** Code that has not been validated as part of the cryptographic module or a validated download.
101	C.P.	4.5	4.5.1		“All CSPs shall be zeroized before each operator‘s session is terminated and a new operator’s session is begun.” Do we need the AND part? Is this not enough? “All CSPs shall be zeroized before each operator‘s session is terminated.” “All MSI commands in a session shall be run on behalf of a single operator.” If the system is restricted to a single operator session, do we need this requirement?	Claudia Popa - CSE	**Rejected:** This text has been removed. **Rejected:** This text has been removed.
106	C.P.	4.5			In the standard all the references to “firmware” were removed, but in the Security Policy there are still references to firmware modules.	Claudia Popa - CSE	**Accepted:** References to firmware will be added again.
125	D.F.	4.5			“The operating system shall prevent operators and external executing processes from reading cryptographic software stored within the cryptographic boundary.” The Windows binary code is not a secret. The executable files that contain the crypto code are readable by the user. The code of a dynamic link library (DLL) in user space is readable by any thread in that process. Depending on how the various terms are interpreted this could be an impossible requirement to meet. What does this requirement actually mean?	David Friant Microsoft, Redmond, WA.	**Accepted:** This text has been changed to “The operating system shall be configured to prevent access by other processes to CSPs. .

161	J.R.	4.5	4.5.1		The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not. o The operating system shall prevent operators from gaining either read or write access to SSPs of other operators. Comments:(notes) This definition is very unclear - what is an OS process and what is not on a given platform? For unix-like platforms the "root" user has full access; for windows-like platforms the administrator user has full access. Many processes in both types of environment run which are not "operating system processes". It would make sense to require the OS to enforce separation of state between the various authenticated operating system users - i.e. preclude sharing of state between different operators - by technical measures implemented in the module. However a privileged user can work around all these mechanisms by definition - that is one of the core concepts of being on a general purpose platform. If "operators" is defined as all non-privileged users (i.e. all users of the module shall not be operating system privileged users) then there is scope for these requirements being able to be met in a fashion; however one OS user has access to another instance of the same OS users internal state (unless the module operates as the operating system privileged user and does not use standard in-process dynamic linking/shared library access techniques. i.e. if the module is constructed in an entirely different manner to current 140-2 software based cryptographic modules.	James Randall RSA	**Rejected:** This text has been reworded. **Accepted:** Privileged users should be privileged module users as well

169	J.R.	4.5	4.5.1		SECURITY LEVEL 1 The following requirements shall apply to operating systems restricted to a single operator session at any given time (i.e., concurrent operators are explicitly excluded) for Security Level 1. • All MSI commands in a session shall be run on behalf of a single operator. • All CSPs shall be zeroized before each operator's session is terminated and a new operator's session is begun. • Processes that are spawned by the cryptographic module shall be owned by the module operator. . Comments: (notes) This is not how current platforms operate - and would require that the module run as a separate user on the system and not as dynamically loadable libraries or shared libraries. For modules which require external processes this will break the current handling under 140-2	Janes Randall RSA	**Accepted:** Bullets 1and 2 have been removed. Bullet 3 has been reworded. This text has been reworded.
179	D.F.	4.5	Sec. 4.5.1		"The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not." On the face of it, this appears to disallow most/all debuggers. Perhaps it needs an exception for maintenance mode? Proposed Disposition: Leave requirement as is. Debuggers should be run in the maintenance mode.	David Friant Microsoft, Redmond, WA.	**Rejected:**
180	D.F.	4.5	Sec. 4.5.1		It is not clear from the definition of cryptographic boundary in section 4.1.2 whether the requirement would restrict any application from reading the compiled code of a crypto module DLL. It is also not clear if "external executing processes" refers to processes running in different user contexts or those that run on a different CPU or computer. A clearer definition for external executing processes is needed. What does this mean about OS controlled memory, paging, etc?	David Friant Microsoft, Redmond, WA.	**Accepted:** The text has been reworded

200	J.R.	4.5	4.5.1		The configuration of the operating system to meet the above requirements shall be specified in a Crypto Officer guideline. The Crypto Officer guideline shall state that the operating system must be configured as specified, before the module contents can be considered as protected. Comments: (Inset) for the module to be operating in an approved manner in accordance with the module's security policy.	James Randall RSA	**Rejected:** Text seems OK as written.
204	J.R.	4.5	4.5.1		• The operating system shall provide an audit mechanism to record modifications, accesses, deletions, and additions of cryptographic data and SSPs. If audit information is stored outside of the module, then the module shall use Approved cryptographic mechanisms to protect the information when external to the module from unauthorized disclosure and modification. Comments: (note) The audit mechanism is outside the module - and hence outside the control of any protection mechanisms. If the intent is that all information passed to the audit service of the operating system requires to be protected prior to being sent to the audit mechanism then that should be clearly stated - either it gets protected before going to the OS or it is unprotected.	James Randall RSA	**Accepted:** FIPS 140-3 does put requirements on the operational environment if they are modifiable. This is a requirement on the operating system to protect CSPs. Inside the module audit info is protected by the operating system
205	J.R.	4.5	4.5.1		The module Security Policy shall specify whether identification and authentication of module operators is performed by operating system code or vendor supplied code. In either case, the identification and authentication mechanism shall meet the requirements of Section 4.3.2. Comments: (insert)by the module " vendor supplied code."	James Randall RSA	**Rejected:** This text has been reworded.

206	J.R.	4.5	4.5.1		All SSPs, authentication data, control inputs, and status outputs shall be communicated via a Trusted Channel. Communications via this Trusted Channel shall be activated exclusively by an operator or the cryptographic module. The Trusted Channel shall provide source authentication and shall prevent unauthorized modification, substitution, disclosure, and playback of sensitive security parameters. Comments:(notes) What is meant by "source authentication" in this context?	James Randall RSA	**Accepted:** Source authentication is the authentication of module operators or trusted entities operating on behalf of the operators.
207	J.R.	4.5	4.5.1		SECURITY LEVELS 4 AND 5 In addition to the applicable requirements for Security Level 3, the following requirements shall apply for Security Levels 4 and 5. • The audit mechanism shall be permanently configured so that the following events are always audited: Comments: (delete) permanently	James Randall RSA	**Rejected:** Levels 4 and 5 have been removed from this section.
274	J.L.	4.5	1.5		This is a general comment. It is clear that each security level consists of all the requirements of the lower levels plus some additional requirements from the new level. However, in reading the document the security requirements are not always presented consistently: some state the new requirement includes the lower level requirements and some do not. Uniformity supports clarity.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Rejected:** Not true for Section 4.5 but the entire document should be checked. Section 1 is a summary so statements about inclusion of lower level requirements are not necessary.
298	J.L.	4.5	4.3.2		Fourth para - 'for a software … of this section' states nothing about the security status of the Operating system; must the OS be evaluated, and if so, to what standard? An authentication mechanism on an untrusted operating system, may not provide the needed security;	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted:** Move to Section 4.3.2. The assurance required for the operating system can be specified in the DTR.

303	J.L.	4.5	4.5.1		Comments: Ref to 2nd sub bullet in security level 2 - how long is the audit trail kept? I suggest adding a ref to provide guidance. Needed for clarity, completeness and to ensure security. • The operating system shall137 provide an audit mechanism to record modifications, accesses, deletions, and additions of cryptographic data and SSPs. If audit information is stored outside of the module, then the module shall138 use Approved cryptographic mechanisms to protect the information when external to the module from unauthorized disclosure and modification. o The following events shall139 be recorded by the audit mechanism: - attempts to provide invalid input for Cryptographic Officer functions, and - addition or deletion of an operator to and from a cryptographic Officer role. o The audit mechanism shall140 be capable of auditing the following events: - all operator read or write accesses to audit data stored in the audit trail, - 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, - the use of an authentication mechanism (e.g., login) associated with the cryptographic module, and - explicit requests to assume a crypto officer role.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Rejected:** This may be beyond the scope of FIPS 140-3 since the audit data may be exported from the operating environment it could be kept indefinitely. We don't say how long a key may be kept.
331	J.L.	4.5	Sec. 1.5		This is a general comment. It is clear that each security level consists of all the requirements of the lower levels plus some additional requirements from the new level. However, in reading the document the security requirements are not always presented consistently: some state the new requirement includes the lower level requirements and some do not. Uniformity supports clarity.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted:** Each level in Section 4.5, above level 1, states that it includes the previous level. Other sections need to be checked.
383	J.K.	4.5	4.5.1		What does "system SSPs" mean? Define the "system SSP" in section 2.1.	JCMVP19 Junichi Kondo	**Rejected:** Section 2.2 states that SSP stands for Sensitive Security Parameter. Section 2.1 defines the term.

384	J.K.	4.5	4.5.1		"Crypto Officer guideline" seems to be "Administrator guidance". Rewrite "Crypto Officer guideline" as "Administrator guidance".	JCMVP18 Junichi Kondo	**Accepted:**
385	J.K.	4.5	4.5.1		What does "session" mean? Define the "session" in section 2.1.	JCMVP17 Junichi Kondo	**Rejected:** No longer used in the standard.
397	M.S.	4.5			Several of the security requirements specified in Section 4.5 might also be applied to software modules that are not functioning in a modifiable operational environment. That is to say, these requirements might be more appropriate in Section 4.4. For example, why shouldn't auditing requirements be applied to all Level 2 and above software and firmware modules rather than only those operating in a modifiable operational environment? Also, why shouldn't a trusted channel be required between authenticated operators and the module at Level 3 and above for all software modules rather than only those operating in a modifiable operational environment? I would recommend that NIST consider which of the requirements of Section 4.5 might be more appropriate in Section 4.4.	Miles E. Smid	**Accepted:**
462	J.L.	4.5	Sec. 4.5.1		Ref to 2nd sub bullet in security level 2 - how long is the audit trail kept? I suggest adding a ref to provide guidance. Needed for clarity, completeness and to ensure security.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted:** Same as previous comment
513	T.C.	4.5	Sec 1.2		How are the O/S functionalities specified in Section 4.5 verified? Also, DAC appears to already come in Level 1 in Section 4.5.	Tom Casar	**Rejected:** See DTR for verification. DAC is no longer required.
515	T.C.	4.5	Sec. 1.5		Level 4 already has EFP mechanisms, so why mention here again?	Tom Casar	**Accepted:** Move comment to Section 1.
540	T.I.	4.5	Sec. 4.5 Operational Environment		As the trusted channel of Security Level 3, there required preventive measures against alteration, replacements, exposures and playbacks. Does the all parameters of "The Trusted Channel…parameter." have to be satisfied? The authentication function of "The Trusted Channel" can be altered by the function of "Operator Authentication Function" in the 4.3.2?	Toru Ito - Cryptrec & INSTAC	Must prevent unauthorized disclosure and spoofing.

565	J.C.	4.5			The requirements of this section apply only to modules containing software that run in a modifiable operational environment. The requirements of this section do not apply to hardware only modules or any modules with a non-modifiable operational environment. Comments: The opening paragraphs are too long.	Jean Campbell - CSE	**Accepted:** This text has been removed; however, Section 4.4 has a similar introductory paragraph. Should it be removed? Also non-modifiable has not been defined.
573	J.C.	4.5	Sec. 4.5		The opening paragraphs are too long.	Jean Campbell - CSE	
591	B.M.	4.5	Sec. 4.5.1		Regarding the audit mechanism, it is not clear how audit information should be processed by a smart card with limited memory resources. A PIV Card is typically used at a reader in a relying system; it does not have network communications capability while in use, and cannot depend on the presence of a trusted channel. Would it be satisfactory for a PIV Card to retain the last N audit records (where N is a small integer)?	Bill MacGregor NIST	**Accepted:** Audit data need not be stored on the card.
595	C.B.	4.5	Section 4.5.1		Operating System Requirements for Modifiable Operational Environments. Security Level 1 2nd Bullet states: "All CSP's that shall be zeroized before each operator's session is terminated and a new operator's session is begun." If I were to interpret this requirement for a disk encryption product, all keys must be zeroized when a session is terminated. If all the keys are zeroized, the hard disk cannot be unencrypted as all the keys will have been destroyed. Please reconsider this requirement or clarify the requirement.	Chris Brych - DOMUS	**Accepted:** The key could be output and re-entered, however, this text has been removed.
602	C.R.	4.5	Section 4.5.1		Recommend updating bullet text to clarify by saying "All CSP's related to the operator's session shall be zeroized". The current wording implies that all CSP's must be zeroized within the cryptographic boundary. Zeroizing all CSP's at the conclusion of each operator session would cause a large burden on users of the validated product.	Chris Romeo - Cisco	**Rejected:** This text has been removed.

603	C.R.	4.5	Section 4.5.1		Text: "The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not." This guidance appears to prevent software upgrades because neither operators nor executing processes can be modified. We recommend that the text be updated to specifically allow software upgrades to occur while operating in FIPS mode. Eliminating software updates would lock the cryptographic officer into a single FIPS validated release of code and would stop them from updating to the latest version of software for added protection in the face of new threats. For cryptographic modules that contain failover components that run multiple versions of code simultaneously, the secondary module could be upgraded and could then execute it's software load and integrity tests and then failover from the primary. Once the secondary takes over, the same process could be repeated for the primary device. For devices that run a single instance of code, a new software load to upgrade the FIPS validated version should be permitted followed by a reboot of the module. If a hot upgrade is performed without rebooting the module, notification of the update event and execution of all self-tests and software load / integrity test should then allow the module to continue to operate in FIPS mode.	Chris Romeo - Cisco	**Accepted:** This text has been reworded to only prevent access to CSPs by “other processes”.
620	M.S.	4.5	Sec. 4.5		Several of the security requirements specified in Section 4.5 might also be applied to software modules that are not functioning in a modifiable operational environment. That is to say, these requirements might be more appropriate in Section 4.4. For example, why shouldn’t auditing requirements be applied to all Level 2 and above software modules rather than only those operating in a modifiable operational environment? Also, why shouldn’t a trusted channel be required between authenticated operators and the module at Level 3 and above for all software modules rather than only those operating in a modifiable operational	Miles E. Smid	**Accepted:** Same as previous comment.

					environment? I would recommend that NIST consider which of the requirements of Section 4.5 might be more appropriate in Section 4.4.		
673	W.C.	4.5	Sec. 4.5.		3rd paragraph: Change "smartcard" to "smart card".	Wan-Teh Chang	**Accepted:**
674	W.C.	4.5	Sec. 4.5.		Examples of Operational Environment: In the 4th row, what does "isolate input data" mean? In the 5th row, should "a processor" be changed to "a computer" to be consistent with the 4th and 6th rows? Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Accepted:** Does not permit the execution on input data as code. I think we want some input parameters to enter the module but perhaps not others. Changed processor to computer.
675	W.C.	4.5	Sec. 4.5.1		Change "physical protection to the module" to physical protection of the module. Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Rejected:** This text could not be found.
676	W.C.	4.5	Sec. 4.5.2		SECURITY LEVEL 1: If the operating system allows multiple concurrent operators, matching operator authentication requirements need to be added to Section 4.3.2. Page 25, last bullet item "The operating system shall prevent operators and external executing processes from reading cryptographic software stored within the cryptographic boundary.": In a general purpose operating system, the operator can attach a debugger (process) to a cryptographic process to read and modify executing cryptographic software. Moreover, the root user (also known as the Administrator) may be able to attach a debugger (process) to a cryptographic process of the operator. Does this requirement allow the debugging capability and the root user privilege as exceptions? Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Rejected:** This text has been removed.

746	EW	4.5	Sec. 1.5		Level 5 modules have environmental failure protection mechanisms that protect the module from fluctuations in temperature and voltage. Level 5 modules are opaque to non-visual radiation examination and the tamper detection and zeroization circuitry is protected against disablement. When zeroization is required, PSPs as well as CSPs are zeroized. Should this not say “non-visible”?	EWA	**Accepted:** Move to section 1.5
826	IG	4.5	Sec. 4.5		The wording of this requirement makes little or no sense.	InfoGard	**Rejected:** Text has been removed.
827	IG	4.5			Table 2, 4th row: It’s not clear what ‘Software on a computer that does not isolate input data’ means.	InfoGard	**Accepted:** Same as previous comment
828	IG	4.5	Sec. 4.5.1		Immediately after Table 2: If the operational environment is non-modifiable, the operating system requirements in Section 4.5.1 do not apply. Note: This should likely read that “…in Section 4.5.1 shall not apply.”	InfoGard	**Accepted:** This has been addressed in the new version.
829	IG	4.5	Sec. 4.5.1		2nd bullet of Security Level 1: It would seem this should apply to ‘user specific’ CSPs such as those related to authenticating a particular user. "All CSPs shall125 be zeroized before each operator’s session is terminated and a new operator’s session is begun."	Inforgard	**Rejected:** This requirement has been removed.
830	IG	4.5	Sec. 4.5.1		3rd bullet: It’s not clear what ‘owned by external processes’ means.	InfoGard	**Accepted:** This has been removed or reworded..
831	IG	4.5	Sec. 4.5.1		(general): The notion of crypto module roles and operating system ‘users’ is conflated.	Inforgard	**Accepted:** The operating system must protect CSPs and crypto code. When a user is authenticated, access to the module is permitted by the operating system. If the user is not authenticated, then access is controlled by the operating system.
832	IG	4.5	Sec. 4.5.1		Level 2, 3rd bullet: Shall audit mechanisms audit and not just be capable of auditing?	InfoGard	**Accepted:** That may be application dependent.

883-1	AT	4.5			•Section 4.5.1, Security Level 1 requirements, the language in this section seems to disallow multi-threaded software applications. Is this truly the CMVP's intent? Perhaps definition of what constitutes a "session" would be helpful in understanding the intent.	Atlan	**Accepted:** Multi threading is allowed. The text has been modified.
883-2	AT	4.5			•Section 4.5.1, Security Level 2 requirements, first bullet. The responsibilities of the OS and the module seem to be blurred. If audit information is stored in a flat file on an operating system and then copied outside the bounds of the PC onto a networked drive, does this need to be encrypted? Is audit information considered confidential? Should this audit information be protected against unauthorized substitution and modification? •Has the CMVP reviewed the widely used Operating Systems to see if they can meet these requirements? Are we setting the bar too high to be achieved?	Atlan	**Accepted:** Data inside the PC is protected by operating system. Data outside PC is protected cryptographically. Changed to just require modification and substitution protection. Audit information should be protected protect against unauthorized substitution and modification.
884-1	AT	4.5	Software Security		•Do the software security requirements apply to all modules? Most "hardware" products today contain software/firmware running within the module. Recommend making this explicit in the standard.	Atlan	Does this comment apply to Section 4.4 or Section 4.5? Section 4.4 applies to all modules containing software or firmware. Section 4.5 applies only to modifiable operational environments.
884-2	AT	4.5	Software Security		•Last bullet, "if a specific format for externally provided data is expected, then the module shall verify the format." What level of format checking is necessary?	Atlan	**Rejected:** This text has been removed
884-3	AT	4.5	Software Security		•First bullet of Security Level 3 section, the last sentence is confusing. "The MSI command shall return an indication as to whether the Software Integrity Test was successful and a newly computed hash value." The last half of the last sentence seems to be incomplete.	Atlan	**Rejected:** Text has been removed.
884-4	AT	4.5	Software Security		•Security Level 4 bullets. The intent of these requirements is not clear. Is the CMVP requiring that software modules be distributed the vendor in encrypted form? The third bullet also seems to indicate that the integrity test needs to be recalculated upon initial installation using a new key pair generated by the	Atlan	**Rejected:** This text has been removed.

					module. Is this truly the case? If so, it's not clear what additional security this provides a module.		
896	CL	4.5	Section 4.5.1		"attempts to use the trusted channel function" Should the success or failure of the attempt also be stored in the audit record?	CEAL	**Accepted:** Yes incorporate this requirement.
897	CL	4.5	Sec. 4.5.1		Should there be an explicit requirement that the audit record include date and time information for each audit event? If so should there be crypto officer guidance requiring the CO to ensure that the clock the audit record is using is accurate?	CEAL	**Accepted:** Consider this comment
898	CL	4.5	Sec. 4.5.1		"If audit information is stored outside of the module" By "module" do you mean the vendor software (e.g. crypto library) or the whole computer? Ensuring audit data is encrypted prior to sending it out of the computer is more manageable (but still runs into problem with companies that have set up central audit servers at the OS level, which the module might be unaware of), but forcing the OS to encrypt data before the OS writes it to the audit log is likely impractical.	CEAL	**Accepted:** (Security level 2 first bullet) Outside of the operational environment was intended here. In other words, the module would have an encrypt capability for export of audit data command and decrypt capability upon import. This should be clarified Changed to only modification and substitution protection.
899	CL	4.5	Sec. 4.5.1		"The operating system shall prevent operators and external executing processes from reading cryptographic software stored within the cryptographic boundary." Is this intended to apply to other operators with normal user permissions, or is the OS somehow suppose to protect against operators or processes running at the root / super-user / administrator / system level? And does the prohibition against read access from external executing processes apply to system backup software?	CEAL	**Accepted:** (Secrurity Level 1) This text has been re-written.
900	CL	4.5	Sec. 4.5.1		"Processes that are spawned by the cryptographic module shall be owned by the module and shall not be owned by external processes/operators." This works for threaded processes, threads are owned by the parent process. But how does this requirement apply to helper or forked processes. They are usually owned by the operator who is running the process that called them, but they don't have a parent process so can't really said to be owned by the module's process.	CEAL	**Accepted:** This text has been re-written

932	CL	4.5	Sec. 4.5		Can an operation environment be considered non-modifiable if there are steps required prior to initialization which lock down the environment transforming it from a modifiable environment to a non-modifiable one? After these steps are performed the environment would be incapable of loading code (except potentially using the software load test function) and the steps could not be reversed, the module would have to be deleted and reinstalled to get out of the locked down configuration.	CEAL	**Accepted:** Yes.
941	CL	4.5	Sec. 4.5		"Software on a computer whose operating system is reconfigurable by the operator allowing the removal of the security protections." Does a bypass mode count as "the removal of the security protections"? Is a module with a bypass mode inherently considered to be running on a modifiable operational environment?	CEAL	**Rejected:** No. The existence of a bypass is independent of the modifiability of the operational environment.
953	CL	4.5	Section 4.5 & Section 4.6		The definition of "non-modifiable operational environment" and "a cryptographic module implemented completely in software" seem to allow for the potential of a module which was implemented completely in software on a non-modifiable operation environment. Such a module appears to circumvent the requirements of both Section 4.5 and Section 4.6.	CEAL	**Rejected:** Yes they can be considered NA Circumvent is not the correct term here.
1059	R.E.	4.5	Table 2 Example of Operational Environment		Software on a processor that allows the input of non-validated executable code. Modifiable. Comments: This standard should be independent of any validation authority or process.	Randy Easter - NIST	**Accepted:** A non-modifiable module can input validated code but cannot input non-validated code. Is reworded text acceptable? Consider a smart card. It can be either limited or modifiable. See definition of modifiable operational environment
1068	R.E.	4.5			The configuration of the operating system to meet the above requirements shall be specified in a Crypto Officer guideline. The Crypto Officer guideline shall state that the operating system must be configured as specified, before the module contents can be considered as protected. Comments: At Level 1, what if being protected? It is an unevaluated OS with untrusted applications running concurrently …	Randy Easter - NIST	**Rejected:** This text has been removed.

1159	R.E.	4.5			• All CSPs shall be zeroized before each operator's session is terminated and a new operator's session is begun. Comments: So all CSPs must be zeroized between each User (a User is an operator) of an instance of a module? How can this be?	Randy Easter - NIST	**Rejected:** This text has been removed.
1160	R.E.	4.5			The operational environment of a cryptographic module is the set of all software and hardware required for the module to operate securely. For example, the operational environment of a software module includes the module itself, the processor on which the software is executed, and the operating system that controls the execution of the software. An operational environment can be non-modifiable or modifiable. Comments: (Insert) What is the relationship to operational environment and module boundary? Unclear.	Randy Easter - NIST	**Accepted:** The operational environment contains the module boundary since it "includes the module itself" See first paragraph of Section 4.5 May need a second definition for software cryptographic module boundary.
1161	R.E.	4.5			• All MSI commands in a session shall be run on behalf of a single operator. Comments: (Strikeout)(in a session)" for each executable instance of a software module …"	Randy Easter - NIST	**Rejected:** This text is no longer present.
1163	R.E.	4.5			Operating systems are considered to be modifiable operational environments if software 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.	Randy Easter - NIST	**Accepted:**
1168	R.E.	4.5	4.5.1		The following requirements shall apply to operating systems restricted to a single operator session at any given time (i.e., concurrent operators are explicitly excluded) for Security Level 1. Comments: This appears to contradict an earlier section of the standard where concurrent operators are allowed.	Randy Easter - NIST	**Rejected:** This text has been removed.

1169	R.E.	4.5			The following requirements shall apply to operating systems restricted to a single operator session at any given time (i.e., concurrent operators are explicitly excluded) for Security Level 1 Comments: This appears to contradict an earlier section of the standard where concurrent operators are allowed.	Randy Easter - NIST	**Rejected:** This text has been removed.
1170	R.E.	4.5			A non-modifiable operational environment is designed to contain only validated software. This environment may be software operating in a non-programmable computer (e.g., a non-programmable card or non-programmable smartcard), or software whose update is controlled using Approved data authentication processes (i.e., through the Software Load Test specified in Section 4.9.2). If the operational environment is non-modifiable the n the operational environment components that enforce the non-modifiability shall be bound to the software module. Comment: "operational environment" What is the relationship to operational environment and module boundary? Unclear.	Randy Easter - NIST	**Accepted:** See previous comment # 1160
1171	R.E.	4.5			A modifiable operational environment is designed to allow loading of non-validated software. This environment may include general purpose operating system capabilities (e.g., use of a computer O/S or configurable smart card O/S). Operating systems are considered to be modifiable operational environments if software 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. Comment: (1) (non-validated) un-authenticated? Comment: (2) (O/S) operating system? Is this abbreviation or term defined? Comment: (3) (validation) Replace with" boundary"	Randy Easter - NIST	**Accepted:** Text reworded (See definition of modifiable operational environment) 1. No. It means "not included as part of the validation of the module" 2. Use operating system 3. Could be outside of the boundary but within the operational environment.

1262	R.V.	4.5	Sec. 4.5.1		Achieving a Security Level Certification for Smart Cards in the Current Draft Section 4.5.1 Operating System Requirements for Modifiable Operational Environments in particular details the requirements for a modifiable operational environment. When this section is reviewed from a smart card cryptographic module implementation perspective one observes the following: 1. Security Level 1 appears to be achievable by the most-deployed configurations of smart card operating systems offered today (e.g., MULTOS or JavaCard with GlobalPlatform) when restricted to a single operator session, as is the normal practice. 2. Security Level 2 may be difficult to achieve depending on the interpretation of the requirement. For example, the FIPS 140-3 draft states: "The audit mechanism shall be capable of auditing the following events: … the use of an authentication mechanism (e.g., login) associated with the cryptographic module…" Such a requirement may not be practical for smart cards with limited storage capability and frequent use of such authentication mechanisms. FIPS 140-3 allows audit information to be stored outside of the module to cover such a situation where storage is limited. However, to store this audit information outside of this type of "module" raises other issues such as the availability of the module when an audit is requested for security or operational needs. (Such "modules" are deployed in the millions to end users and are outside of the immediate control of the cryptographic officer). 3. Security Level 3 may be impossible to achieve depending on the interpretation of what constitutes an acceptable Trusted Channel. For example, GlobalPlatform (GP) offers a "Secure Channel" (GP Secure Channel Protocol 01 / 02). This tool is used by the government today to provide confidentiality and data integrity checking for information from an authorized operator to the module; it is not a bi-directional mechanism (for SCP01). Modifying the Secure Channel would break most, if not all, smart card personalization and operational systems in use in the Federal government today. The smart card industry is concerned about achieving the necessary security levels as currently drafted in	Randy Vanderhoof, Executive Director, Smart Card Alliance	**Accepted:** External storage could be used This is only for smart cards that are modifiable operational environments. Is GP Secure Channel Protocol acceptable? If the protocol protects against unauthorized modification, substitution, disclosure and provides authentication of the source.

					FIPS 140-3 and suggests that NIST add clarifying language on how to achieve each security level. We further suggest that NIST employ a combination of language changes to this draft and craft one or more Special Publications resulting in a clear and unambiguous Standard.		NIST security requirements should be achievable; however, vendors typically do not desire that NIST specify the design to meet the requirement. NIST will produce a DTR. NIST will produce further documentation as needed.

tID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
90	J.C.	4.6	Sec. 4.6.1		In the first bulleted item in “Security Level 3” it is unclear if the immediate zeroization of CSPs requires an energy storage (battery) device. If it does, what action should be taken when the battery contains insufficient energy to perform the required zeroization?	James Cottrell- MITRE	**Rejected:** Implementation Guidance.
91	J.C.	4.6	Sec. 4.6.5.2		Are the environmental testing procedures to be run in series, only testing temperature outside of normal range and only testing voltages outside of normal range, or should the two be run in combination, vary voltage near lower and higher temperature limits? Should there be any tests that sufficient current is being supplied at the necessary voltage(s)?	James Cottrell- MITRE	**Rejected:** Implementation Guidance
107	W.L.	4.6			Comments submitted by Gore during the development of the FIPS 140-3 draft called for an additional level of security between the current level 3 and 4, based on the following: There is a very wide gap in physical security between Level 3 and Level 4. This gap is widened further by artificially restricting how a certification lab may test [attack] a module. The DTR’s prohibit them from using a drill to penetrate the module housing. This serves to dramatically dumb down the physical protection at Level 3. It also serves to disconnect Level 3 from any real threat scenario, since attackers don’t play by the DTR rules. Limiting tamper respondent solutions to covers and doors further dumbs down such protection. Level 4 physical security, originally thought to very challenging, has now been demonstrated to be quite straightforward, even routine at modest cost using commercial solutions. Applications exist that can benefit from physical protection beyond that of Level 3, but which may not be able to justify the cost of an overall Level 4 certification	W.L. Gore & Associates	**Rejected:**

108	W.L.	4.6			Physical volume protection solutions have been demonstrated which lack the sophisticated protection of Level 4 but would nevertheless provide much enhanced protection at Level 3. • Examples of such solutions can be found in USPS modules and PCI PIN entry devices. • Such protection costs just slightly more than current Level 3 solutions. As an alternative to hard potting, these newer, economical tamper respondent solutions are more manufacturing friendly.	W.L. Gore & Associates	**Rejected:** The standard does not preclude such implementations.
109	W.L.	4.6			We propose the establishment of an overall Level 3.5 in the FIPS 140-3 standard • Coordinate FIPS 140-3 and its companion documents to remove the artificial constraint against drilling into the module. • Provide language that allows a low-end tamper respondent solution that protects the entire module, not just covers and doors. • Dropping environmental sensing [in Level 4 language] could be considered. Where SECURITY LEVEL 4 calls out [in a couple places] “hard…coating…such that attempting to peel or pry…will have a high probability of resulting in serious damage to the module (i.e. the module will not function).” Gore requests that zeroization of CSP be considered as fulfilling the requirement that the module no longer functions, hence allowing tamper respondent solutions as an alternative to such hard coatings.	W.L. Gore & Associates	**Rejected:** Implementation Guidance
110	W.L.	4.6			We notice that the new Level 5 includes a physical security requirement “opaque to non-visual radiation examination”. We suspect this was intended to mean non-analysis by such examination. In any case, this has been a standard feature of Gore’s technology that already protects most current Level 4 modules. We suggest the wording be corrected to say “non-analysis” and that it be part of both Level 4 and 5.	W.L. Gore & Associates	**Accepted:**

116	W.L.	4.8	Sec 5.8		The following comment is a repeat from comments submitted previously by Gore. It relates to the FIPS 140-3 suite of documents, including the expected DTR revisions: • At Level 4 physical security, FIPS 140-2 requires that "a tamper detection envelope … shall detect tampering … to an extent sufficient for accessing … CSP's." • At Level 4 physical security, the FIPS 140-1 Implementation Guidance Section 5.8 still applies. It defines what constitutes a "breach in the barrier/enclosure of the module's tamper-detection envelope". The resolution states that the "module is considered breached and fails TE05.12.1 / TE05.22.02 if the testing laboratory…is able to penetrate the module's barrier/enclosure and gain undetected physical access to critical security parameters." The word "and" in the above sentence requires that the certification laboratory "is able" to do two things to fail the module: 1) undetected penetration, and 2) gain physical access to CSP's.	W.L. Gore & Associates	**Accepted:**
117	W.L.	4.8	Sec 5.8		The FIPS 140-2 DTR, Section AS05.41, appears less clear in its definition of a successful breach. While AS05.41 again establishes the context of undetected penetration sufficient to access CSP's, the associated "Required Test Procedures", TE05.41.01 refers to "any breach". It is possible to confuse the language of the FIPS 140-2 DTR, TE05.41.01 with the language of FIPS 140-2 and the FIPS 140-1 Implementation Guidance, Section 5.8.	W.L. Gore & Associates	**Accepted:**
118	W.L.	4.6			We propose a clarification of language:• All three documents must be synchronized in the language that defines a breach that would fail a module. • The language that a "laboratory…is able…to gain undetected access to critical security parameters" should be further clarified as having two necessary conditions:1. Physical penetration that is undetected by the tamper detection envelope2. Such undetected physical penetration must be useful to actually gain access to CSP's. We suggest that if required by NIST, the laboratory	W.L. Gore & Associates	**Rejected:** DTR or Implementation Guidance

					must be able to show how they would actually gain access to CSP's through the undetected physical penetration.		
119	W.L.	4.6			The following comments are repeated from our February 28, 2005 submission: • The language of FIPS 140-2 and its associated documents assumes and describes that a tamper detection envelope at Level 4 completely surrounds the module and incorporates tamper evidence if compromised. • The market requires Level 4 physical security via an enclosure that is reusable, or re-enterable, for performing warranty repair, chip upgrades, etc. without damage to the enclosure. It is assumed that zeroization would occur [by a switch or similar means], but the module could be re-closed and CSP's reloaded by an authorized technician. • Gore has solutions for reusable enclosures that should meet the intent of Level 4 physical security. FIPS 140-3 should specifically address and provide guidance for reusable enclosures. Opening the enclosure via the provided means should cause zeroization. Tamper evident tape over the opening of a reusable enclosure could provide the necessary tamper evidence.	W.L. Gore & Associates	**Rejected:** RE: Maintenance role
120-1	W.L.	4.6			Level 3 physical security provides for ventilation holes or slits, as long as at least one 90° bend is in the ventilation path. Clearly one could incorporate such a serpentine ventilation path and still meet the other requirements of Level 4. We propose that similar language for ventilation be added to Level 4.Other Clarifications. The distinction between standalone and embedded multiple-chip modules should be revisited and clarified, with more examples to better instruct the differences.	W.L. Gore & Associates	**Accepted:**
120-2	W.L.	4.6			·FIPS 140-2 layers the requirements of Levels 1-4. For example to meet Level 4 requires all Level 1, 2 and 3 requirements to be met. When this involves such things as hard potting materials or strong enclosures, certain useful configurations for Level 4 might be ruled out. Additional clarity is needed on exactly what is required at physical Level 3 and 4.	W.L. Gore & Associates	**Rejected:** Implementation Guidance

191	J.B.	4.6	4.6.1		The requirement in sec. 4.6.1 General Physical Security Requirements at security level 5 is problematic as there is no clear definition as to the parameters that may be considered to make a module opaque to non-visual radiation. So for example when blocking x-rays, the required density of the materials (which are often hazardous) is directly related to the 'strength' of x-ray beam. Likewise for thermal imaging the sensitivity of the equipment defines whether the module may be classed as opaque. Therefore is very difficult for a vendor to comply to this requirement as it is currently ill-defined. Thales e-Security feels that this requirement, although valuable in terms of the security, needs more definition. It is difficult to provide comments without understanding how a module can comply with this requirement.	Jason Bennet- -Thales e-Security	**Accepted:**
208	J.R.	4.6	4.6.3		Possible attacks against the cryptographic module include but are not limited to the catastrophic and sudden disabling of the tamper detection response circuitry or components. If the disabling method renders the response circuitry disabled such that CSPs are no longer protected from disclosure, this requirement is not met. If the disabling method renders the response circuitry disabled and either concurrently zeroizes the CSPs and PSPs or renders the CSPs and PSPs destroyed then this requirement is met. Comments: (note) Is "destroyed" an option in the other cases where zeroization is required? It would seem to make sense to either require zeroization everywhere or allow destruction everywhere as an alternative to zeroization.	James Randall RSA	**Accepted:**
209	J.R.	4.6	4.6.4		Possible attacks against the cryptographic module include but are not limited to the catastrophic and sudden disabling of the tamper detection response circuitry or components. If the disabling method renders the response circuitry disabled such that CSPs are no longer protected from disclosure, this requirement is not met. If the disabling method renders the response circuitry disabled and either concurrently zeroizes the CSPs or renders the CSPs destroyed this requirement is met.	James Randall RSA	**Accepted:**

					Comments: (notes) zeroization/destroyed - same comment as previous section.		
225	M.W.	4.6			"We would like to recommend that basic resistance against all types of side channel analysis be considered for Security Level 3 (Timing, SPA, DPA, SEMA, DEMA). Resistance against advanced differential and high-order techniques can be required for Level 4 and 5."	Marc Witteman (Amanda van der Berg) - Riscure	**Accepted:**
233	J.H.	4.6	Sec. 4.6.1		There appears to be a portion of the text missing in the Level 3 requirements. The place where text appears to be missing is indicated by red text. "If the cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in manner to prevent the gathering of information of the module's internal construction or components by direct visual observation using artificial light sources in the visual spectrum, then the module shall contain tamper response and zeroization circuitry."	Johnn Hsiung - for - SafeNety	**Accepted:** Will check comment submission to verify.
306	J.W.	4.6	4.6.1		In line 4 of the first bulleted paragraph, either change "then" to "and," or delete "then" and begin a new sentence as "Also, the module …" / There has already been one "then" to follow the initial "if." This makes for easier reading.	BAH/NSA I181 SETA	**Accepted:**
382	J.K.	4.6	4.6.5.2		"EFT shall involve a combination of analysis, simulation, and testing…" Analysis and simulation are not included in EFT but in EFP. Rewrite as follows: "EFT shall involve a testing…"	JCMVP20	**Accepted:**
463	J.W.	4.6	Sec. 4.6.1		In line 2 of the first bulleted paragraph, insert "a" between "in" and "manner" / self explanatory	BAH/NSA I181 SETA; Jay White, 410-684-6675	**Accepted:**
464	J.W.	4.6	Sec. 4.6.1		In line 4 of the first bulleted paragraph, either change "then" to "and," or delete "then" and begin a new sentence as "Also, the module …" / There has already been one "then" to follow the initial "if." This makes for easier reading.	Jay White, 410-684-6675	

489	S.K.	4.6			We understand that it is a very difficult and delicate task to map side channel attacks to each of five Security Levels in the draft FIPS140-3. The followings are the mapping employed in the draft: Level 1 and 2: no requirement Level 3: Timing Analysis Level 4: SPA and DPA Level 5: EME.	Shinichi Kawamura - TSRC	**Accepted:** 2nd Draft
490	S.K.	4.6			On the other hand, Level 1 is to achieve the lowest security and Level 5 is the highest. Therefore, the mapping above seems to assume the strength of side channel attacks increases in the following order: Timing Analysis, SPA/DPA, and then EME. Technically, however, it is not necessarily true that EME attack is stronger than Timing Analysis. Thus, the present mapping might potentially cause a conflict between security Levels and the security strength achieved, or at least mislead users to think that EME is the strongest side channel attack. In the joint comments with CRYPTREC (Cryptography Research and Evaluation Committees) separately submitted to NIST, we will propose a different mapping.	Shinichi Kawamura - TSRC	**Accepted:** 2nd Draft
492	S.K.	4.6			We think fault-based attack is important. It is worthwhile to check whether requirements in the draft FIPS140-3 will cover fault-based attack adequately (See also comment 6). Source: Tamper-resistance Standardization Research Committee (TSRC)*1 Chair: Prof. Tsutomu Matsumoto (tsutomu@ynu.ac.jp) Secretary: Dr. Shinichi Kawamura (shinichi2.kawamura@toshiba.co.jp)	Shinichi Kawamura - TSRC	**Accepted:** 2nd Draft
493	S.K.	4.6			Comment 5: We propose to add in the draft the notice that a side channel attack may become relatively easy to apply, depending on how Cryptographic boundary is defined.	Shinichi Kawamura - TSRC	**Accepted:** 2nd Draft
494	S.K.	4.6	Sec. 4.6.5		Comment 6: “EFP/EFT” in section 4.6.5 takes into account of temperature and voltage only. It is, however, well known that for a cryptographic module with external clock supply, there are attacks to manipulate clock signal from the normal operating range, e.g. to provide much faster clock signal for a short period of time, to cause faulty operation resulting in derivation of	Shinichi Kawamura - TSRC	**Accepted:** DTR and/or IG

					some secret parameters. Smart card is a typical cryptographic module with external clock supply. It should be required that cryptographic module shall detect or respond appropriately if a clock signal falls out of the normal range of operation.		
541	T.I.	4.6	Sec. 4.6 Phisical Security		What does the Radiation Fault Induction of Security Level 5 mean? Since the 3rd - description of Security Level 5 in the 4.6.1 is somewhat blurry and is necessary to specifically be described. (The same review process is necessary in the description of the 4.7 as well.)	Toru Ito - Cryptrec & INSTAC	**Accepted:** DTR – currently obsolete
542	T.I.	4.6	Sec. 4.6.1 General Physical Security Requirement		About the Maintenance Role: It is necessary to maintain consistency.	Toru Ito - Cryptrec & INSTAC	**Accepted:**
543	T.I.	4.6	Sec. 4.6.2 Single-Chip Cryptographic Modules		It seems that the Security Level 4 and 5 should be collectively presented. As with the FIPS140-2: In case there is such level which does not have additional requirements, it should be described “There are no additional requirements (for xxx) at Security Level X.” only when Low Level which consecutively follows from LV1 unless otherwise the concerned level should be described together with the additional requirements of the sub-levels.	Toru Ito - Cryptrec & INSTAC	**Accepted:**
544	T.I.	4.6	Sec. 4.6.5 Environmental Failure Protection/Testing		“EFP/EFT” in section 4.6.5 takes into account of temperature and voltage only. It is, however, well known that for a cryptographic module with external clock supply, there are attacks to manipulate clock signal from the normal operating range, e.g. to provide much faster clock signal for a short period of time, to cause faulty operation resulting in derivation of some secret parameters. Smart card is a typical cryptographic module with external clock supply. It should be required that cryptographic module shall detect or respond appropriately if a clock signal falls out of the normal range of operation. (It seems that the relevant description is 4.6.5; it should be added that “there is no description about the malfunction in conjunction with the instantaneous environmental anomaly” either in the current description of 4.6.5 or in	Toru Ito - Cryptrec & INSTAC	**Accepted:**

					the Other Attacks column of 4.11.)		
596-1	C.B.	4.6	Section 4.6.2		Single-Chip Cryptographic Modules. Security Level 2, 1st bullet states: "The cryptographic module shall be covered with a tamper-evident coating (eg., a tamper-evident passivation material or a tamper-evident material covering the passivation) or contained in a tamper-evident enclosure to deter direct observation, or manipulation of the module and to provide evidence of attempts to tamper with or remove the module." A) Can you please give an example of a tamper-evident material covering the passivation?	Chris Brych - DOMUS	**Rejected:** Implementation Guidance
596-2	C.B.	4.6	Section 4.6.2		B) Also, for semi-custom IC (FPGA, network controller) or Custom IC (encryption processor) cryptographic module that is meant to be embedded in a GPC or mobile computing device, it may not be possible to continuously view a module to see if it has been tampered with. Although the GPC may be compromised by an attacker assuming they have physical access to the computing device, the operator will not know that their cryptographic module residing on a GPC has been compromised as the module will be embedded within the GPC. This stated, I'm not sure how this requirement can be applied to a network processor or custom encryption IC cryptographic module and make sense from a security perspective. Will the CMVP make Federal users rip apart their PC's or notebooks to view if an IC has been tampered with? In many cases, this will void the warranty of a notebook.	Chris Brych - DOMUS	**Rejected:** Out-of-Scope

604	C.R.	4.6	Section 4.6.1, Security Level 2		Please consider the value of the physical security requirements for Federal agencies as they are written at Level 2. As the standard is currently drafted, "Security Level 2 requires the addition of tamper-evident mechanisms and the inability to gather information about the internal operations of the critical areas of the module (opaqueness)." We regard the current Level 2 opacity requirements as providing minimal protection. If an attacker wishes to gather information and formulate a plan of attack against a level 2 module they will just purchase a collection of them, tear them apart in their own lab and gain the direct knowledge that they would observe by peering through the ventilation holes of a deployed module. Cisco believes that the Level 2 requirements should be amended to state that the tamper evident labels are required but the concept of opacity should be removed. If this requirement is left in the new standard unchanged, please consider including an engineering specification to clearly specify the size of ventilation holes that are acceptable. Specifically to Security Level 3, the first sentence in the first bullet on page 30 of the standard gives the impression that not all the documented conditions apply to Level 3. We believe they should but suggest re-wording that first sentence to remove the use of the word "then".	Chris Romeo - Cisco	**Rejected:** Implementation Guidance
680	W.C.	4.6	Sec. 4.6		last bullet item "Multiple-chip standalone cryptographic modules": At the beginning of the last sentence "Examples of multiple-chip, standalone cryptographic modules", remove the comma. Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Accepted:**
836	IG	4.6	Sec. 4.6		How will the disclosure of PSPs compromise the security of the module?	Inforgard	**Accepted:**
837	IG	4.6	Sec. 4.6.1		Typically, detection circuitry necessary for non-visual radiation examination requires active power. Would this be a feasible requirement for single-chip devices? It is assumed that this is to be active at all times (main power on or not).	Inforgard	**Accepted:** deferred IG

838	IG	4.6	Sec. 4.6.2		Between Level 3 and 4, the same term “high probability” is used, which is not consistent with the summary.	Inforgard	**Accepted:**
895	CL	4.6	Sec. 4.6.1 & 4.8.6		“All CSPs (also, PSPs if Security Level 5) shall be zeroized when the maintenance access interface is accessed” Do encrypted CSPs need to be zeroized? Please clarify. In section 4.8.6 it states that below level 5 CSPs which are encrypted or stored in an embedded validated module, don’t need to be zeroized. A Note should be added acknowledging that zeroization at level 5 OR of a software or hybrid module will destroy required self-test keys and require the reinstallation or replacement of the module.	CEAL	**Accepted:**
921	CL	4.6	Sec. 4.6.5.1		“Immediately zeroize all CSPs and PSPs” Are PSPs required to be zeroized if a level 4 module chooses to implement EFP features?	CEAL	**Accepted:**
922	CL	4.6	Sec. 4.6.3 & 4.6.4		”Again, should this be the “SSPs”, or the “CSPs and PSPs”?	CEAL	**Accepted:**
923	CL	4.6	Sec. 4.6.3 & 4.6.4		“CSPs shall be protected from disclosure if the tamper detection response circuitry or components are disabled” Should this be the “SSPs”, or the “CSPs and PSPs”?	CEAL	**Accepted:**
924	CL	4.6	Sec. 4.6.3 & 4.6.4		“…protected with uniquely number tamper-evident seals” Could a more inclusive word be chosen? There are tamper evident mechanisms such as tamper evident screw covers which aren’t the stickers one normally thinks of as tamper seals, but which are effective at providing tamper evidence.	CEAL	**Accepted:**
925	CL	4.6	Sec. 4.6.2 & Section 4.6.3, and Section 4.6.4		Why is there no requirement that the removal or penetration of the epoxy have a “high probability of causing serious damage to the cryptographic module”?	CEAL	**Accepted:**

942	CL	4.6	Sec. 4.6.1		This bullet point appears to have been mangled in editing. The requirement appears to be for removable door and covers, but starts off discussing ventilation holes or slits.	CEAL	**Accepted:**
948	CL	4.6	Sec. 4.6.1 Section 4.6.1		"…prevent gathering of information about the internal operations of the critical areas of the module" Please define critical area. For hardware modules that are essentially off the shelf PCs in a custom enclosure, there are few critical areas. (One critical area would be any custom hardware that performs tamper detection for the module) Knowledge of the motherboard layout (often discoverable from the security policy) provides no useful information about the module's functionality, because that functionality is expressed in the software contained within the module.	CEAL	**Accepted:** deferred IG
957	CL	4.6	Sec. 4.6.5.2		Does the module pass, or fail, if it operates correctly without shutting down or disclosing CSPs (and PSPs at level 5) over the entire specified temperature range from -100 to +200 C?	CEAL	**Accepted:**
960	C.B.	4.6	Sec. 4.6.1		Please define "opaque" to thermal imaging. If the visible heat is non-uniform (where the hottest spot is likely to be at the CPU) does the module fail?	CEAL	**Accepted:**
1181	R.E.	4.6	4.6.1		Whenever zeroization is performed for physical security purposes, the zeroization shall occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time of detection and the actual zeroization.	Randy Easter - NIST	**Accepted:**
1190	R.E.	4.6			If the cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or obstruction with a substantial blocking material). Comments: Not defined. (substantial)	Randy Easter - NIST	**Accepted:**

841	IG	4.6	Sec. 4.5		Security Level 3, 1st bullet: There are disparate definitions (or examples) of 'passivation' layers between the glossary and Section 4.5.	Inforgard	**Accepted:**
259	R.E.	4.6	Sec. 1.3		In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the unauthorized access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts that provide Replace with : increase the difficulty of Comment: At Level 3, if a module does not have covers or doors, there is no requirement for the module to respond to a physical attempt to access CSPs. Suggest re-wording.	Randy Easter - NIST	**Accepted:**

tID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
4	J.C.	4.7	1. 2	GE	The definition of “Non-invasive attack” should be modified to include SPA, DPA and EME, since use of these techniques is not invasive to the module, but does require access or close proximity to the module or the power for the module. Recommend changing the definition to “**an attack that can be performed on a cryptographic module without direct physical contact with items within the Cryptographic boundary**”.	James Cottrell - Mitre	**Accepted.**
`216	M.W.	4.3, 4.7			*"As a specialised laboratory, we have limited involvement in formal evaluation schemes and our laboratory does not provide Common Criteria or FIPS evaluations. At the same time, we follow these standards with great interest and support their application. We further participate in security certification schemes of MasterCard (CAST, Mobile Payment Certification) and Visa (Mobile Payment Certification) and we are a member of the JIL Hardware Attacks Subgroup (JHAS) in Europe."* *Our feedback on FIPS 140-3 is centred around the proposed security classification. FIPS 140-3 specifies five security levels for cryptographic modules. We note the following aspects:* "Security Level 3 aims to offer resistance against attacks that require physical access to the module. Level 3 requires protection against timing analysis attacks and it mandates identity-based authentication mechanisms." "Security Level 4 increases security by requiring resistance against **power analysis attacks**. Further, Level 4 requires **two-factor authentication**." "Security level 5 is the highest level and amongst other things, it requires protection from electromagnetic emanation attacks." ***We would like to comment on two-factor authentication and side channel attacks.***	Marc Witteman (Amanda van der Berg) - Riscure	**No Action Necessary.**

					"Many smart card applications on the market do not require two-factor authentication. This would simply that Level 4 goes beyond the level supported by commonly used smart card applications for mobile communication, finance and conditional access. At the same time these smart card products are generally perceived and can be considered as highly secure devices that can safely operate in a hostile environment. **We would therefore like to recommend that the requirement for two-factor authentication be revisited. We propose to require this for the highest level only**." "Side channel analysis is a dangerous class of attack for cryptographic devices to which an attacker has physical access. **We therefore support that protection against side channel analysis has been introduced to the security levels of the FIPS 140 scheme**. However, we believe that the current division between Level 3, 4 and 5 is not the optimal representation of the threat that these techniques pose to cryptographic devices."		
9	P.T	4.7		GE	My basic question is therefore: Why did you not include EME attack resistance at Security Level 4? In the investigation that I'm participating in, we have been looking at the risks of both DPA and EME attacks on cryptographic processors, with particular relevance to smart cards. We were pointed at FIPS 140-3's draft as the reason why designers of chips and manufacturers of crypto devices (or at least those in the western hemisphere) want to be better protected from both DPA and EME attack, but I am doubtful about the effect of the July 2007 FIPS 140-3 on EME attack resistance. This is because you only include EME attack resistance at Security Level 5. The group for whom we are working are of the opinion that counter-measures against EM attacks are not as effective as counter-measures against DPA, and also that EME counter-measures are relatively easily by-passed. Then they believe that the activity in the underlying chip is more easily monitored using EM methods than using DPA methods.	Peter Tomlinson	**Accepted:** EME is included in levels 3, 4, and 5. See 2nd draft.

					I remember, while working on tests for the UK NatWest Bank Mondex e-money scheme during the early 1990s, being, with others, well aware that DPA was going to be possible (although someone else claims that he invented the concept). With the technology available then, EME attacks were going to be more difficult and thus DPA would come first, but I suspect that a better electronic engineer than me could now target a small area of a chip and record the activity there.		
10	CR	4.7	4.7	GE	Cryptography Research discovered Simple Power Analysis (SPA) and Differential Power Analysis (DPA) in the late 19901s, and continues to conduct leading research in the field of power analysis and other side channel attacks such as timing analysis.	Cryptography Research Inc.	**No Action Necessary.**
11	CR	4.7	Sec. 4.7	GE	The introduction of Section 4.7 'Physical Security - Non invasive Attacks' is an Ratcliffe, Steve appropriate that NIST recognizes the need to mandate the consideration of modem non-invasive attacks in validating cryptographic modules.	Cryptography Research Inc.	**No Action Necessary.**
12	CR	4.7	4.7	GE	We believe that the categories of attacks identified in Section 4.7 -Timing Analysis (TA), Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Electromagnetic Emanation (EMA) -are appropriate for FIPS 140-3. As with requirements in the FIPS 140 framework, specific testing procedures (and, indirectly, the required security capabilities) will be defined in the Derived Test Requirements (DTR).	Cryptography Research Inc.	**No Action Necessary.**
13	CR	4.7		GE	We believe that the requirement in the specification for product documentation to specify the mitigation techniques against the various non-invasive attacks is good. This description will greatly assist the laboratories in conducting their validation work and provide them valuable information to conduct efficient and focused testing of modules.	Cryptography Research Inc.	**No Action Necessary.**

14	CR	4.7		GE	Our recommendations for changes to the FIPS 140-3 draft are limited to requesting changes to the security levels at which resistance to power analysis attacks are required. These changes are important to make the security requirements match the objectives (and hence relying parties' assumptions) for each level. Our proposals for these changes are outlined below.	Cryptography Research Inc.	**No Action Necessary.**
15	CR	4.7			Comments on Protection against Simple Power Analysis (SPA) It is our opinion that mitigation of Simple Power Analysis (SPA) attacks should be required for devices with Level 2 tamper resistance, not level 4 as currently stated, for the following reasons:	Cryptography Research Inc.	**Rejected.** Level 2 provides physical tamper evidence, assumes unprepared attacker. Non-invasive attack requirements begin at Security Level 3.
16	CR	4.7			Devices validated to Level 2 are expected to provide some degree of tamper evidence. Devices which are vulnerable to SPA can be trivially broken without disrupting tamper-evident seals and other Level 2 security measures. As a result, protection against basic SPA attacks is required for the tamper evidence requirements to be meaningful. SPA attacks against devices which are unprotected are very easy to implement, and require only momentary external access to the module (e.g., to measure from either the power or ground input). 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. Power traces can be collected during normal device operation, so audit records or security sensors cannot mitigate the risk. The equipment for implementing SPA attacks is	Cryptography Research Inc.	**Rejected.** Level 2 provides physical tamper evidence, assumes unprepared attacker. Non-invasive attack requirements begin at Security Level 3.

					widely available. For example, the HP 54645D oscilloscope was used by Cryptography Research for several years as our primary oscilloscope for SPA and DPA analysis. The HP 54645D is now available cheaply. For example, one sold on eBay on Sept. 2, 2007 for $338 (http:llcgi.ebay.comlwsleBaylSAPl.dll?Viewltem&item=280147093421). The display capabilities of digital oscilloscopes such as the HP 54645D are sufficient for the analysis, so it is not necessary to have a personal computer or any other analysis hardware or software		
17	CR	4.7		GE	Appropriate mitigation of simple power analysis attacks is important for the long term credibility of FIPS 140. For example, because SPA is so simple to perform and does not require any detailed knowledge or documentation relating to the target module, it is now sometimes used as a class project for high school students and college undergraduates. SPA vulnerabilities in Level 2 devices are potentially newsworthy because such devices are expected to have some degree of tamper-evidence. Testing for basic SPA vulnerabilities can be done easily by FIPS testing labs. In particular, visual inspection of power traces using inexpensive equipment such as the HP 54645D can quickly identify basic SPA vulnerabilities.	Cryptography Research Inc.	**Rejected.** Level 2 provides physical tamper evidence, assumes unprepared attacker. Non-invasive attack requirements begin at Security Level 3.
18	CR	4.7		GE	Comments on Protection against Timing Attacks (TA) Mitigation of timing attacks is currently required at Level 3. Although a case could be made that such protection should be moved to Level 2, we believe that leaving the timing attack requirement at Level 3 is appropriate. These attacks are more complex than SPA so there is somewhat greater lab sophistication involved in testing for timing attacks than SPA. Mandating protection against timing attacks seems in line with other security requirements for Level 3.	Cryptography Research Inc.	**No Action Necessary.**

20	CR	4.7		GE	A few hundred power traces can be sufficient for a successful DPA attack if the device has poor leakage characteristics and does not employ countermeasures. We feel that such a level of protection is consistent with the expectation that Level 2 devices be tamper-evident, and is certainly needed for Level 3 devices which are expected to be tamper resistant. The techniques for performing DPA attacks are now widely known and have been widely researched. For example, knowledge of how to perform DPA is more widespread than for timing physical attacks or other attacks against cryptographic module Level 2: Protection against the simplest DPA attacks - low sample count (e.g. traces from <I000 operations, or other threshold below the maximum device utilization), analysis with standard partitioning and summation of signal sets only. Level 3: Protection against standard DPA attacks - moderate sample count (e.g. <50,000 traces), basic signal processing (trace alignment, data compression) Level 4: Protection against sophisticated and high order DPA attacks - high sample count (e.g. >100,000 traces, or other threshold corresponding to an exceptionally high device utilization rate), extensive signal processing, high-order analysis, chosen message attacks, and methods using advanced data acquisition and collection hardware.	Cryptography Research Inc.	**Rejected.** Level 2 provides physical tamper evidence, assumes unprepared attacker. Non-invasive attack requirements begin at Security Level 3.
021-1	CR	4.7		GE	These differing levels could be addressed in the DTR (see below), and would not necessarily require changes to the FIPS 140-3 requirements except to change the levels at which modules must mitigate DPA vulnerabilities.	Cryptography Research Inc.	**Accepted:** additional guidelines will be in Annex F and in the Derived Test Requirements (DTR).

021-2	CR	4.7		GE	Laboratory Training and Test Equipment for SPAIDPA Although many security testing laboratories have extensive experience with non-invasive and side channel testing, we are also aware that some FIPS 140 laboratories currently have less experience in this area. However, we also understand that the validations under FIPS 140 allow for components of the testing to be carried out by subcontractors, which we believe is an appropriate process for labs new to side channel techniques to gain experience in the area while still enabling them to conduct product evaluations.	Cryptography Research Inc.	**No Action Necessary.**
22	CR	4.7		GE	Cryptography Research would be pleased to support in the education and training of laboratories -- indeed we have already conducted training in SPA and DPA with some of the laboratories who are accredited to conduct FIPS evaluations. We also lead training courses in side channel analysis, which can range from a basic introduction to SPA and DPA, to an intensive hands-on training. These training courses typically run from 1-5 days, and we would be open to help design any additional training courses for FIPS laboratories that would be appropriate for FIPS 140- Remarks on Derived Test Requirements (DTR) We recognize that the DTR will need to provide sufficient detail and guidance to assist laboratories in testing devices against non-invasive attacks. CRI can provide assistance and recommendations in the development of these documents. We also sell test equipment for SPNDPA testing. At least two other organizations also offer such equipment. Accordingly the general availability of test equipment and training should make it straightforward for any labs with competent personnel to develop the ability to perform SPAIDPA validations.	Cryptography Research Inc.	**Out-of-scope.**
88	J.C.	4.7			Does the tamper-evident or potting material have to cover all interconnecting circuits between multi-chip modules?	James Cottrell- MITRE	Wrong section.

92	J.C.	4.7	Sec. 4.7		Should attacks using the branch prediction table, cache hit and page swapping be added to the list?	James Cottrell- MITRE	**Rejected:** However, all other attacks are covered in Section 4.11.
93	J.C.	4.7	Sec. 4.7		Isn't Simple Power Analysis a Timing based attack using current draw? If this is true, shouldn't SPA be required at Security Level 3?	James Cottrell- MITRE	**Accepted.**
198	J.H.	4.7	Introduction Section		Protection against Timing Analysis attacks – Must this be provided at all times for Level 3 and above or just be capable of? Some techniques for mitigating timing analysis attacks, like RSA blinding, impose a significant performance penalty that not everyone will want to incur for the sake of having a Level 3 validated module. Indication that the module is in Approved mode – Does this have to be constantly displayed? Could it be provided at start-up only?	Johnny Hsiung - for - SafeNet	**No Action Necessary.** Address in DTR.
234	J.H.	4.7	Sec. 4.7		For Level 4 protection against SPA and DPA, how is "mitigation technique" defined? Comments: It is clearly not possible to prevent an attacker making measurements of the power drawn by the module under various conditions. Would a design that ensures that power measurements can only be made of the module's overall power usage – i.e., including, memory reads and writes, I/O processing and non-sensitive CPU operations where the sensitive operations are performed in a separate ASIC - represent a "mitigation technique" in that access to the power measurements directly associated with the sensitive operations are not possible?	Johnny Hsiung - for - SafeNet	**No Action Necessary**. For Level 4, mitigation technique must: 1. Be described 2. Meet metrics in Annex F.
247	J.K.	4.7	Sec. 4.7		It is necessary to discuss which security levels are proper for TA, SPA, DPA and EME.	JCMVP21 Junichi Kondo	**Accepted.**
255	J.K.	4.7	4.7		Typo For Security Level 4 and 5 modules, describe does the module provides protection for the CSPs against SPA and DPA attacks. Rewrite as follows. For Security Level 4 and 5 modules, describe the module provides protection for the CSPs against SPA and DPA attacks.	JCMVP50 Junichi Kondo	**Accepted.** New text reads, "Documentation shall specify the mitigation techniques employed against these attacks and how these techniques mitigate access to the module's CSPs."

308	J.W.	4.7	Sec 4.7		Is: “These attacks include Simple Power Analysis, Differential Power Analysis, Electromagnetic Emanation and Timing Analysis.” "4.7 Physical Security – Non-Invasive Attacks Attacks on the operations of the module that are physical (not logical) in nature and do not require physical contact or direct observation of the module are specified in this section. These attacks include Simple Power Analysis, Differential Power Analysis, Electromagnetic Emanation and Timing Analysis. Other non-invasive attacks may exist but defence against them is currently considered optional at all Security Levels." Change to: “These attacks include Simple Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic Emanation (EME), and Timing Analysis (TA).”	BAH/NSA/I181	**Accepted.**
381	J.K.	4.7	4.7		Are the requirements for non-invasive attacks needed to apply to multi-chip embedded and multi-chip standalone cryptographic modules?	JCMVP22 Junichi Kondo	**No Action Necessary.** Answer isYes.
465	L.F.	4.7	Sec 4.7; Para 1		Is: “These attacks include Simple Power Analysis, Differential Power Analysis, Electromagnetic Emanation and Timing Analysis.” Change to: “These attacks include Simple Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic Emanation (EME), and Timing Analysis (TA).”	BAH/NSA/I181; Larry Fishman, 410-684-7803	**Accepted.** See above.
472	X.R.	4.7	Sec. 4.7		1. How does the testing Lab measure and evaluate if the IUT meets requirements in Section 4.7 regarding the four side channel attacks? What level of mitigation the IUT must have (for each of the four attacks), in order to pass the tests?	Corsec Security, Inc. Xiaoyu Ruan 10340 Democracy Lane, Ste. 201 Fairfax, Virginia 22030-2518 Phone: (703) 267-6050 ext 126 Cell: (571) 251-5020 Fax: (703) 267-6810	**No Action Necessary.** additional guidelines will be in Annex F and in the Derived Test Requirements (DTR).

481	P.G.	4.7	Sec. 4.7		1.The introduction of requirements on non-invasive attacks is appropriate given the current state of the art in attacking secure devices. 2.Side Channel Attacks can be difficult to protect against. Perfect countermeasures are sometimes not feasible, or even not possible. Due to this, requirements are usually stated with reference to a particular level of protection. The FIPS 140-3 categorization in levels provides the opportunity to make this type of layered requirements.	Brightsight bv Pascal van Gimst	**No Action Necessary.**
483	P.G.	4.7	Sec. 4.7		4.Differential Power Analysis (DPA) is a more sophisticated technique than SPA. However, for devices without proper countermeasures it is very powerful and therefore represents a very promising attack path. In addition to this, the technique is widely known and many publications are publicly available that describe improvements and adaptations. Implementation of certain countermeasures typically results in increased protection against DPA, but not in perfect resistance. The aim is usually to disrupt the attacker's business case, not to completely defeat the attack. Furthermore, countermeasures sometimes have an impact on performance, and a trade-off must be made. Due to this, we feel it is more appropriate to define multiple levels of DPA resistance, for example with the number of measurements required for a successful attack as the main parameter. For example, a distinction could be made in three levels: 'no', 'low', 'high', where the 'low' protection level requires a component to be resistance against DPA attacks with a maximum of 5000 measurements, and the 'high' level requiring protection up to 50000 measurements. In such a layered requirement, 'low' resistance would be required in FIPS 140-3 level 3, and 'high' resistance at level 4 and 5. The lower levels would not put requirements on the DPA resistance.	Brightsight bv Pascal van Gimst	**Accepted.** additional guidelines will be in Annex F and in the Derived Test Requirements (DTR).
484	P.G.	4.7	Sec. 4.7		5.The inclusion of resistance against timing attacks at level 3 is appropriate, since timing attacks are relatively sophisticated. It should be noted that, if a secure device is developed without consideration of timing attacks, it is very likely to be sensitive to them.	Brightsight bv Pascal van Gimst	**No Action Necessary.**

					Therefore, we feel the level 3 classification is appropriate, but should not be relaxed.		
487	S.K.	4.7	Sec. 4.7		We welcome that side channel security requirements are introduced in section 4.7. We take it mandatory to specify side channel security requirement for a cryptographic module.	Shinichi Kawamura - TSRC	**No Action Necessary.**
488	S.K.	4.7	Sec. 4.7		Description of side channel security requirement in section 4.7 is based on attack method, i.e. the requirement refers to the names of attack methods to be considered. In the comments we submitted in Feb 2005, we classified three types of description method for side channel security requirement as (1) attack-based, (2) countermeasure-based, and (3) metric-based. Since we think the metric-based description is an ideal approach, we hope that forthcoming documents such as DTR should describe the requirements in the metric-based manner when well-established metrics are ready.	Shinichi Kawamura - TSRC	**Accepted.** additional guidelines will be in Annex F and in the Derived Test Requirements (DTR).
545	T.I.	4.7	Sec. 4.7 Physical Security -Non-Invasive Attacks		Description of side channel security requirement in section 4.7 is based on attack method, i.e. the requirement refers to the names of attack methods to be considered. Description method for side channel security requirement is classified into three types as (1) attack-based, (2) countermeasure-based, and (3) metric-based. Since we think the metric-based description is an ideal approach, it is preferable that forthcoming documents such as DTR should describe the requirements in the metric-based manner when well-established metrics are ready.	Toru Ito - Cryptrec & INSTAC	**Accepted.** additional guidelines will be in Annex F and in the Derived Test Requirements (DTR).
626	P.G.	4.7			In reviewing the draft, it became apparent that our comments relate to section 4.7 'Physical Security – Non Invasive Attacks'. Our comments are rooted chiefly in our experience in performing such attacks, and observing the requirements imposed upon products in other evaluation schemes. They can be summarized as follows: 1.The introduction of requirements on non-invasive attacks is appropriate given the current state of the art in attacking secure devices.	Pascal van Gimst Pascal van Gimst Manager IC evaluations Brightsight Pascal van Gimst Manager IC evaluations Brightsight	**No Action Necessary.**

627	P.G.	4.7			2.Side Channel Attacks can be difficult to protect against. Perfect countermeasures are sometimes not feasible, or even not possible. Due to this, requirements are usually stated with reference to a particular level of protection. The FIPS 140-3 categorization in levels provides the opportunity to make this type of layered requirements.	Pascal van Gimst	**No Action Necessary.**
628	P.G.	4.7			3.Simple Power Analysis (SPA) is a very straightforward technique, which does not require much technological sophistication or complicated equipment. Since it is non-invasive, it can be considered more threatening than the type of physical attack that is thwarted by requiring devices to be tamper-evident, which in the FIPS 140-3 specification is a level 2 requirement. Given this, we feel SPA resistance should be a level 2 requirement, not level 4 as currently proposed.	Brightsight bv Pascal van Gimst	**Rejected.** Level 2 provides physical tamper evidence, assumes unprepared attacker. Non-invasive attack requirements begin at Security Level 3.
629	P.G.	4.7			4.Differential Power Analysis (DPA) is a more sophisticated technique than SPA. However, for devices without proper countermeasures it is very powerful and therefore represents a very promising attack path. In addition to this, the technique is widely known and many publications are publicly available that describe improvements and adaptations. Implementation of certain countermeasures typically results in increased protection against DPA, but not in perfect resistance. The aim is usually to disrupt the attacker's business case, not to completely defeat the attack. Furthermore, countermeasures sometimes have an impact on performance, and a trade-off must be made. Due to this, we feel it is more appropriate to define multiple levels of DPA resistance, for example with the number of measurements required for a successful attack as the main parameter. For example, a distinction could be made in three levels: 'no', 'low', 'high', where the 'low' protection level requires a component to be resistance against DPA attacks with a maximum of 5000 measurements, and the 'high' level requiring protection up to 50000 measurements. In such a layered requirement, 'low'	Pascal van Gimst	**Accepted.** additional guidelines will be in Annex F and in the Derived Test Requirements (DTR).

					resistance would be required in FIPS 140-3 level 3, and 'high' resistance at level 4 and 5. The lower levels would not put requirements on the DPA resistance.		
631	P.G.	4.7			Brightsight would be pleased to offer its knowledge and expertise on side channel attacks to the FIPS committee, or one of the accredited FIPS labs. Brightsight also offers a side channel analysis tool that has been developed, used and improved in house since 1998. Brightsight's security experts use this tool on a daily basis in their globally recognized security evaluations.	Pascal van Gimst	**Out-of-scope.**
682	W.C.	4.7	Sec. 4.7		Reorder "Simple Power Analysis, Differential Power Analysis, Electromagnetic Emanation and Timing Analysis" as "Timing Analysis, Simple Power Analysis, Differential Power Analysis, and Electromagnetic Emanation" because they are discussed in that order.	Wan-Teh Chang Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	**Rejected.** No longer necessary in second draft.
881	AT	4.7			•The opacity requirement adds no value to the standard. In today's world, an real attacker would simply purchase (or steal) a secondary unit and open the enclosure of the module. The concept of a "casual" attacker walking does not exist. •Generally speaking, for all of the more advanced physical attacks such as SPA, DPA, and EME, the CMVP must be able to define repeatable and consistent tests that all labs can execute consistently. If it cannot be tested consistently across all labs, then the requirements cannot be included.	Atlan	**Accepted.**
1199	R.E.	4.7	4.7		Attacks on the operations of the module that are physical (not logical) in nature and do not require physical contact or direct observation of the module are specified in this section. These attacks include Simple Power Analysis, Differential Power Analysis, Electromagnetic Emanation and Timing Analysis. Other non-invasive attacks may exist but defence against them is currently considered optional at all Security Levels.	Randy Easter - NIST	**No Action Necessary.**

19	CR	4.7		GE	Comments on Protection against Differential Power Analysis (DPA) Mitigation of DPA attacks is currently required at Level 4. It is our opinion that this requirement should be reduced to Level 3. Alternatively, we would also support a requirement that at Level 2 modules should address the simplest DPA attacks. DPA attacks are non-invasive and only require external power measurements recorded during normal device operation. As with SPA an unprotected device can be broken with minimal access to the device.	Cryptography Research Inc.	**Accepted** DPA at Level 3. **Rejected** DPA at Level 2. Level 2 provides physical tamper evidence, assumes unprepared attacker. Non-invasive attack requirements begin at Security Level 3.
23	CR	4.7		GE	Summary and Conclusions Cryptography Research welcomes the introduction of requirements for the mitigation of non-invasive attacks in the FIPS 140-3 specification. The addition of these requirements is an appropriate evolution of the specifications and is important for FIPS 140 to keep up-to-date with modem threats that cryptographic modules must address. We believe that defenses to classes of non-invasive attacks should be validated at lower security levels than currently proposed in the FIPS 140-3 draft. These attacks are relatively easy for malicious adversaries to perform, are widely known, and risk potentially devastating consequences if left unaddressed. We also recognize that the introduction of these new requirements into the specification may require some education and training for the testing laboratories. Cryptography Research currently offers such training, as do other technology vendors around the world. We would be pleased to work with NIST and the testing laboratories to help develop any additional training materials appropriate for FIPS 140-3. If you have any questions or would like to discuss any of the issues addressed in these comments, please contact us.	Cryptography Research Inc.	**No Action Necessary.** 2nd draft has SPA, DPA, EME, and TA at levels 3 and 4 - additional guidelines will be in Annex F and in the Derived Test Requirements (DTR).

					Paul Kocher President & Chief Scientist Benjamin Jun VP of Technology Josh Jaffe Research Scientist		
63	J.C.	4.7	Sec. 1.4		With the advances in Differential Power Analysis (DPA) demonstrated and documented by Cryptography Research Inc., http://www.cryptography.com/resources/whitepapers/DPA_Attacks.pdf, against AES in Counter Mode recommend that Simple Power Analysis (SPA) and DPA protections be required for cryptographic modules evaluated at Security Level 3 using AES in Counter Mode.	James Cottrell- MITRE	**Accepted.**

tID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
102	C.P.	4.8	Sec. 4.8.4		"Non- electronically transported PSPs…" Why do we need here the specification of "Non- electronically transported PSPs"?	Claudia Popa - CSE	**Rejected:** Do not see the harm ALR: We may need this.
116	W.L.	4.8	Sec 5.8		The following comment is a repeat from comments submitted previously by Gore. It relates to the FIPS 140-3 suite of documents, including the expected DTR revisions: • At Level 4 physical security, FIPS 140-2 requires that "a tamper detection envelope … shall detect tampering … to an extent sufficient for accessing … CSP's." • At Level 4 physical security, the FIPS 140-1 Implementation Guidance Section 5.8 still applies. It defines what constitutes a "breach in the barrier/enclosure of the module's tamper-detection envelope". The resolution states that the "module is considered breached and fails TE05.12.1 / TE05.22.02 if the testing laboratory…is able to penetrate the module's barrier/enclosure and gain undetected physical access to critical security parameters." The word "and" in the above sentence requires that the certification laboratory "is able" to do two things to fail the module: 1) undetected penetration, and 2) gain physical access to CSP's.	W.L. Gore & Associates	**Rejected:** The text reflects the author's intent ALR: It is not clear what text this applies to. It should apply to the Physical Security section.
117	W.L.	4.8	Sec 5.8		The FIPS 140-2 DTR, Section AS05.41, appears less clear in its definition of a successful breach. While AS05.41 again establishes the context of undetected penetration sufficient to access CSP's, the associated "Required Test Procedures", TE05.41.01 refers to "any breach". It is possible to confuse the language of the FIPS 140-2 DTR, TE05.41.01 with the language of FIPS 140-2 and the FIPS 140-1 Implementation Guidance, Section 5.8.	W.L. Gore & Associates	**Rejected:** Not a FIPS 140-3 issue. ALR: Same as the previous comment

192	J.B.	4.8	Sec. 4.8.6		In sec. 4.9 SSP Zeroization at security level 5 the requirement is stated that a method shall be provided to zeroize all PSPs. Performing this action will effectively make the module non-operational, as keys used for pre-operational tests on cryptographic algorithms are considered as PSPs and therefore the tests cannot be run. In addition it does not seem possible to securely return the unit to an operational state as PSPs are used for authentication of entities and external code loading. These methods are likely to be used for 're-activation' of a module. This requirement is particularly dangerous for modules which provide tamper protection through the use of potting. In these cases, the module cannot ever be returned to an operational state as direct access is prevented to the internal circuitry. Thales e-Security believes the requirement should be modified so that PSPs that are required to return the module to an operational state should not be required to be zeroized. In essence, this may be considered as returning the module to its factory default state before it is delivered to a customer i.e. only PSPs created by operation of the module in the field are required to be zeroized.	Jason Bennet- -Thales e-Security	**Probably obsolete**: new text says: "*CSPs 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)*" ALR: This is the intention. At Level 5 the module should not return to the operation status after the zeroization is performed.
210	J.R.	4.8	4.8		For a software module, the Software Integrity Test key is a CSP. For a hardware module that contains software components, the Software Integrity Test key is a PSP. For the hybrid module, the key used for the Software Integrity Test is a CSP. If another key is used to test the integrity of software in the hardware portion of the hybrid module, this key is not a SSP. Comments: (note) The software integrity test may not involve a key that is a CSP inside the module - in the case of a digital signature based system there is a PSP (the public key).	James Randall RSA	**Obsolete:** (statement was in 140-3 first draft, 4.8, but got removed in 2nd draft)

211	J.R	4.8	4.8.1		If entropy is provided from outside of the module then the claimed minimum entropy value shall be provided to the module. The module shall verify that the claimed minimum entropy provided by the RBG entropy source is sufficient to support the intended security strength of RBG that uses the entropy. Comments:(note) This requirement is somewhat strange in that a check that an external unvalidated assertion is inside a given range without an actual verification of the details (which is not feasible) adds little value beyond checking that the user can provide the right parameter at the same time as the entropy. If random values are required in an IV, used by an Approved security function(s), then an Approved RBG shall be used to generate this IV. Comments:(Insert)these values. (There are more contexts than "IV" in which RBG output is used - this statement shouldn't limit the requirement to just the "IV" usage).	James Randall RSA	**Obsolete:** "*The module shall verify that the claimed minimum entropy provided by the RBG entropy source is sufficient to support the intended security strength of RBG that uses the entropy*" has been removed in 2nd draft **Accepted:** recommend: "*If random values are required by an Approved security function(s), then an Approved RBG **shall** be used to generate these values.*"
213	J.R	4.8	4.8.6 SSP		A module shall provide methods to zeroize all CSPs (including temporarily stored values) within the module. Once a CSP is zeroized, the CSP shall not be retrievable from the module. 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 at levels below Security Level 5. Keys used only to perform pre-operational self-tests shall be considered as PSPs. Hash values of passwords that, if known, would be subject to an off-line exhaustion attack shall be considered as CSPs. RBG state information shall be considered a CSP. Comments:(Insert)exhaustion(ve (i.e. exhaustive)) attack	James Randall RSA	**Accepted:** replace "exhaustion" with "exhaustive" **Obsolete**: Text has been modified in FIPS 140-3 2nd draft. ALR Except for this change above, I would reject the comment. The standard should not talk about attacks.

236-1	J.H.	4.8	Sec. 4.8.1		The requirement: “If a module contains an RBG or an RBG entropy source in an Approved mode then: • RBG entropy sources shall be subject to the RBG Entropy Source Test as specified in Section 4.9.2. “ appears to contradict section 4.9.2, where it is specified as a test that is required for entropy sources contained within the operational environment only.	Johnn Hsiung - for - SafeNety	**Accepted:** text has been modified
236-2	J.H.	4.8	Sec. 4.8.1		The requirement statement: “If entropy is provided from outside of the module then the claimed minimum entropy value shall be provided to the module. The module shall verify that the claimed minimum entropy provided by the RBG entropy source is sufficient to support the intended security strength of RBG that uses the entropy.” is not clear. What does “claimed minimum entropy value shall be provided to the module” mean? Does it mean, for example, that the external source is responsible to provide a measurement of the minimum entropy as a parameter when it provides the random bits to the module’s internal RBG? If so, this would be imposing a FIPS 140-3 requirement on a component that is outside the module’s crypto boundary. How does the module verify that the claimed minimum entropy has actually been provided? Minimum entropy calculation is a statistical process and can’t reliably be done on the basis of a small number of bits (e.g., 128 or 256) being provided to the module. If it is just doing the verification on the basis of checking a number provided as a parameter by the external source, then, once again, a requirement is being levied on the external component to properly perform the calculation of minimum entropy.	Johnn Hsiung - for - SafeNety	**Accepted:** text has been modified. ALR: If entropy is provided from the outside then some information may be needed. This was out of scope in FIPS 140-2. **Obsolete:** Text removed in the 2nd draft

236-3	J.H.	4.8	Sec. 4.8.1		Why is the last sentence, i.e., “If random values are required in an IV, used by an Approved security function(s), then an Approved RBG shall be used to generate this IV.”, included in this section? It is not a requirement to be satisfied by an RBG, it is a requirement for the use of an RBG. It should perhaps be included in section 4.8.2.	Johnn Hsiung - for - SafeNety	**Accepted:** Statement should be moved
237		4.8	Sec. 4.8.2 - 4.8.3		The use of the term SSP in these sections seems inappropriate since the term includes Public Security Parameters as well as Critical Security Parameters and the topics addressed by these sections apply to CSPs only. In section 4.8.2, generation always applies to CSPs rather than PSPs. I would not categorize a public key component, produced as part of an asymmetric key pair generation, as a PSP. Section 4.8.3 talks about establishment techniques, which are applied exclusively to secret keys (CSPs)	Johnn Hsiung - for - SafeNety	**Rejected**: If one generates asymmetric keys, they are SSP (PSP + CSP).
238	J.H.	4.8	Sec. 4.8.4		“A module shall associate an SSP entered into or output from the module with the correct entity (i.e., person, group, role, or process) to which the SSP is assigned.” is impossible to meet as written. The module can maintain an association of SSPs with external entities (e.g., public key certificate A is associated with John Smith or AES Key B is associated with the data encryption application program) but it does not have the necessary information to determine whether the association is correct. The correctness of the associations must be determined by the using organization prior to providing the association information to the module.	Johnn Hsiung - for - SafeNety	**Accepted:** Remove “correct”. (4.8.4 – Third paragraph)
239	J.H.	4.8	Sec. 4.8.5		In the same way as for section 4.8.4, the module cannot determine or guarantee the correctness of the association between an entity and a stored SSP. See # 238	Johnn Hsiung – for SafeNety	**Accepted:** Remove “correct”. (4.8.5 – second sentence)

256	J.K.	4.8	4.8		Typo Provide a key table specifying the key type(s), strength(s) in bits, security function(s), security function certification number(s), where and how the key(s) is generated, whether the key(s) is imported or exported, any key establishment method used, indicate any related keys. Insert “and” before “indicate any related keys”.	JCMVP51 Junichi Kondo	**Accepted:** Insert “and” before “indicate any related keys”.
311	J.L.	4.8	4.8.5		Is there an upper limit on the number of SSPs stored in a module? I suggest including an upper bound (or guidance to determine one). The rationale is that in the event of a compromise, the size of the compromise would be limited.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Rejected:** The upper limit should be correlated with the module usage – different module might have different requirements. The standard specifies the zeroization requirements for different levels and categories. ALR: I agree with the rejection. The standard should not specify an upper limit.
374	J>K>	4.8	4.8.6		It is better to merge SECURITY LEVEL 3 and SECURITY LEVEL 4. Rewrite sentences for Security Levels 3 and 4 as follows. SECURITY LEVELS 3 AND 4 The cryptographic module shall control the zeroization of the CSPs.	JCMVP Junichi Kondo	**Obsolete:** Text has been already changed in the 2nd draft
376	J.K.	4.8	4.8.6		What does “the atmospheric destruction of a module during reentry” mean? Please rewrite more clearly.	JCMVP27	**Rejected:** It is an example applicable to a particular class of modules
377	J.K.	4.8	4.8.5		The word, “substitution”, is missing before the word, “when”. Rewrite as follows: “How PSPs are protected from unauthorized modification and substitution when stored within the module.”	JCMVP26 Junichi Kondo	**Obsolete:** Already corrected in the 2nd draft
378	J.K.	4.8	4.8.4		Maybe typo “the algorithms shall by Approved and meet or exceed the documented security strength of the module.” Rewrite “by” as “be”. “the algorithms shall be Approved and meet or	JCMVP25 Junichi Kondo	**Obsolete:** Already corrected in the 2nd draft

					exceed the documented security strength of the module.”		
379	J.K.	4.8	4.8.1		How does the module verify that the claimed minimum entropy is sufficient?	JCMVP24 Junichi Kondo	**Obsolete:** Text removed in the 2nd draft
380	J.K.	4.8	4.8		Wrong reference. Keys used only to test the cryptographic algorithms as specified in Section 4.9.2 are PSPs. There is no cryptographic algorithm specified in Section 4.9.2. Section 4.9.2 should be section 4.9.1.	JCMVP23 Junichi Kondo	**Obsolete:** Text modified in the 2nd draft.
399	D.W.	4.8	Sec. 4.8.6		Comments: The current guidance on Page 39, Section 4.8.6 on SSP Zeroization is not as detailed (or strongly worded) as it could be. For example, in the second paragraph under Section 4.8.6 there is a statement that requires documentation to specify the Critical Security Parameter (CSP) zeroization method(s), but there is no requirement (at any security level) that any specific methods be used. Suggest that acceptable methods of zeroization (such as multiple overwriting of memory) be specified in order to prevent the use of ineffective methods such as deleting a pointer to memory. 4.8.6 SSP Zeroization A module shall300 provide methods to zeroize all CSPs (including temporarily stored values) within the module. Once a CSP is zeroized, the CSP shall not301 be retrievable from the module. 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 at levels below Security Level 5. Keys used only to perform pre-operational self-tests shall302 be considered as PSPs. Hash values of passwords that, if known, would be subject to an off-line exhaustion attack shall303 be considered as CSPs. RBG state information shall304 be considered a CSP. Documentation shall305 specify the CSP zeroization method(s) employed by a module and the rationale as to why the method(s) prevent the retrieval and	Debby Waller- NSA	**Obsolete:** 2nd draft provides additional requirements.

					reuse the zeroized CSPs. Temporary CSPs (e.g., ephemeral keys) shall306 be zeroized when they are no longer in use. SECURITY LEVELS 1 AND 2 The zeroization of CSPs may be performed procedurally, and independent of the module's control. For example, the operator executes the destruction of the module (e.g., reformatting of a hard drive, the atmospheric destruction of a module during reentry). SECURITY LEVEL 3 The cryptographic module shall307 control the zeroization of the CSPs. SECURITY LEVEL 4 There are no additional requirements for Security Level 4. SECURITY LEVEL 5 The following security requirements shall308 be met: • A module shall309 provide methods to zeroize all PSPs (including temporarily stored values) within the module. • Documentation shall310 specify the PSP zeroization methods employed by a module and the rationale as to why the methods prevent the retrieval and reuse of the zeroized data. • Temporary PSPs shall311 be zeroized when they are no longer needed.		
401	D.W.	4.8	Sec. 4.8.6		During zeroization of data (e.g. SSPs), output from cryptographic modules with access to that data must be prohibited.	Debby Waller- NSA	**Rejected:** Text exists: "Once a CSP is zeroized, the CSP **shall not** be retrievable from the module. "
402	D.W.	4.8	Sec. 4.8.6		The cryptographic module should be designed so that the zeroization process can be successfully completed in the event that external power supplied to the cryptographic module is not present when zeroization is required and/or an externally supplied clock is not present when zeroization is required.	Debby Waller- NSA	**Rejected:** more information is necessary from the reviewer to justify it. ALR: Not clear.
403	D.W.	4.8	Sec. 4.8.6		In the event that there is a loss of both internal and external power to a cryptographic module, a passive zeroization capability shall be provided. To further clarify, the concern is that there is a window of time in which power must be present to achieve active zeroization. There will be instances in which internal and external power may be lost in such way that	Debby Waller- NSA	**Rejected:** more information is necessary from the reviewer to justify such a requirement for all security levels.

					there is insufficient time to actively zeroize, in which case a passive zeroization capability is required.		
404	D.W.	4.8	Sec. 4.8.6		Zeroization shall zeroize all CSPs in all locations with a single command or indication.	Debby Waller- NSA	**Rejected:** deferred to the IG. ALR: I like the way it is written in the draft now.
405	D.W.	4.8	Sec. 4.8.6		When external power is off and internal power drops low, CSPs shall be zeroized and the zeroization shall be checked and verified.	Debby Waller- NSA	**Rejected:** more information is necessary from the reviewer to justify it.
406	D.W.	4.8	Sec. 4.8.6		There shall be a key status indicator to indicate whether the module is keyed, not keyed, or zeroized.	Debby Waller- NSA	**Accepted:** Text added
409	D.W.	4.8			Although the FIPS PUB 140-3 provides guidance on entropy and testing for Random Bit Generation (RBG) data streams (in the section on conditional self-tests, for example), there are several additional requirements that address critical implementation issues that can affect the overall security of the random process. The following requirements address potential implementation concerns:	Debbie Wallner- NSA	-Comments follow below (next 3 rows) ALR: I believe this and the next three comments should be rejected as N/A.
410	D.W.	4.8			a) The logic which controls the input/output of random bits into/out of a cryptographic module and/or a cryptographic process implemented by that module (e.g., control gates, mod 2 adder, etc.) must be checked and/or alarmed.	Debby Waller- NSA	**Rejected:** more information is necessary from the reviewer to justify it.
411	D.W.	4.8			b) The clock rate of the source of random bits employed by a cryptographic module must be at least as fast as that of the cryptographic module, to preclude multiple sampling of the source.	Debby Waller- NSA	**Rejected:** more information is necessary from the reviewer to justify it.
412	D.W.	4.8			c) When required for use during the next call to the DRBG, the working state of a deterministic random bit generator implemented by a cryptographic module must be retained during quiescent states.	Debby Waller- NSA	**Rejected:** more information is necessary from the reviewer to justify it.

466	J.W.	4.8	Bullet 3		Change “shall by Approved” to “shall be Approved.” / self explanatory "• In order to prevent misuse of any SSP, a cryptographic module shall utilize a Trusted Channel for the input or output of all SSPs, whether or not cryptographically protected. If a Trusted Channel is established and maintained using the cryptographic algorithms, the algorithms shall by Approved and meet or exceed the documented security strength of the module."	BAH/NSA I181 SETA; Jay White, 410-684-6675	**Obsolete:** - Text already corrected in the 2nd draft
473	X.R.	4.8			For RBG, if seed is input from an external entropy source, then each time a seed is input to the module, the current min-entropy value (a float-type variable) must also be input to the module for comparison with the minimum min-entropy the RBG is expecting, is this correct?	Corsec Security, Inc. Xiaoyu Ruan	**Obsolete:** Text “*The module shall verify that the claimed minimum entropy provided by the RBG entropy source is sufficient to support the intended security strength of RBG that uses the entropy*.” has been removed from 2nd draft.
474	X.R.	4.8			For RBG, no matter the seed is obtained from an internal or external entropy source, a “min-entropy assessment” is required (inside or outside of the module) in order to compute the min-entropy. There are many models for assessing the min-entropy. Can you please specify assessment methods that are allowed to be used here?	Corsec Security, Inc. Xiaoyu Ruan	**Obsolete:** ALR: Should be rejected as Obsolete.
475	X.R.	4.8			For popular RBGs, such as FIPS 186-2 Appendix 3.1 with SHA-1, ANSI X9.31 Appendix A.2.4 with AES, ANSI X9.31 Appendix A.2.4 with 2-key TDES, and ANSI X9.31 Appendix A.2.4 with 3-key TDES, can you please let me know their minimum min-entropy values required for the seeding entropy pool?	Corsec Security, Inc. Xiaoyu Ruan	**Rejected:** Out of scope for the standard. IG/DTR issue
551	B.W.	4.8	Sec. 4.8.1		The following statement should be added to the requirements for entropy provided from outside the module: The value of the min-entropy shall be calculated using an approved method for assessing min-entropy.	Bridgete Walsh - CSE	**Rejected:** more information is necessary from the reviewer to justify it. ALR: Reject.
575	J.C.	4.8	Sec. 4.8.2		Use full terms and not acronyms in titles.	Jean Campbell - CSE	**Accepted**

576	J.C.	4.8	Sec. 4.8.6		A module shall provide methods to zeroize all CSPs (including temporarily stored values) within the module. Once a CSP is zeroized, the CSP shall not be retrievable from the module. 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 at levels below Security Level 5. Keys used only to perform pre-operational self-tests shall be considered as PSPs. Hash values of passwords that, if known, would be subject to an off-line exhaustion attack shall be considered as CSPs. RBG state information shall be considered a CSP. Comments: Should we introduce the concept of controlled zeroization?	Jean Campbell - CSE	**Resolved** by previous resolutions
597	C.B.	4.8	Section 4.8		Sensitive Security Parameter Management, 2nd last paragraph states: "For a software module, the software integrity test key is a CSP…… If this key is considered a CSP and it is zeroized, the module will no longer be able to check its integrity. This said, the module will have to be reinstalled. This not may make sense for mission critical Federal applications to support this feature. Also, if this key is considered a CSP, it must be encrypted. If it is encrypted, how can a module decrypt it as part of the initialization sequence without using some sort of cryptography which has not been tested as part of the POST. I think you must readdress this requirement.	Chris Brych - DOMUS	**Obsolete:** Text has been removed in the 2nd draft
605	C.R.	4.8	Section 4.8.1, Para 4		The current requirement states that "[i]f random values are required in an IV, used by an Approved security function(s), then an Approved RBG shall be used to generate this IV". However, according to Special Publication 800-38A, appendix C, none of the approved modes of operation require a random value for the IV (CBC and CFB require unpredictable values, but appendix C explicitly gives a method that does not involve any randomness). Please update the final version of the standard to be consistent with Special Publication 800-38A, Appendix C.	Chris Romeo - Cisco	**Reject:** SP 800-38A is a 2001 document. Also, SP 800-38D does require that an IV is random (at least as an option.) Besides, this is only an IF statement.

684	W.C.	4.8	Sec. 4.8		6th paragraph of the section "Keys used only to test the cryptographic algorithms as specified in Section 4.9.2 are PSPs.": Change "Section 4.9.2" to "Section 4.9.1".	Wan-Teh Chang	**Obsolete:** Text has been modified in the 2nd draft
686	W.C.	4.8	Sec. 4.8.1		3rd paragraph: Add a comma after "If entropy is provided from outside of the module". Page 37, 4th paragraph: In "used by an Approved security function(s)", remove "(s)". Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Accepted:** Text will be modified
687	W.C.	4.8	Sec. 4.8.2		2nd paragraph of the section: Please define "seeds" and "seed keys" and their differences. Member of the NSS Project http://www.mozilla.org/projects/security/pki/nss/	Wan-Teh Chang	**Accepted:** “seed key” already defined in the 2nd draft. “seed” will be added.
699	W.C.	4.8	Sec. 4.8.6		Consider removing "additional" from "an additional embedded validated module". Consider changing "exhaustion attack" to "dictionary attack".	Wan-Teh Chang	**Obsolete:** - Text has been modified in the 2nd draft However, the two terms are not identical:
772	IG	4.8	Sec. 4.8.4		The trusted channel requirement for CSP transport appears primarily in section 1 (see references below). The only treatment of this in section 4.8.4 SSP Entry and Output follows under the statement "If split knowledge procedures are used:", which separate from section 1 implies that the trusted channel requirement only applies to non-encrypted CSPs (those requiring split knowledge). In fact, reading section 4.8.4 (besides the split knowledge bullet items) reads as if CSP transport requirements are equivalent to 140-2. If the intent is to strengthen the requirement, specifics should be clarified in section 4.8.4.	InfoGard	**Rejected:** more information is necessary from the reviewer to justify it.
777	IG	4.8	Sec. 4.8.4		1. The trusted channel requirement for CSP transport appears primarily in section 1 (see references below). The only treatment of this in section 4.8.4 SSP Entry and Output follows under the statement "If split knowledge procedures are used:", which separate from section 1 implies that the trusted channel requirement only applies to non-encrypted CSPs (those requiring split knowledge). In fact, reading section 4.8.4 (besides the split	InfoGard Vendor	

					knowledge bullet items) reads as if CSP transport requirements are equivalent to 140-2. If the intent is to strengthen the requirement, specifics should be clarified in section 4.8.4. 2. If the trusted channel is transporting encrypted CSPs, does the channel still need to provide confidentiality?		**Rejected:** Out of scope of FIPS 140-3 review – an IG issue ALR: Reject, because by the nature of the Trusted Channel it should provide the confidentiality.
839	IG	4.8	Sec. 4.8.4		The first word and the last word of this sentence appears to contradict each other.	InfoGard	**Rejected:** Incomplete comment ALR: AI could not find a place in the draft to which this incomplete comment applies.
840	IG	4.8	Sec. 4.8.6:		The module should be responsible for providing the functionality to zeroize its secrets.	InfoGard	**Rejected:** Text reads now: "A module **shall** provide methods to zeroize all CSPs" More information is necessary from the reviewer to justify it.
843	IG	4.8	Sec. 4.8.1		Paragraph 3: Now that RBGs use 'entropy' instead of 'seed keys' there should be a statement that the value of entropy (as an actual sample from its source) shall be a CSP, and that the claimed minimum entropy value shall be a PSP. This ensures that they are covered in SSP entry/output.	InfoGard	**1st part – Accept.** Entropy is a CSP. **2nd part – Obsolete:** since the minimum entropy value is not transmitted electronically (per the latest draft).
844	IG	4.8	Sec. 4.8.2		It isn't clear that all SSPs would be random in nature, so it isn't clear that all SSPs should be generated using a RBG.	InfoGard	**Rejected:** more information is necessary from the reviewer.
845	IG	4.8	Sec. 4.8.3		This could be worded to be clearer.	InfoGard	**Rejected:** more information is necessary from the reviewer.
846	IG	4.8	Sec. 4.8.4		This assertion seems unnecessary. In the standard, for something to be 'encrypted' is must be encrypted with an approved security function.	InfoGard	**Rejected:** reviewer's incorrectly interprets the standard or more information is necessary from the reviewer.
847	IG	4.8	Sec. 4.8.4		The term "encrypted" should be replaced with "cryptographically protected".	InfoGard	**Accepted**
848	IG	4.8	Sec. 4.8.4		On the 6th paragraph, it should be clarified if the input and output to/from the module is referring to	InfoGard	**Rejected:** ALR: N/A

					the MSI interface or the physical boundary.		
849	IG	4.8	Sec. 4.8.4		the term "protected" should be replaced with "cryptographically protected".	InfoGard	**Accepted**
850	IG	4.8	Sec. 4.8.4		“Electronically transported CSPs shall be entered into and output from…”	InfoGard	**Rejected:** Incomplete comment
851	IG	4.8	Sec. 4.8.4		The third bullet does not relate to split knowledge and should be removed from this bulleted list.	InfoGard	**Accepted**.
852	IG	4.8	Sec. 4.8.4		This should be removed. It will just confuse vendors with the operator being authenticated and possibly thinking this means the keys don’t have to pass the manual key entry test. This is not clear: “Non-electronically… whether they are entered manually or electronically.” Should this be “Locally entered PSPs…”	InfoGard	**Rejected:** if clarification is required, the IG will provide it.
853	IG	4.8	Sec. 4.8.4		Split knowledge procedures, bullet 2: This seems like it would make more sense if the module ensured that no single operator could obtain enough key components to reconstruct the original key.	InfoGard	**Rejected:** The proposed text is equivalent to the original text.
854	IG	4.8	Sec. 4.8.5		The last sentence isn’t entirely clear. This should be changed to indicate that the embedded module must meet or exceed the security level of the module it is embedded in or provide metrics on how the requirements are applied to the embedded module relative to the larger module.	InfoGard	**Rejected:** N/A.
855	IG	4.8	Sec. 4.8.5		Should this be SSPs and not PSPs?	InfoGard	**Rejected:** Not an error.
856	IG	4.8	Sec. 4.8.5		RBG Entropy Source Test: Will the ‘min-entropy’ test be dictated in the standard or in the DTRs? How can this test be written such that all types of cryptographic modules can actually meet the requirement in some way?	InfoGard	**Rejected:** DTR issue
857	IG	4.8	Sec. 4.8.5		It is not reasonable to require that PSPs be zeroized at any level. For most modules, this will necessarily result in the destruction of the modules (note that known answer test keys are PSPs, as is the public key used for the software integrity test).	InfoGard	**Obsolete:** Level 5 has been removed in FIPS 140-3, 2nd draft.

858	IG	4.8	Sec. 4.8.6		We consider zeroization of PSPs overkill under certain circumstances, such as those typical in IBM HSMs. We agree that zeroization of PSPs increases security if the device can become operational after zeroization. In such a case, zeroizing PSPs ensures that, for example, administrator login status is removed when the device is tampered. However, PSPs still would not need to be protected from disclosure, therefore the requirement to zeroize them must be useful only to limit PSP lifecycle (to between zeroization events). We argue that a module that never regains operational status after zeroization does not gain security when zeroizing PSPs. In such a case, a PSP that survives zeroization may not be misused by the module, as it may never enter an operational state with PSPs persisting from before a tamper event. Under these restrictions (which are representative of all IBM HSMs), we would propose to remove the requirement on PSP zeroization.	InfoGard:.	**Obsolete:** Text has been modified in the 2nd draft.
859	IG	4.8	Sec. 4.8.4		While integrity-protection requirements on PSPs mirror those of CSPs (4.8.4), one may question the differentiation between electronically and non-electronically transported PSPs. While operational procedures may externally differentiate between the origin of PSPs (such as trusted CA certificates), modules themselves are probably unable to recognize the difference. In such a case, one could mandate authenticating all PSPs, or include a type indicator with the PSP (which itself need to be authenticated). Practically, as PSPs may be exported from the module, and queried, one could probably rely on such verification, and not mandate additional authentication of PSPs.	InfoGard	**Obsolete:** Text has been modified in the 2nd draft.

878	AT	4.8	Sec. 4.8.1		•The 2nd sentence in the 2nd paragraph "Non-Approved functions can be performed if they are not used to provide security relevant functionality…" seems to conflict with the Section 4.8.1 statement "All RBGs used in an Approved mode shall be Approved and listed in Annex A." oThe statement in Section 4.8.1 seems to be an absolute statement which prevents module from using a non-Approved RBG, regardless of what it's used for. oUnclear if this is intentional or not, but could lead to confusion to the use of non-Approved RBGs.	Atlan	**Obsolete** - Text has been modified in the 2nd draft.
879	AT	4.8			SSP Zeroization Replace the last sentence of the first paragraph with "Hash values of passwords that, if known, would be subject to an off-line exhaustion attack shall be considered as plaintext CSPs." Recommend that procedural zeroization may only be allowed for Level 1 modules. It's our opinion that this actually lowers the current level of assurance provided by Level 2 modules. Add the following Level 4 requirement, "For Security Levels 4, temporary key variables used within the module to process cryptographic algorithms must also meet key zeroization requirements above." Security Level 5 requirements. A requirement to zeroize PSP's is somewhat strange. Perhaps a better zeroization mechanism would be to zeroize the entire contents of flash including the module binary image.	Atlan	**Obsolete** - Text has been modified in the 2nd draft **Accepted** **Obsolete** - Text has been modified in the 2nd draft Security levels 2,3 and 4 : **"**Temporary SSPs **shall** be zeroized when they are no longer needed." **Obsolete:** The module will return to the factory state.

880	AT	4.8			•Section 4.8.1 – Random Bit Generators The second sentence states "the cryptographic module may be solely an RBG or an RBG entropy source." I believe the intent is to identify that one could have a module that only provides a single RBG service. This seems to be consistent with existing CMVP policy. However, the last portion of the sentence, "or and RBG entropy source." Does this mean that one could have a module that only supports a non-Approved RBG? The last requirement in this section states "If random values are required in an IV, used by an Approved security function(s), then an Approved RBG shall be used to generate this IV." Is this consistent with the various cryptographic algorithm standards. Do IV's truly need to be random?	Atlan	**The answer to the first question is "yes".** If the module is only used to generate entropy, one of the entropy-generating methods has to be Approved. **The answer to the 2nd question is "Obsolete",** the reference to an IV has been removed.
893	AT	4.8			•Section 4.8.5 – SSP Storage Last sentence in the first paragraph states "An SSP may also be stored within an embedded cryptographic module that meets or exceeds the requirements of the standard…" Is the CMVP trying to state that one cannot use a FIPS 140-1 or FIPS 140-2 embedded cryptographic module? If so, this would seem to contradict existing CMVP policy about allowing the use of existing validated modules.	Atlan	**Rejected:** The question is out of scope for the FIPS 140-3 – an IG and/or a programmatic issue.
919	CL	4.8	Sec. 4.8.1		"The cryptographic module may be solely an RBG or an RBG entropy source." If the cryptographic module is "solely [..] an RBG entropy source" then it doesn't appear to meet the minimum requirement that a module must contain at least 1 Approved security function.	CEAL	**Accepted:** If the module is only used to generate entropy, one of the entropy-generating methods has to be Approved.
920	CL	4.8	Sec. 4.8		"For a hardware module that contains software components, the Software Integrity Test key is a PSP. For the hybrid module, the key used for the Software Integrity Test is a CSP. If another key is used to test the integrity of software in the hardware portion of the hybrid module, this key is not a SSP." Should the software integrity key for the hardware half of a hybrid module be subjected to the same requirements as the software integrity key of a hardware module? If so, it is a PSP, rather that "not	CEAL	**Obsolete** - Text has been modified in the 2nd draft

					a SSP"?		
927	CL	4.8	Sec. 4.8.4		"During manual SSP entry, the entered values may be temporarily displayed to allow visual verification and to improve accuracy" If Passwords are CSPs and thus SSPs this seems to allow the password to be temporarily display when entered (presumably during a password change operation; since other requirements apply to password entry for authentication)	CEAL	**Rejected:** There are instances when the visual verification is needed – vendor's call (very long, hex format, etc)
928	CL	4.8	Sec. 4.8.4		Section 4.8.4 – Security Level 3, 4, and 5 "For Security Levels 3, 4, and 5, non-electronically transported CSPs shall be entered into or output from a module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext components.)" If Passwords are CSPs do they need to be entered (presumably during a password change operation) encrypted or using split knowledge?	CEAL	**Accepted.**
936	CL	4.8	Sec. 4.8.1 para 1		"Data output from the RBG shall pass the Continuous RBG Test as specified in Section 4.9.2." Shouldn't this be "Data output from each RBG shall"? This would avoid the implication that only one RBG needs the continuous RBG test.	CEAL	**Accepted.**
937	CL	4.8	Sec. 4.8.4		Manual vs. Electronic key entry is defined in this section, but Manual vs. Electronic key transport isn't.; even though requirements are applied to keys transported electronically.	CEAL	**Rejected:** Key *transport* is always electronic. There is a manual key *entry*.
938	CL	4.8	Sec. 4.8.4		The requirements don't explicitly state that each operator can only have or enter one component.	CEAL	**Rejected:** The draft says: "The module **shall** verify that no two operators entering or outputting key components have the same identities." – which means one operator can not have/enter more than one component of the split knowledge.
939	CL	4.8	4.8.4 Security Levels 1 and 2		No requirements are set (or inherited from the general requirements) for CSPs that are distributed manually for hardware or hybrid modules.	CEAL	**Rejected:** N/A. The text applies to all modules.

940	CL	4.8	Sec. 4.8.5		SSPs include CSPs, so this section should mention the requirement from Section 4.4 for modules which include software - at level 4 store CSPs encrypted and at level 5 store CSPs and PSPs encrypted.	CEAL	**Obsolete:** Text has been modified in the 2nd draft, section 4.4
946		4.8	Sec. 4.8.2		"Hash values of passwords that, if known, would be subject to an off-line exhaustion attack shall be considered as CSPs." The standard appears to be inconsistent about whether (or when) passwords or other authentication data (e.g. biometrics) are CSPs. If they are always CSPs, then they are subject to CSP zeroization requirements, and at level 4 and 5 subject to CSP encryption requirements.	CEAL	**Accepted:** Your statement is correct.
1001	D.W.	4.8	Sec. 4.8.6		The current guidance on Page 39, Section 4.8.6 on SSP Zeroization is not as detailed (or strongly worded) as it could be. For example, in the second paragraph under Section 4.8.6 there is a statement that requires documentation to specify the Critical Security Parameter (CSP) zeroization method(s), but there is no requirement (at any security level) that any specific methods be used. Suggest that acceptable methods of zeroization (such as multiple overwriting of memory) be specified in order to prevent the use of ineffective methods such as deleting a pointer to memory.	Debbie Wallner-NSA	**Rejected:** Duplicate entry
1093	D.W.	4.8	Sec. 4.8.6		Given the criticality of zeroization, especially of CSPs, the following (slightly modified/reworded) requirements seem appropriate for inclusion in the FIPS PUB 140-3 (in either the section on zeroization or the section on environmental failure protection), at least at some of the higher security level ratings:	Debbie Wallner-NSA	This and the next one is probably one comment.
1094	D.W.	4.8	Sec. 4.8.6		Superseded SSPs must be zeroized	Debbie Wallner-NSA	**Accepted.**
1135	D.W.	4.8	Sec. 4.8.4		third bullet under split knowledge procedures, typographical error: ".…….the algorithms shall by Approved and meet…..". Change "by" to "be".	Debbie Wallner-NSA	**Obsolete:** Text already modified

1201	R.E.	4.8	4.8.1		"If entropy is provided from outside of the module then the claimed minimum entropy value shall be provided to the module. The module shall verify that the claimed minimum entropy provided by the RBG entropy source is sufficient to support the intended security strength of RBG that uses the entropy."	Randy Easter - NIST	**Rejected:** no comment. However, text has been modified in the 2nd draft.
C01	CLP.	4.8	4.8.1		"Intermediate key generation values shall be considered a CSP." This shall become "Intermediate key generation values shall be considered CSPs."	Claudia Popa– CSEC	**Accepted**.
C02	CLP.	4.8	4.8.1		'deterministic components of an RBG shall be subject to the Cryptographic Test in Section 4.9.2" should become "deterministic components of an RBG shall be subject to the Conditional Cryptographic Algorithm Test in Section 4.9.2." ."	Claudia Popa– CSEC	**Accepted.**
C03	CLP.	4.8	4.8.1		"data output from the RBG shall pass the Continuous RBG Test as specified in Section 4.9.2." needs to be removed."	Claudia Popa– CSEC	**Accepted,** removed
C04	CLP.	4.8	4.8.1		"If an Approved security function(s), then an random values are required in an IV, used Approved RBG shall be used to generate this IV by." Is this a repeat for: "All RBGs used in an Approved mode shall be Approved or Allowed"?	Claudia Popa– CSEC	**Obsolete:** The reference to the IVs has been removed.
C05	CLP.	4.8	4.8.1		Add "as" to say "as listed in Annexes C and D."	Claudia Popa– CSEC	**Rejected:** Not needed. Annexes are providing a list not a method to follow so "as" is not needed in the sentence. "SSPs generated by the module for use by an Approved or Allowed security function **shall** be generated using an Approved or Allowed SSP generation

							method listed in Annexes C and D. “
C06	CLP.	4.8	4.8.1		an SSP establishment method in an Approved If mode requires random values as an input, Approved or Allowed RBG shall be used provide these values. Same as above, #4 above. Does the standard allow for non-approved in FIPS approved mode? If not, do we need to repeat?	Claudia Popa– CSEC	**Accepted.**
C07	CLP.	4.8	4.8.4		SECURITY LEVELS 3, 4, AND 5 CSPs shall be entered into or output from the module in encrypted form. PSPs may be entered into or output from a module in plaintext form. (a) The module shall utilize a separate, dedicated physical port for the input or output of unprotected CSPs, or a Trusted Channel shall be utilized to protect the CSPs entering and outputting the cryptographic module. If a Trusted Channel is used, the documentation shall specify the characteristics of the Trusted Channel First sentence (a) requires that the input and output of the CSPs to be done encrypted. Why do we need the second sentence (b), that deals to unprotected CSPs, if the requirement is to have the CSPs input/output in encrypted form? So we have (a) and then we have c) Non-electronically transported CSPs shall be entered into or output from a module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext components.) c) Why do we need c)? Is not enough to have (a) modified like: CSPs shall be entered into or output from the module in encrypted form or using split knowledge procedures (i.e., as two or more plaintext components.)	Claudia Popa– CSEC	**Obsolete.** The draft underwent substantial changes with respect to the definition and the use of the Trusted Channels.

C08	CLP.	4.8	4.8.4		The third bullet under the “if the split knowledge is used”	Claudia Popa– CSEC	**Accepted:** does not belong here

.

tID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
006-1	D.F.	4.9	Section 4.9.1		A cryptographic module shall permit operators to initiate the pre-operational tests on demand for periodic testing of the module. It is not clear how this requirement applies to software only crypto modules. Depending on the interpretation of the text, this could be interpreted as a requirement to allow operators to initiate pre-operational tests for every instance of a crypto module running within in the system. “The pre-operational tests shall be performed by a cryptographic module between the time a cryptographic module is powered on, either from a power-off state or a quiescent state (e.g., low power, suspend or hibernate) and the time that the cryptographic module uses a function or provides a service using the function to be tested.” Newer portable devices and operating systems are being very aggressive about entering power-conserving states. In some cases (such as mobile or embedded devices) this might boil down to a self-test before every operation. At a minimum, this needs a much more restrictive definition of quiescent states. Retesting when coming out of hibernate may be justifiable from a security perspective, but doing it when resuming from sleep seems like overkill. This requirement will likely require significant re-engineering for software only crypto modules. The draft should provide a set of security threats this requirement was designed to mitigate to help justify the engineering investments. Windows may suspend or hibernate during a cryptographic operation. It may be very difficult to temporarily stop cryptographic operations to perform self-tests when the computer powers up again. Moreover, this requirement will result all cryptographic process to re-run self-tests at the same time. It will be difficult to justify the performance degradation to a majority of Windows users who do not need FIPS certified crypto. Windows notifies applications when the machine	David Friant - Microsoft	**Accepted: Text has been modified**

					resumes from low power, suspend, or hibernate states by broadcasting the **WM_POWERBROADCAST** message to all applications with visible windows. The current mechanism is not appropriate for applications such as command line tools or background services that do not have visible windows. **Microsoft needs to perform a more thorough study to determine if there is an appropriate mechanism to communicate power events to crypto modules that are loaded into the application's process.**		
006-2	D.F.	4.9	Section 4.9.1		"The vendor shall specify a critical time period that specifies the maximum operational time before pre-operational tests must be repeated." A periodic self-test requirement adds a lot of complexity to crypto modules, especially for those that run in kernel mode. Moreover, running periodic self-tests may have an unpredictable side effect on real-time scenarios such as media playback. The draft did not specify a maximum requirement, other than documenting a maximum time between tests.	David Friant - Microsoft	**Accepted: Text has been modified**
006-3	D.F.	4.9	Section 4.9.1		"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" A continuous test is incompatible with pre-operational testing. If a module chooses this option, when should they consider the pre-operational test complete? Perhaps this should be in a different section.	David Friant - Microsoft	**Accepted: Text has been modified**

006-4	D.F.	4.5	Section 4.9.1		"The operating system shall prevent operators and external executing processes from reading cryptographic software stored within the cryptographic boundary." What does this requirement mean? What operational property is it intended to insure? Windows binary code is not a secret. Executable files that contain the crypto code are readable by the user. The code of a DLL in user space is readable by any thread in that process. Depending on how the various terms are interpreted this could be an impossible requirement to meet. Depending on what this requirement actually means an appropriate HSM should be used to provide implementation secrecy.	David Friant - Microsoft	**Requirement removed.**
7	D.F.	4.9	4.9.2 Under RBG Entropy Source Test:	GE	"If each call to a RBG produces blocks of n bits (where n > 63), the first n-bit block generated after power-up, initialization, or reset shall not be used, but shall be saved for comparison with the next n-bit block to be generated. Each subsequent generation of an n-bit block shall be compared with the previously generated block. The test shall fail if any two compared n-bit blocks are equal. If each call to a RBG produces fewer than 64 bits, the first n bits generated after power-up, initialization, or reset (for some n > 63) shall not be used, but shall be saved for comparison with the next n generated bits. Each subsequent generation of n bits shall be compared with the previously generated n bits. The test fails if any two compared n-bit sequences are equal." This requirement doesn't work well with SP800-90 since AES counter mode generates variable length output and there is no guarantee the second call will generate the same number of bits.	David Friant Microsoft, Redmond, WA.	**Requirement removed.**

42	J.R.	4.9	4.9.1		The pre-operational tests shall be performed by a cryptographic module between the time a cryptographic module is powered on, either from a power-off state or a quiescent state (e.g., low power, suspend or hibernate) and the time that the cryptographic module uses a function or provides a service using the function to be tested. Prior to using a security function, the pre-operational test(s) of that security function shall pass successfully. The pre-operational self-tests shall be initiated automatically and shall not require operator intervention. The vendor shall specify a critical time period that specifies the maximum operational time before pre-operational tests must be repeated. When a pre-operational test is completed, the results (i.e., indications of success or failure) may be output via the “status output” interface. 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. Comments:(note) Do any existing modules handle this requirement? The wording should be "should be repeated" rather than "must" unless there is a requirement for a technical measure to enforce this to be inside the module.	James Randall RSA	**Accepted: Text has been modified**
47	J.R.	4.9	4.9.2		If each call to a RBG produces fewer than 64 bits, the first n bits generated after power-up, initialization, or reset (for some n > 63) shall not be used, but shall be saved for comparison with the next n generated bits. Each subsequent generation of n bits shall be compared with the previously generated n bits. The test fails if any two compared n-bit sequences are equal. Comments:(Insert)shall fail (use the same wording as the previous paragraph)	James Randall RSA	**Requirement removed**

48	J.R.	4.9	4.9.2		If the keys are used to perform key agreement, then the arithmetic validity of the keys shall be tested by verifying the correct mathematical relationship between the public key and private key values. Comments: (note) It would make more sense to explicitly state that key agreement itself shall be performed and verified. The previous two steps are performing the desired operation - this one should also be the same. "arithmetic validity" could equally be applied to the previous two cases - but direct statement that performing the desired operation and confirming that it works is the requirement would be clearer.	James Randall RSA	**Accepted: Text has been modified**
49	J.R.	4.9	491		perform a KAT for each cryptographic algorithm and mode to be tested in accordance with the specified condition. A KAT is not required for the security function in the Approved Data Authentication technique used by the Software Integrity Test. Comments: (Strikeout) That the IGs allow for the Software Integrity Test to operate as a KAT is something which could reasonably be changed so that all algorithms go through the same requirements in this area.	Janes Randall RSA	**Accepted: Text has been modified**
85	J.C.	4.9	Sec. 4.4		The first bulleted item under “Security Level 3” requires that a “cryptographic officer” role be required to execute a Software Integrity Test. Paragraph 4.3.3 “Perform Self-Test” requires that the module “Initiate and run pre-operational self-tests” when commanded. Paragraph 4.9.1 requires that the Software Integrity Test is one of these “pre-operational self tests” performed before a cryptographic module is ready to operate? From the requirement in 4.9.1 it would appear that limiting running a Software Integrity Test to “cryptographic officer” may be too restrictive.	James Cottrell- MITRE	**Accepted: Text has been modified**
94	J.C.	4.9	Sec. 4.9		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-	James Cottrell- MITRE	**Accepted: Text has been modified**

					test failure). These two paragraphs appear to contradict each other.		
95	J.C.	4.9	Sec. 4.9.1		Acronyms DSA and ECDSA are used on not defined.	James Cottrell- MITRE	**Obsolete**
103	C.P.	4.9	Sec. 4.9.2		Manual Key Entry Test If cryptographic keys or key components are manually entered into a cryptographic module, or if error on the part of the human operator could result in the incorrect entry of the intended key, then the following manual key entry tests shall be performed:… " Continuous RBG Test, page 42 "If each call to a RBG produces fewer than 64 bits, the first n bits generated after power-up, initialization, or reset (for some n>63) shall not be used… Do we need this part of the sentence: "or if error on the part of the human operator could result in the incorrect entry of the intended key"? What do we try to clarify with (for some n > 63)?	Claudia Popa - CSE	**Accepted: RBG requirements have been removed, the rest of the text remains.**
105	C.P.	4.9	4.9.2		Non clear for me what is considered a pre-operational self- test or a conditional self-test. The first paragraph mentions: "The pre-operational self-tests must be performed and passed successfully prior to the module providing any services. Conditional self-tests shall be performed when an applicable security function is invoked". and later in 4.9.1 there is this statement "Prior to using a security function, the pre-operational test(s) of that security function shall pass successfully." So the same test, for a security function, will be performed as part of the pre-operational testing and also each time a security function is called? Is this the intention?	Claudia Popa - CSE	**Accepted: Text has been modified**
160	J.R.	4.9	4.9.1		If a cryptographic module includes two)insert(independent implementations of the same cryptographic algorithm, then the module shall:	James Randall RSA	**Rejected:**

					Comments: (Insert) or more		
181	D.F.	4.9	Sec 4.9.1		A cryptographic module shall permit operators to initiate the pre-operational tests on demand for periodic testing of the module. It is not clear how this requirement applies to software only crypto modules. Depending on the interpretation of the text, this could be interpreted as a requirement to allow operators to initiate pre-operational tests for every instance of a crypto module running within in the system. Proposed Disposition: No change required. The module shall permit each operator to initiate the pre-operational tests. The tests do not have to be run for each instance of the operator.	David Friant Microsoft, Redmond, WA.	**Accepted: Text has been modified**
182	D.F.	4.9	Sec 4.9.1		The pre-operational tests shall be performed by a cryptographic module between the time a cryptographic module is powered on, either from a power-off state or a quiescent state (e.g., low power, suspend or hibernate) and the time that the cryptographic module uses a function or provides a service using the function to be tested. Newer portable devices and operating systems are being very aggressive about entering power-conserving states. In some cases (such as mobile or embedded devices) this might boil down to a self-test before every operation. At a minimum, this needs a much more restrictive definition of quiescent states. Retesting when coming out of hibernate may be justifiable from a security perspective, but doing it when resuming from sleep seems like overkill.	David Friant Microsoft, Redmond, WA.	**Accepted: Text has been modified**
193	J.B.	4.9	Sec. 4.9.1		The requirement in sec. 4.9.1 Pre-Operational Self-tests for automatically running the pre-operational tests at a time specified in the documentation does not take into account modules that are used in environments where non-operational time is considered a critical issue, as it is implied in paragraph three that running the tests will cause “interruption of the module’s operation”. Where it is unacceptable to interrupt the module’s operation, self	Jason Bennet- -Thales e-Security	**Accepted: Text has been modified**

					tests may be designed such that the pre-operational self-tests required can be run without the module's operation being interrupted. Due to these constraints Thales e-Security believes that the requirement for preoperational self-tests at a defined and fixed time period should be clarified to indicate that this does not mean that the unit's operation will have to be interrupted.		
197	J.F.	4.9	Sec. 4.9.1		"In addition to performing the pre-operational tests when powered up or at some point before a particular cryptographic algorithm or function is used, a cryptographic module shall permit operators to initiate the tests on demand for periodic testing of the module. Does "In addition" preclude labs from saying that the operator hitting the power up or reset button would test the module? I have seen this in a few reports and this seems acceptable however I think this clearly states an additional command to perform the periodic testing should be incorporated.	Jim Fox - NIST	**Accepted: Text has been modified**
202	J.R.	4.9	4.9.1		Public key cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the DSA or the ECDSA) shall be tested using a known-answer test if the random number responsible for the variability of the output can be fixed, or shall be tested using a Pair-Wise Consistency Test (see Section 4.9.2) with a fixed pair of public and private keys. Comments:(note) This requirement does clash with other statements about RBG usage - and those statements should make it clear that in pre-operational tests it is allowed for the RBG to be substituted for a fixed stream. Appropriate mechanisms need to be in place to ensure that this fixed stream is not used outside of this context,	James Randall RSA	**Accepted: Text has been modified**

203	J.R.	4.9	4.9		A cryptographic module shall perform pre-operational self-tests, conditional self-tests and, if applicable, critical functions tests to ensure that the module is functioning properly. The pre-operational self-tests must be performed and passed successfully prior to the module providing any services. Conditional self-tests shall be performed when an applicable security function is invoked (i.e., security functions for which self-tests are required). A cryptographic module may perform other tests in addition to the tests specified in this standard. Comments: (note) It needs to be clearer that only services which use an algorithm require that the algorithms self tests have passed before providing services as the "any services" wording precludes other described operational behaviour. See section 4.1.4 for "degraded mode of operation" and section 4.9.1. Self-tests for an algorithm should be able to be explicitly delayed until the algorithm is first used.	James Randall RSA	**Accepted: Text has been modified**
240	J.H.	4.9	Sec. 4.9		The statements: “The cryptographic module shall not utilize any functionality that relies upon a function or algorithm that failed a self-test until the relevant self-test has been repeated and successfully passed.” and “Prior to using a security function, the pre-operational test(s) of that security function shall pass successfully.”, from section 4.9.1 indicate that only functions for which the self-test fails must be prohibited until the self-test passes. But the statements: “The pre-operational self-tests must be performed and passed successfully prior to the module providing any services.” and “The cryptographic module shall not perform any cryptographic operations or output data via the data output interface while in an error state.” indicate that no services can proceed if any self-test fails. Which overall requirement statement is correct – services for which a self-test fails cannot be provided or no services can be provided if any self-test fails?	Johnn Hsiung - for - SafeNety	**Accepted: Text has been modified**

242-1	J.H.	4.9	Sec. 4.9.2		For “Pair-Wise Consistency Test”, if pair-wise consistency checking is used as a technique in an intermediate step in the key pair search algorithm and is also applied to the final candidate key pair, must each of the failures at the intermediate steps be reported or is it sufficient to report an error if the final candidate fails the test? The second paragraph of section 4.9 says that the module must enter an error state and output an error indicator if any self-test fails. While this makes sense in the context of the self-tests being applied when success is expected and a failure represents that something is actually not performing correctly, it does not make sense when applying one of the self-test techniques during an intermediate step in a key pair search algorithm where the occasional failure is expected due to the probabilistic nature of the search algorithm and actually represents correct operation of the algorithm.	Johnn Hsiung - for - SafeNety	**Accepted: Text has been modified**
242-2	J.H.	4.9	Sec. 4.9.2		For “Software Load Test”, the first bullet says. “An approved digital signature technique …” and the second bullet says, “ The applied Approved data authentication technique …”. Is there a reason for the different wording from one bullet to another?	Johnn Hsiung - for - SafeNety	**Accepted: Text has been modified**
242-3	J.H.	4.9	Sec. 4.9.2		The third bullet of Software Load Test says, “ Before the newly loaded software is operationally used, the requirements of section 4.9.1 shall be satisfied.” Does this mean that the software has to be verified again using the Software Integrity Test when it has just been verified as part of the Software Load Test? This seems redundant.	Johnn Hsiung - for - SafeNety	**Accepted: Text has been modified**
242-4	J.H.	4.9	Sec. 4.9.2		For “RBG Entropy Source Test”: a. “If an RNG …” should read “If an RBG …” b. Referring to comment 1 on section 4.8.1, does this test apply only to the use entropy sources external to the module? c. I could not find a description of “min-entropy assessment”. There is a definition of “min-entropy” but that doesn’t give any information regarding, for example, what is a reasonable sample size to use or what word length to use in calculating the min-entropy (you might get a result of 2bits per 4-bit word & 5 bits per word for an 8-bit word using the same	Johnn Hsiung - for - SafeNety	**Requirement removed.**

					sample). d. The wording indicates that the min-entropy assessment has to be performed on each output of the entropy source. This is not a reasonable requirement since the entropy source might, for example, be providing 64 bits in each output and that is clearly not a sufficient sample size on which to base a calculation of the min-entropy.		
246	J.K.	4.9	4.9.2		It is impossible to perform the min-entropy assessment in conditional self-tests. Delete the requirements of RBG Entropy Source Test.	JCMVP32	**Requirement removed.**
312	R.A.	4.9	4.9 par 2		This information would also be useful in a users manual or a user's guide "If a cryptographic module fails a self-test, the module shall enter an error state and shall output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations or output data via the data output interface while in an error state. The cryptographic module shall not utilize any functionality that relies upon a function or algorithm that failed a self-test until the relevant self-test has been repeated and successfully passed."	NSA/SETA/ SPARTA Rowland Albert, 410-865-7992	**Accepted: Text has been modified**
313	J.W.	4.9	4.9.1		Reword the paragraph as: “Cryptographic Algorithm Test. This test shall be conducted for every implementation of all Approved and Allowed cryptographic algorithms (e.g., encryption, decryption, data authentication and random it generation) by a cryptographic module via any of the following methods.” / This emphasizes the fact that it is the software implementation that is being tested, and not the algorithm.	NSA/SETA/ SPARTABAH/NSA I181 SETA Jay White, 410-684-6675	**Accepted: Text has been modified**
315-1	J.L.	4.9	4.9.2		Continuous RBG test - I suggest adding NIST SPUB 800-22 to describe NIST approved methods to test RBGs. Needed for clarity, completeness and to ensure security.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Accepted: Text has been modified**

315-2	J.L.	4.9	4.9.2		"4.9.2 Conditional Self-Tests Conditional tests shall be performed by a cryptographic module when the conditions specified for the following tests occur: Pair-Wise Consistency Test, Software Load Test, Manual Key Entry Test, Continuous RBG Test, RBG Entropy Source Test, and Conditional Bypass Test. Pair-Wise Consistency Test (for public and private keys). If a cryptographic module generates public or private keys, then the following pair-wise consistency tests for every pair of generated public and private keys shall be performed: • If the keys are used to perform key transport, then the public key shall encrypt a plaintext value. The resulting ciphertext value shall be compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key shall be used to decrypt the ciphertext and the resulting value shall be compared to the original plaintext value. If the two values are not equal, the test shall fail."	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Incomplete comment**
371	J.K.	4.9	4.9.2		Replace “Approved data authentication technique” with “Approved digital signature technique” Rewrite as follows: The applied Approved digital signature technique shall be successfully verified otherwise the Software Load Test shall fail.	JCMVP31	**Accepted: Text has been modified**
372	J.K.	4.9	4.9.1		In multi-thread software modules, the data output from each thread is disabled when a thread is performing a pre-operational self-test. However how do the other threads know that a pre-operational self-test begins in the different thread and disable output?	JCMVP30 Junichi Kondo	**Accepted: Text has been modified**
375	J.K.	4.9	4.9		Replace “must” with “shall”. “The pre-operational self-tests shall be performed and passed successfully prior to the module providing any services.”	JCMVP29 Junichi Kondo	**Accepted: Text has been modified**

425		4.9			“The vendor shall specify a critical time period that specifies the maximum operational time before pre-operational tests must be repeated.” The draft did not specify a maximum requirement, other than documenting a maximum time between tests. Proposed Disposition: It is already a requirement that pre-operational tests be done automatically at power-up and that the operator shall be able to initiate pre-operational tests upon demand. Therefore the requirement for the vendor to specify a maximum time between pre-operational tests is not necessary and the requirement can be dropped.	David Friant Microsoft, Redmond, WA.	**Accepted: Text has been modified**
431	D.F.	4.9			“If each call to a RBG produces blocks of n bits (where n > 63), the first n-bit block generated after power-up, initialization, or reset shall not be used, but shall be saved for comparison with the next n-bit block to be generated. Each subsequent generation of an n-bit block shall be compared with the previously generated block. The test shall fail if any two compared n-bit blocks are equal. If each call to a RBG produces fewer than 64 bits, the first n bits generated after power-up, initialization, or reset (for some n > 63) shall not be used, but shall be saved for comparison with the next n generated bits. Each subsequent generation of n bits shall be compared with the previously generated n bits. The test fails if any two compared n-bit sequences are equal.” This requirement doesn't work well with SP800-90 since AES counter mode generates variable length output and there is no guarantee the second call will generate the same number of bits. Proposed Disposition: Remove this requirement and require SP 800-90 instead.	David Friant Microsoft, Redmond, WA.	**Accepted: Requirement has been removed**
435	D.F.	4.9	Sec. 9		Section 9 – Self Tests: 2) How should we implement this test?	David Friant Microsoft, Redmond, WA.	**Rejected: deferred to DTR**

468	R.A.	4.9	Sec. 4.9 par 2 4.9.1		This information would also be useful in a users manual or a user's guide.	NSA/SETA/ SPARTA; Rowland Albert, 410-865-7992	**Accepted:**
469	J.W.	4.9	Sec. 4.9.1		Reword the paragraph as: “Cryptographic Algorithm Test. This test shall be conducted for every implementation of all Approved and Allowed cryptographic algorithms (e.g., encryption, decryption, data authentication and random it generation) by a cryptographic module via any of the following methods.” / This emphasizes the fact that it is the software implementation that is being tested, and not the algorithm.	BAH/NSA I181 SETA; Jay White, 410-684-6675	**Accepted: Text has been modified**
470	J.L.	4.9	Sec. 4.9.2		Continuous RBG test - I suggest adding NIST SPUB 800-22 to describe NIST approved methods to test RBGs. Needed for clarity, completeness and to ensure security.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**Obsolete**
552	B.W.	4.9	Sec. 4.9.1		The following statements should be added to the description of the test: The min-entropy assessment shall be performed within the entropy source, using an approved method.	Bridgete Walsh - CSE	**Requirement Removed**
606	C.R.	4.9	Section 4.9.1, Para 5		With regard to this requirement, we believe it provides limited security improvement over the current checksum method defined in FIPS 140-2. Our analysis of this requirement results in a conclusion that the requirement is mainly focused on detection of deliberate software image overwrites. We analyzed and concluded that: 1. Because the public key, expected signature and code that does the signature validation is allowed to reside in the image, it is possible that a deliberate overwrite would also overwrite any one of the three items. 2. Because it runs only periodically, a corrupted image may be able to run a considerable amount of time before the test is run to detect it 3. Embedded systems often install a single image on the device which contains a combination of program text and initialized data. When the Software Integrity Test is invoked from an MSI command the initialized data may have changed during the normal operation of the system and the test will fail. We conclude that this run time test offers limited protection and should be relaxed to the existing checksum requirement	Chris Romeo - Cisco	**Accepted:**

					found in FIPS 140-2. Cisco also believes that vendors should be allowed to create a new signature locally of just the program text upon conclusion of the Software Load Test, and subsequently use the locally generated signature as validation of the Software Integrity Test.		
607	C.R.	4.9	Section 4.9.1, Para 5 and Section 4.9.2, Para 3		Please clarify the Software Integrity Test requirements with respect to products that have multiple special purpose processors. When the cryptographic module is made up of multiple special purpose processors some of the processors may not have the capability to execute the software integrity test on their own. The initial software is loaded into the FIPS 140 boundary in one load and smaller images are extracted from that load to run in the various processors. We would like the standard to acknowledge that each special purpose processor may not have the capability of executing its own Software Integrity Test using a digital signature algorithm.	Chris Romeo - Cisco	**Accepted:** Addressed in DTR as an implementation issue.
608	C.R.	4.9	Section 4.9.2, "RGB Entropy Source Test"		Requirement: "[i]f an RNG entropy source is contained within the operational environment, then the min-entropy assessment shall be performed on each output of the entropy source". Please clarify what tests are to be executed in support of this requirement. We believe the intention of this requirement is to execute a source-specific test designed to catch anticipated failure modes of the entropy source.	Chris Romeo - Cisco	**Accepted:** Requirement removed.
701	W.C.	4.9	Sec. 4.9.1.		Consider changing "uses a function or provides a service using the function to be tested" to "uses a function to be tested or provides a service using the function".XXX Does a software module need to perform the pre-operational tests after the computer wakes up from the suspend or hibernate state? Consider removing "a critical time period that specifies", or changing "that specifies" to "that is".	Wan-Teh Chang	**Accepted: Text has been modified**
705	W.C.	4.9	Sec. 4.9.2		Consider changing "the public key shall encrypt" to "the public key shall be used to encrypt".	Wan-Teh Chang	**Obsolete:**

712	W.C.	4.9	Sec. 4.9.3		the paragraph under SECURITY LEVELS 2, 3, 4 AND 5: Should we change "when the module is powered up" to "before the module uses the critical functions"? I asked because power-up self-tests have been renamed pre-operational self-tests.	Wan-Teh Chang Member of the NSS Project	**Obsolete: Text has been already modified**
860	IG	4.9	Sec. 4.9.1		The second sentence should be struck. This is not consistent with the notion of delayed self-tests described in Section 4.9.1.	Inforgard	**Accepted: Text has been modified**
861	IG	4.9	Sec. 4.9.2		Under the Software Load Test, the second bullet should reference a digital signature technique, not an approved data authentication technique.	Inforgard	**Accepted: Text has been modified**
862	IG	4.9	Sec. 4.9.2		Under the Continuous RBG test, the two bullets should be rephrased to be consistent with the description of the test: These two options apply to both RBG output and RBG entropy source output.	Inforgard	**Obsolete: Text has been modified**
877	AT	4.9	Sec. 4.9.2		•Section 4.9.2 – Conditional Self-Tests, RBG Entropy Source Test. This may be quire difficult for software modules to implement such a test during operation. •Conditional Self-Tests; Pairwise Consistency Test (for public and private keys) Replace the second bullet with “If the keys are used to perform the calculation and verification of digital signature then the consistency of the keys shall be tested using the following method:” Verify a known message using a fixed signature and known public key Sign a random or fixed message using a known private key Verify the generated signature using a known public key Add the following Level 3+ requirement, “For Security Level 3, the pair-wise consistency test (for public and private keys), must also be performed when a key pair is entered into the module.”	Atlan	**Accepted:**

894	AT	4.9	Sec. 4.9.1		•Section 4.9.1 – Pre-Operational Self-Tests section, requiring pre-operational tests to be re-executed from a low power state might be too difficult to achieve. This may also prevent some software modules from being validated if the operating system does not appropriately broadcast the power-up state of the OS.	Atlan	**Accepted:** Requirement removed.
918	CL	4.9	Sec. 4.9		"If a cryptographic module fails a self-test, the module shall enter an error state and shall output an error indicator via the status output interface." According to section 4.2 status indicators can be explicit or implicit. This requirement seems to prohibit an implicit error status indicator. What was intended? In Section 4.9.1, Paragraph 1 it states that "When a pre-operational test is completed, the results (i.e., indications of success or failure) may be output via the "status output" interface." This also seems to permit an implicit error status indicator.	CEAL	**Accepted: Text has been removed**
926	CL	4.9	Sec. 4.9.1		"The pre-operational self-tests shall be initiated automatically and shall not require operator intervention." See comment from Section 4.4 – Security Level 4, Bullet Point 2. If the Software Integrity Test Decryption Key must be provided on each power up at levels 4 and 5 then this requirement should be modified to make it clear that operator intervention to provide this key doesn't cause the module to fail the requirement.	CEAL	**Accepted:** Requirement removed.
943	CL	4.9	Sec. 4.9.1		Add a reference back to section 4.4 where it talks about requiring the software integrity test to be stored encrypted at levels 4 and 5.	CEAL	**Accepted:**
954	CL	4.9	Sec. 4.9.1		"A KAT is not required for the security function in the Approved Data Authentication technique used by the Software Integrity Test." If DSA is used as the software integrity test then performing the software integrity test only tests DSA sig ver, not any of the other functions. FIPS 140-2 IG 9.3 explains why this should be insufficient to fully test DSA.	CEAL	**Accepted:**

955	CL	4.9	Sec. 4.9.2		For testing RBG entropy sources, how should this be done for a module which gathers entropy from various sources like key stroke timing, mouse movements, network traffic, etc? Should the pooled entropy output be monitored when it is sent to the RBG? Or should each source be monitored when it adds to the "entropy pool"? Or is this requirement just intended to apply to non-deterministic RNGs that are used as RBG entropy sources?	CEAL	**Accepted:** Requirement removed.
958	CL	4.9	Sec. 4.9.2		"If the keys are used to perform key agreement, then the arithmetic validity of the keys shall be tested by verifying the correct mathematical relationship between the public key and private key values." For Diffie-Hellman key agreement, how would this be accomplished?	CEAL	**Accepted:** Text provided to key agreement schemes.
959	CL	4.9	Sec. 4.9.2		Please provide guidance that vendors can look at for so they can understand how and what to implement in their modules to meet this requirement.	CEAL	**Accepted:** Will be provided in DTR.
1123	D.W.	4.9	Sec. 4.9.1		Before a cryptographic module can begin operating securely, it must transition from a power-off state or quiescent state to a secure operational state. This requires verification that the module is functioning properly via pre-operational self-tests – such as those described in 4.9.1. Once the pre-operational self-tests have been conducted (and passed), the initialization. The following initialization requirement should be considered (at the appropriate security level rating) for FIPS 140-3: cryptographic algorithms implemented by the module must be properly initialized in preparation for use. This includes determining appropriate values (including randomization) for the quantities defining the state of each cryptographic process. Setting the initial operational state of a cryptographic process is referred to as cryptographic initialization. The following initialization requirement should be considered (at the appropriate security level rating) for FIPS 140-3: •Cryptographic initialization (including randomization) must be performed following cold start-up, power interruptions, changes in SSPs, updating of software (etc.), alarm checks and, depending on the	Debbie Wallner-NSA	**Accepted:**

					cryptologic, may be performed aperiodically, or as part of selected operating mode changes.		
1136	D.W.	4.9	Sec. 4.9.1		last paragraph, last sentence, suggest changing the phrase, “is first exercised” to “is first used operationally” to enhance readability.	Debbie Wallner-NSA	**Accepted:** This is a pre-operation test so text is removed.
1203	R.E.	4.9	4.9		A cryptographic module shall perform pre-operational self-tests, conditional self-tests and, if applicable, critical functions tests to ensure that the module is functioning properly. The pre-operational self-tests must be performed and passed successfully prior to the module providing any services. Conditional self-tests shall be performed when an applicable security function is invoked (i.e., security functions for which self-tests are required). A cryptographic module may perform other tests in addition to the tests specified in this standard.	Randy Easter - NIST	**Rejected:** No question.
1205	R.E.	4.9	4.9.1		The pre-operational tests shall be performed by a cryptographic module between the time a cryptographic module is powered on, either from a power-off state or a quiescent state (e.g., low power, suspend or hibernate) and the time that the cryptographic module uses a function or provides a service using the function to be tested. Prior to using a security function, the pre-operational test(s) of that security function shall pass successfully. The pre-operational self-tests shall be initiated automatically and shall not require operator intervention. The vendor shall specify a critical time period that specifies the maximum operational time before pre-operational tests must be repeated. When a pre-operational test is completed, the results (i.e., indications of success or failure) may be output via the “status output” interface. 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.	Randy Easter - NIST	**Rejected:** No question.
8	D.F.	4.9		GE	Section 9 – Self Tests: 2) How should we implement this test?	David Friant - Microsoft	**Rejected:** Comment is too vague.

124	D.F.	4.9			Microsoft is very concerned about the new requirements around running self-tests on resume from standby / hibernate and periodical re-test. We do not understand how this will make products more secure. MES: FIPS 140-2 states: “Power-up tests shall be performed by a cryptographic module when the module is powered up (after being powered off, reset, rebooted, etc.).” FIPS 140-3 states: “The pre-operational tests shall be performed by a cryptographic module between the time a cryptographic module is powered on, either from a power-off state or a quiescent state (e.g., low power, suspend or hibernate) and the time that the cryptographic module uses a function or provides a service using the function to be tested.” FIPS 140-3 would require pre-operational test after low power, suspend or hibernate. The more often a test is performed, the sooner it might detect an error, thus improving security. However, the question seems to be whether the efficiency impact of this testing is worth the security benefit. Proposed Disposition: Change the requirement to state “The pre-operational Tests shall be performed by a cryptographic module between the time a cryptographic module is powered on and the time that the cryptographic module uses a function or provides a service using the function to be tested.”	David Friant Microsoft, Redmond, WA.	**Accepted:** Text changed
241	J.H.	4.9	Sec. 4.9.1		The “Software Integrity Test” description contains some wording whose meaning is unclear. It says, “The Software Integrity Test is not required for any software excluded from the security requirements of this standard or for any executable code stored in non-reconfigurable memory.” Does this mean, for example, that the firmware loaded into a hardware crypto module would not be subject to the SIT since it is loaded in memory that is reconfigurable only via the approved software load operation? This would make sense since the firmware code would be properly verified using the Software Load Test and then cannot be changed, except by a subsequent software load. However, the wording of	Johnn Hsiung - for - SafeNety	**Accepted:** additional information can be found in the DTRs

					section 4.9.2 appears to say that the SIT has to pass after the Software Load test has been completed, which would indicate that consideration for the Software Load Test is not being given with respect to applying the SIT. (See the comment on section 4.9.2 also).		
424	D.F.	4.9			"The vendor shall specify a critical time period that specifies the maximum operational time before pre-operational tests must be repeated." A periodic self-test requirement adds a lot of complexity to crypto modules, especially for those that run in kernel mode. Moreover, running periodic self-tests may have an unpredictable side effect on real-time scenarios such as media playback.	David Friant Microsoft, Redmond, WA.	**Accepted: Text has been modified** **Duplicate of 006-2**
428	D.F.	4.9			"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" A continuous test is incompatible with pre-operational testing. If a module chooses this option, when should they consider the pre-operational test complete? Perhaps this should be in a different section. Proposed Disposition: No change is necessary. The continuous comparison of outputs is in lieu of KAT tests.	David Friant Microsoft, Redmond, WA.	**Duplicate of 006-3**

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
38	J.R.	4.10	4.10.4	GE	In addition to the requirements for Security Level 1, the following requirements shall apply to cryptographic modules for Security Levels 2 and 3: • All software within a cryptographic module shall be implemented using a high-level, non-proprietary language, except that the limited use of a low-level language (e.g., assembly language or microcode) is allowed if essential to the performance of the module or when a high-level language is not available. • Custom integrated circuits within a cryptographic module shall be implemented using a high-level HDL (e.g., VHDL or Verilog). Comments: (note) The last exception effectively removes the "shall" from the requirement. Suggest that this be reworded. What is the intent of this requirement?	James Randall RSA	**Rejected**: the reviewer needs to provide additional explanation.
39	J.R.	4.10	4.10.4	GE	• If a cryptographic module contains software, documentation shall specify the compilers, configuration settings, and methods to compile the source code into an executable form. The documentation shall also include the source code for the software, annotated with comments that depict the correspondence of the software to the design of the module. Comments: (insert) compiler versions, runtime libraries, runtime library versions, (basically anything involved in the conversion of source code into executable form should be included in the list of required documentation).	James Randall RSA	**ACCEPTED** Inserted suggested text.
40	J.R.	4.10	4.10.3	GE	The FSM of a cryptographic module shall include the (at least)following operational and error states: Comments: (insert) at least	James Randall RSA	**ACCEPTED** Inserted suggested text.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
97	C.P.	4.10	4.10.4		Standard: The hardware and software of a cryptographic module can be excluded from the requirements of this standard if the vendor can demonstrate. Suggestion: The hardware and software components of a cryptographic module can be excluded from the requirements of this standard if the vendor can demonstrate.	Claudia Popa - CSE	**ACCEPTED** Inserted suggested text in section 4.1
194	J.B.	4.10	Sec. 4.10.4		The requirement in sec. 4.10.4 Development for documentation specifying compiler settings does not seem to serve any security purpose, as for the vast majority of software build processes, the compiler settings will be defined as part of an overall build system that is defined by resources such as a Visual C++ project files or makefiles etc. These resources will themselves be configuration managed. In addition the compiler options may not be constant throughout the build process. A simple example is the use of compiler options that are embedded in C language files which override any options defined at a global build level. Therefore Thales e-Security believes that the requirement should be changed to requiring that the build process is documented and all resources required to perform this task are configuration managed so as to provide assurance that the executable form of the software used by the module is reproducible and maintainable.	Jason Bennet- -Thales e-Security	**ACCEPTED** Inserted suggested text

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
195	J.B.	4.10	Appendix C:		The inclusion of additional information that is relevant to an end-user in the Security Policy and its alignment with the FIPS 140-3 security requirements categories is welcomed with the exception of the Life-Cycle Assurance section. This includes information that may be considered IPR to the vendor and thus would not generally be made publicly available although it would be considered for release to a customer with specific concerns. In addition it is unclear as to how this aids the end-user as this information has already been validated as part of the FIPS 140 process and does not describe security characteristics of the module. For these reasons it is felt that information that deals with a vendor's own internal development processes in sec. 10 Life-Cycle Assurance should not be included in the Security Policy.	Jason Bennet- -Thales e-Security	**ACCEPTED** References to configuration management, development and testing have been removed from Appendix C.
243	J.H.	4.10	Sec. 4.10.6		Similar to comment 2 on section 4.3.2, the requirement at Levels 3,4 &5 for an authorized operator to authenticate to the module using authentication data provided by the vendor is not feasible in the case of personal use devices.	Johnn Hsiung - for - SafeNet	**REJECTED** The level of difficulty for what the vendor-provided authentication data is not specified. We may have to develop an IG on this.
257	J.K.	4.10	4.10		"Describe the correspondence between design, the security policy and the FSM (may be a separate document)." This sentence should not be included in Appendix C but in Appendix A. Move the sentence from Appendix C to Appendix A.	JCMVP 52 Junichi Kondo	**ACCEPTED** Moved the requirement from Appendix C to Appendix A and adjusted to meet the requirement of Section 4.10.2.
258	JC	4.10			There are some difficulties in defining followings. 1.the "state" in FSM 2. the mode of operation of cryptographic module when one thread performs an Approved security function and another thread performs a Non-Approved security function at the same time.	JCMVP	**Obsolete.**

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
317	J.L.	4.10	4.10.1		The configuration manager does not specify the security requirements; the CM manages/tracks the requirements. A CM manages the security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures and test documentation of an automated information system, throughout the development, operational life of a system, storage and secure disposition.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**ACCEPTED** Deleted de word “security” from the sentence.
365	J.K.	4.10	Appendix A,C		“Cryptographic Officer guidance” should be “administrator guidance”. Rewrite “Cryptographic Officer guidance” as “Administrator guidance”.	JCMVP39 Junichi Kondo	**ACCEPTED** Appendix A was changed to reflect the terminology used in section 4.10 and Appendix C (i.e., Administrative and non-administrative)
367	J.K.	4.10	Appendix A		This requirement corresponds to Security Levels 4 and 5. Rewrite “Security Level 4” as “Security Levels 4 and 5”.	JCMVP37	**Obsolete** Security level 5 has been removed
368	J.K.	4.10	4.10 Appendix A		This requirement corresponds to Security Level 5. Replace “Security Level 4” with “Security Level 5”.	JCMVP36 Junichi Kondo	**ACCEPTED** Changed as suggested.
369	J.K.	4.10	4.10 Appendix A		This requirement corresponds to Security Level 5. Replace “Security Level 4” with “Security Level 5”	JCMVP35	**ACCEPTED** Changed as suggested.
370	J.K.	4.10	4.10 Appendix A		This requirement corresponds to Security Level 5. Replace “Security Level 4” with “Security Level 5”.	JCMVP34 Junichi Kondo	**ACCEPTED** Changed as suggested.
373	J.K.	4.10	4.10.3		What is the difference between Approved state and User state? Is an Approved state contained in a User state?	JCMVP33	**ACCEPTED** Removed non-approved services from User Role State.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
476	J.L.	4.10	Sec. 4.10.1		The configuration manager does not specify the security requirements; the CM manages/tracks the requirements. A CM manages the security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures and test documentation of an automated information system, throughout the development, operational life of a system, storage and secure disposition.	SPARTA, NSA I181 SETA, Joe Lisi, 410-865-7991	**ACCEPTED** Deleted de word “security” from the sentence.
592	B.M.	4.10			The new requirement for software implementation in a high-level language has the potential for a large impact on smart card products. Have suppliers been surveyed to determine the implementation methods currently employed, and the potential of this requirement to cause validation delays, and high re-engineering costs, to the manufacturers? Is this requirement meaningful without a security evaluation of the software development tools used to translate the high-level language to object code?	Bill MacGregor NIST	**REJECTED** The standard offers the possibility of using low-level language for the development of firmware. Furthermore, the requirement has been there in FIPS 140-2 and did not appear to cause any issues.
598	C.B.	4.10	Section 4.10.3		I would recommend removing the requirements for the FSM Model for levels 1, 2, and 3 as the states listed are too generic for all types of modules. I would recommend introducing FSM Diagram and Transition Table at Level 4 and above where a FSM Model would make more sense to show pre and post conditions of all states the module could enter. DOMUS feels that this section does not provide much value for modules at levels 1, 2, and 3. At Level 4, we feel that vendors must show more detail to prove their design.	Chris Brych - DOMUS	**REJECTED** The use of an FSM imposes a level of rigor on module developers that we consider necessary for security products.
599	C.B.	4.10	Section 4.10.5		DOMUS is concerned that vendors will not want to provide their testing methodologies to the CMVP.	Chris Brych - DOMUS	**REJECTED** As for any vendor evidence, the proprietary information only goes to and remains at the CST lab, and the CMVP does not require consulting it.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
609	C.R.	4.10	Section 4.10.2, Security Level 1		Please elaborate on what is required of the vendor as correspondence analysis. An example correspondence analysis would be beneficial for vendors as a reference similar to the outline of the Security Policy included in the standard.	Chris Romeo - Cisco	**Accepted:** deferred to IG
610	C.R.	4.10	Section 4.10.2		Requirement: "Cryptographic modules shall be designed to allow the testing of the implemented functionality to this standard, where possible without compromising the security of the module, so that all the services of the cryptographic module can be tested." Please be more specific as to the definition of "all the services of the cryptographic module". The requirement as worded now is very broad and could include many different tests.	Chris Romeo - Cisco	**Accepted:** deferred to IG
611	C.R.	4.10	Section 4.10.6, "Level 3 and above"		"... the procedures shall require the authorized operator to authenticate to the module using authentication data provided by the vendor." This requirement implies that vendors must install authentication credentials during manufacturing. Combined with the requirement in 4.3.2 that credentials be "unique per module unit delivered", we understand that the credentials for any particular module are specific for a particular customer. This requirement adds complexity to the manufacturing process and provides limited advantage for the security of the module. Default credentials as supplied in manufacturing must be upgraded by the cryptographic officer prior to the deployment of the module in a production environment. The inclusion of the credentials does not greatly improve security of the module since they will be changed prior to deployment. The inclusion of a default credentials while the module is in transit to the customer does not improve security of the module. An alternative solution would be to enforce tamper evidence protections in the module delivery process. Instituting a process such as this would provide the administrator with evidence if the module had been tampered with after leaving the manufacturing facility.	Chris Romeo - Cisco	**PARTIALLY ACCEPTED** Requirement in section 4.3.2 has been removed. Added the requirement to specify in Appendix C (security policy) how to detect tamper during the delivery of the module to the authorized operator. The addition of an “out-of-band” delivery of the default password does add some level of assurance to the secure delivery of the module.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
713	W.C.	4.10	Sec, 4.10.1		1st paragraph under SECURITY LEVELS 1 AND 2: Change "security requirement" to "security requirements" (plural) because there are four requirements.	Wan-Teh Chang Member of the NSS Project	**ACCEPTED** Added the suggested text.
714	W.C.	4.10	Sec. 4.10.3		the bullet item under SECURITY LEVEL 2:Consider changing "Documentation shall specify" to "Documentation shall include" because "specify a functional specification" sounds strange.	Wan-Teh Chang Member of the NSS Project	**ACCEPTED** Added the suggested text.
715	W.C.	4.10	Sec. 4.10.3		1st paragraph of the section: The second sentence says "The FSM shall be sufficiently detailed to demonstrate that the cryptographic module complies with all of the requirements of this standard." Do you really mean *all* of the requirements of this standard? This will require vendors to prepare FSMs that are much more complex than what is required for FIPS 140-2.	Wan-Teh Chang Member of the NSS Project	**REJECTED** The CST laboratory will determine whether the FSM meets that requirement. The FSM must be sufficiently detailed to show where all the requirements are met.
722	W.C.	4.10	Sec. 4.10.4		Add "used" after "the compilers, configuration settings, and methods".	Wan-Teh Chang Member of the NSS Project	**ACCEPTED** Added the suggested text.
724	W.C.	4.10	Sec. 4.10.5		Change "testing the security functionality" to "the testing of the security functionality".	Wan-Teh Chang Member of the NSS Project	**ACCEPTED** Added the suggested text.
778	IG	4.10	Sec. 4.10.7		Need to add a glossary term for Administrator Guidance from Section 4.10.7	InfoGard	**ACCEPTED** Moved definition found in section 4.10.7 in the Glossary section.
779	IG	4.10			Need to add a glossary term for Functional Testing from Section 4.10.5	InfoGard	**ACCEPTED** Moved definition found in section 4.10.5 in the Glossary section.
780	IG	4.10	Sec. 4.10.5		Need to add a glossary term for Low Level Testing from Section 4.10.5	InfoGard	**ACCEPTED** Moved definition found in section 4.10.5 in the Glossary section.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
781	IG	4.10			Need to add a glossary term for Non-Admin Guidance from Section 4.10.7	InfoGard	**ACCEPTED** Moved definition found in section 4.10.7 in the Glossary section.
863	IG	4.10	Sec 4.10.2		Level 4, the first bullet: This correspondence should be made to the implementation, not the design of the module.	InfoGard	**REJECTED** Section 4.10.2 deals with the design and not the implementation of the module. The requirements for the creation of the module are specified in section 4.10.4. The correspondence between the design and the implementation is required at Level 1.
864	IG	4.10	Sec. 4.10		Table 1: Level 4 & 5 requirements listed in the table are inconsistent with the sections in 4.10. In Section 4.10, Level 4 & 5 requirements are split among the "Design" and "Development" sections.	InfoGard	**ACCEPTED** Table 1 amended. A new table will be devised.
865	IG	4.10	Sec. 4.10		Level 4 & 5 requirements in general: Clarification of the meaning of "an informal proof". It seems that the vendor should have to explicitly write a document that is classified as "an informal proof". As it is currently written, "an informal proof" could be argued to be nothing that is explicitly written as "an informal proof". Instead it could merely be implied at the discretion of the tester. For example, as it stands, "an informal proof of the correspondence between the formal model and the functional specification" could be nothing more than the tester putting the formal model and the functional specification next to each other and comparing them.	InfoGard	**Accepted:** deferred to IG
866	IG	4.10	Sec. 4.10.2		Level 4: The discussion of pre and post conditions is premature. They should be explicitly defined or a reference should be given.	InfoGard	**Accepted:** deferred to IG

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
867	IG	4.10	Sec. 4.10.4		Levels 4 & 5: The bullet reads, "For each cryptographic module hardware and software component, the documentation shall be annotated with comments that specify...". It seems that "the documentation" should be replaced with "the source code". If not, the vendor will be able to argue that putting pre and post conditions in documentation outside of the code is sufficient and it really is not.	InfoGard	**REJECTED** The source code would unnecessarily be too big.
874	IG	4.10			Automated CMS - The requirement of “Automated CMS” for higher security levels is underspecified (4.10.1). In an enterprise development environment, all CMS technologies would probably qualify. One may probably reduce the explicit “automation” requirement without impacting design assurance.	Inforgard	**REJECTED** The intent is to have a computer-based CMS at higher levels. At lower levels, the use of a paper-based system is allowed.
944	CL	4.10	Sec. 4.10.3		Should the CSP entry state be expanded into a SSP entry state? Or should a PSP entry state be added to the required state list? On the optional states, more possible examples that could be added: Alternating Bypass State (For a module which might support what would have been called an Alternating and an Exclusive bypass mode under 140-2) Non-Approved Mode State Degraded Mode State Maintenance Mode State	CEAL	**REJECTED** The states listed are the minimum list of states. The vendors can add other to help better design their module..
945-1	CL	4.10	Sec. 4.10.6		Add a reference back to section 4.4 which requires, at levels 4 and 5, the software integrity test be encrypted when the module is delivered, and that the crypto officer has the option to change that encryption key during setup.	CEAL	**REJECTED** There is no longer Security Level 4 and 5 software modules.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
945-2	CL	4.10	Sec. 4.10.6		Add a reference back to section 4.4 which requires at level 3 and higher that the software output a hash of the module software so the crypto officer can independently confirm that it matches the expected hash.	CEAL	**REJECTED** The requirement has been removed.
945-3	CL	4.10	Sec. 4.10.6		Appendix C – Software Security, Bullet Point 4 "How is the code obfuscated?" There isn't a requirement for code obfuscation.	CEAL	**ACCEPTED:** deferred to IG.
945-4	CL	4.10	Sec. 4.10.6		Passwords as CSPs As stated in the three references below:	CEAL	Incomplete comment
945-5	CL	4.10	Sec. 4.10.6		Section 1.4 – Paragraph 5 "Level 4 modules that contain software must provide for the encryption and authentication of CSPs…"	CEAL	Incomplete comment
945-6	CL	4.10	Sec. 4.10.6		Section 2.1 "Critical security parameter: security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module."	CEAL	Incomplete comment
945-7	CL	4.10	Sec. 4.10.6		Section 4.5 – Various "To protect plaintext data, cryptographic software, SSPs, and authentication data…" "All SSPs, authentication data, control inputs…" SSPs are CSPs & PSPs, and since the definition of CSP claims that authentication data is a CSP, authentication data is already an SSP. Why call it out separately? Unless authentication data isn't intended to always be a CSP.	CEAL	**REJECTED**: reviewer must provide more information

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
956	CL	4.10	Sec. 4.10.5		“Keys used only to perform pre-operational self-tests shall be considered as PSPs.” This should mention that, per section 4.8, for software modules, and for hybrid modules’ software half, the Software Integrity Test key is a CSP.A Note should be added acknowledging that zeroization at level 5 of a software or hybrid module will destroy required self-test keys and require the reinstallation or replacement of the module.	CEAL	Self-test section
1223	R.E.	4.10	4.10.1		In addition to the requirements for Security Levels 1 and 2, the configuration items shall be managed using an automated configuration management system.	Randy Easter - NIST	**ACCEPTED** The text is already included.
1257	R.E.	4.10	10. LifeCycle assrance		• Provide a statement of the configuration management system and its unique identification. Name the commercial system, if used.• Describe how design requirements are met.• Describe the correspondence between the design, the security policy and the FSM (may be a separate document).• Describe how development requirements are met.• Describe the vendor testing.• Specify the procedures for delivery and operation.• Specify any maintenance requirements.• Provide the Crypto Officer and User guidance (may be a separate document). Why is this of interest to a user?	Randy Easter - NIST	**ACCEPTED** Removed from the Appendix C.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
41	J.R.	4.10	4.10.2	GE	Documentation shall specify a formal model that describes the rules and characteristics of the cryptographic module Security Policy. The formal model shall be specified using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory. Comments: (Strikeout)(that is a rigorous notation based on established mathematics, such as first order logic or set theory.)There should be no specific limit on the formal approach that is used. This can be handled during the review process - as long as the requirements are met any formal method should be acceptable.	James Randall RSA	**Obsolete:** security level 5 has been removed
43	J.R.	4.10	4.10.5		Low-level testing refers to the testing of the individual components or group of components of the cryptographic module and their physical ports and logical interfaces as defined by the documentation required by Section 4.10.2 for Security Level 3. **Comments:** (note) Add this to the glossary in section 2.1	James Randall RSA	**ACCEPTED**
44	J.R.	4.10	4.10.5		This section specifies the security requirements for vendor testing of the cryptographic module, including testing the security functionality implemented in the cryptographic module, providing assurance that the cryptographic module behaves in accordance with the module Security Policy and functional specifications. SECURITY LEVELS 1 AND 2 For Security Levels 1 and 2, documentation shall specify the functional testing performed on the cryptographic module. Functional testing refers to the testing of the cryptographic module functionality as defined by the Functional Specification required by Section 4.10.2. **Comments:** (note) Add this to the glossary in section 2.1	James Randall RSA	**ACCEPTED**

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
45	J.R.	4.10	4.10.2		A design is an engineering solution that addresses the functional specification for a cryptographic module. The design is intended to provide assurance that the functional specification of a cryptographic module corresponds to the intended functionality described in the Security Policy. Cryptographic modules shall be designed to allow the testing of the implemented functionality to this standard, where possible without compromising the security of the module, so that all the services of the cryptographic module can be tested. Comments: (note) For software based modules the documented module services shall be used to perform the required algorithm validation tests. The current 140-2 approach which allows modification of module source for testing purposes or execution of different packaging of code for algorithm validation or "special interfaces" not present in the shipping module should be disallowed. The validation suite should execute via the modules documented services. It should be possible for the end-user to perform algorithm validation confirmation.	James Randall RSA	**ACCEPTED** Addressed in second paragraph of comment.
148-3	J.R.	4.10			10. Life-Cycle Assurance (CMS) Automated CMS. Comment: What is meant by "automated"? TODO - check later sections for this. 10. Life-Cycle Assurance (CMS) Low-level Testing. Comments: What is meant by "low-level" here? TODO - check later sections for this.	James Randall RSA	**REJECTED** “Automated CMS” refers to a computer-based CMS Low-level: Addressed above.

ID	Init	Sub Sec	Para	Type	Comment	Author	Resolution
725	W.C.	4.11	Sec. 4.11		Delete the comma after "not defined elsewhere in this standard".	Wan-Teh Chang Member of the NSS Project	**Accepted:**
8	D.F.			GE	What role does SP800-22 play (if any) in future FIPS certifications? Will it add new self-test requirements to the our general purpose RNG?	David Friant - Microsoft	**Accepted:** NIST SP 800-22 is no longer applicable as relates to FIPS 140-2 or FIPS 140-3.