Ricoh Company, Ltd.

RICOH IM 2500/3000/3500/4000/5000/6000 version JE-1.10-H

Assurance Activity Report

Version 1.0

September 2023

Document prepared by

www.lightshipsec.com

Table of Contents

1 Introduction

1. This Assurance Activity Report (AAR) documents the evaluation activities performed by Lightship Security for the evaluation identified in Table 1. The AAR is produced in accordance with National Information Assurance Program (NIAP) reporting guidelines.

1.1 Evaluation Identifiers

Table 1: Evaluation Identifiers

Scheme	Canadian Common Criteria Scheme
Evaluation Facility	Lightship Security
Developer/Sponsor	Ricoh Company, Ltd.
TOE	RICOH IM 2500/3000/3500/4000/5000/6000 version JE-1.10-H
Security Target	RICOH IM 2500/3000/3500/4000/5000/6000 version JE-1.10-H Security Target, v2.5
Protection Profile	Protection Profile for Hardcopy Devices, v1.0, September 2015 Protection Profile for Hardcopy Devices, v1.0, Errata #1, June 2017

1.2 Evaluation Methods

2. The evaluation was performed using the methods and standards identified in Table 2.

Table 2: Evaluation Methods

Evaluation Criteria	CC v3.1R5
Evaluation Methodology	CEM v3.1R5
Supporting Documents	N/A
Interpretations	**HCD v1.0** TD0157 FCS_IPSEC_EXT.1.1 - Testing SPDs *Applicable – FCS_IPSEC_EXT.1 is claimed.* TD0176 FDP_DSK_EXT.1.2 - SED Testing *Applicable – FDP_DSK_EXT.1.2 is claimed.* TD0219 NIAP Endorsement of Errata for HCD PP v1.0 (Errata #1, June 2017) *Applicable – ST claims conformance to HCD PP v1.0.*

TD0253 Assurance Activities for Key Transport *N/A – FCS_COP.1(i) is not claimed.*
TD0261 Destruction of CSPs in flash *Applicable – FCS_CKM.4 is claimed.*
TD0299 Update to FCS_CKM.4 Assurance Activities *Applicable – FCS_CKM.4 is claimed.*
TD0393 Require FTP_TRP.1(b) only for printing *Applicable – FTP_TRP.1(b) is claimed.*
TD0474 Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1 *Applicable – FCS_TLS_EXT.1 is claimed.*
TD0494 Removal of Mandatory SSH Ciphersuite for HCD *N/A – FCS_SSH_EXT.1 is not claimed.*
TD0562 Test activity for Public Key Algorithms *N/A – FCS_SSH_EXT.1 is not claimed.*
TD0642 FCS_CKM.1(a) Requirement; P-384 keysize moved to selection *Applicable – FCS_CKM.1(a) is claimed.*

2 TOE Details

2.1 Overview

3. The TOE is a Digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents.

2.2 TOE Models

4. The TOE model number indicates the copy rate (higher numbers indicate the higher copy rate). The differences between models are not security relevant and are limited to print engine components (speed) and branding variations (labels, displays, packaging materials and documentation).

Table 3: TOE Models

Branding	Model
RICOH	RICOH IM 2500, RICOH IM 2500F RICOH IM 3500, RICOH IM 3500F RICOH IM 4000, RICOH IM 4000F RICOH IM 5000, RICOH IM 5000F RICOH IM 6000, RICOH IM 6000F* IM 2500, IM 2500A, IM 2500G IM 3000, IM 3000A, IM 3000G IM 3500, IM 3500A, IM 3500G IM 4000, IM 4000A, IM 4000G IM 5000, IM 5000A, IM 5000G IM 6000, IM 6000G
SAVIN	IM 2500, IM 2500A, IM 2500G IM 3000, IM 3000A, IM 3000G IM 3500, IM 3500A, IM 3500G IM 4000, IM 4000G IM 5000, IM 5000G IM 6000, IM 6000G
LANIER	
nashuatec	IM 2500, IM 2500A IM 3000, IM 3000A IM 3500, IM 3500A IM 4000, IM 4000A IM 5000, IM 5000A IM 6000
Rex Rotary	
Gestetner	

* Models sold in Japan include RICOH in the model name.

The TOE includes the following critical components:

a) **Main Controller.** Provides primary printing, scanning, faxing, and networking functionality.

   i) **CPU.** Intel Atom x5-E3930.

   ii) **OS.** LPUX6.0 OS (customized NetBSD 6.0.1).

b) **Operation Unit.** Provides front panel interface control and device extensibility capabilities.

   i) **CPU.** ARM Cortex-A9 Quad Core.

   ii) **OS.** Linux 3.18 (customized).

2.3 Reference Documents

Table 4: List of Reference Documents

Ref	Document
[ST]	RICOH IM 2500/3000/3500/4000/5000/6000 version JE-1.10-H Security Target, v2.5
[PP]	Protection Profile for Hardcopy Devices, v1.0, September 2015 Protection Profile for Hardcopy Devices, v1.0, Errata #1, June 2017
[KMD]	Key Management Description for RICOH IM 7000/8000/9000/9000T version JE-1.10H RICOH IM 2500/3000/3500/4000/5000/6000 version JE-1.10H, Version: D-0.0.6
[ENT]	Entropy Description for RICOH IM C530F/C530FB, version E-1.10-H, RICOH IM 7000/8000/9000/9000T version JE-1.10H, RICOH IM 2500/3000/3500/4000/5000/6000 version JE-1.10H, Version: D-0.0.4
[AGD]	RICOH IM 2500/3000/3500/4000/5000/6000 Common Criteria Guide, v1.5
[UG]	User Guide IM 2500/3000/3500/4000/5000/6000 series, D0CH7853 2023.03 https://support.ricoh.com/services/device/ccmanual/im_2500-3000-3500-4000-5000-6000-re/en-GB/booklist/int/index_book.htm
[SEC]	User Guide Security Reference, D0CH7852-EN 2023/3 https://support.ricoh.com/services/device/ccmanual/im_2500-3000-3500-4000-5000-6000-re/SecurityReference/en-GB/booklist/int/index_book.htm

2.4 Summary of SFRs

Table 5: List of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_STG.1	Protected Audit Trail Storage

Requirement	Title
FAU_STG_EXT.1	Extended: External Audit Trail Storage
FAU_STG.4	Prevention of Audit Data Loss
FCS_CKM.1(a)	Cryptographic Key Generation (for asymmetric keys)
FCS_CKM.1(b)/DAR	Cryptographic Key Generation (for Symmetric keys) [Data At Rest]
FCS_CKM.1(b)/DIM	Cryptographic Key Generation (for Symmetric keys) [Data In Motion]
FCS_CKM_EXT.4	Extended: Cryptographic Key Material Destruction
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1(a)	Cryptographic Operation (Symmetric Encryption/Decryption)
FCS_COP.1(b)	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1(c)/L1	Cryptographic Operation (Hash Algorithm)
FCS_COP.1(c)/L2	Cryptographic Operation (Hash Algorithm)
FCS_COP.1(d)	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(f)	Cryptographic Operation (Key Encryption)
FCS_COP.1(g)	Cryptographic Operation (for keyed-hash message authentication)
FCS_HTTPS_EXT.1	Extended: HTTPS selected
FCS_IPSEC_EXT.1	Extended: IPsec selected
FCS_KYC_EXT.1	Extended: Key Chaining
FCS_RBG EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
FCS_TLS_EXT.1	Extended: TLS selected
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security attribute based access control
FDP_DSK_EXT.1	Extended: Protection of Data on Disk
FDP_FXS_EXT.1	Extended: Fax separation
FDP_RIP.1(a)	Subset residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition

Requirement	Title
FIA_PMG_EXT.1	Extended: Password Management
FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_KYP_EXT.1	Extended: Protection of Key and Key Material
FPT_SKP_EXT.1	Extended: Protection of TSF Data
FPT_STM.1	Reliable Time Stamps
FPT_TST_EXT.1	Extended: TSF testing
FPT_TUD_EXT.1	Extended: Trusted update
FTA_SSL.3	TSF-initiated Termination
FTP_ITC.1/TLS	Inter-TSF trusted channel
FTP_ITC.1/IPsec	Inter-TSF trusted channel
FTP_TRP.1(a)	Trusted Path (for Administrators)
FTP_TRP.1(b)	Trusted Path (for Non-administrators)

3 Evaluation Activities for SFRs

3.1 Security Audit (FAU)

3.1.1 FAU_GEN.1 Audit data generation

3.1.1.1 TSS

5. The evaluator shall check the TOE Summary Specification (TSS) to ensure that auditable events and its recorded information are consistent with the definition of the SFR.

Findings:	[ST] 6.1.1 is consistent with FAU_GEN.1.

3.1.1.2 Operational Guidance

6. The evaluator shall check the guidance documents to ensure that auditable events and its recorded information are consistent with the definition of the SFRs.

Findings:	The [AGD] specifies in Annex A the auditable events. They are consistent with the SFR.

3.1.1.3 Test

7. The evaluator shall also perform the following tests:

8. The evaluator shall check to ensure that the audit record of each of the auditable events described in Table 1 is appropriately generated.

9. The evaluator shall check a representative sample of methods for generating auditable events, if there are multiple methods.

10. The evaluator shall check that FIA_UAU.1 events have been generated for each mechanism, if there are several different I&A mechanisms.

High-Level Test Description
During testing, the evaluator recorded audit messages for each of the events specified in table 1 of the [PP]. All were found to be suitable. Specifically, for FIA_UAU.1, audit logs were found to be sufficient for successful and unsuccessful login attempts across all claimed mechanisms.
Findings: PASS

3.1.2 FAU_GEN.2 User identity association

11. The Assurance Activities for FAU_GEN.1 address this SFR.

3.1.3 FAU_STG_EXT.1 Extended: External Audit Trail Storage

3.1.3.1 TSS

12. The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is

provided. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism.

Findings:	[ST] 6.1.2 - Audit records are buffered in before transfer to a configured remote syslog server over a TLS trusted channel or IPsec trusted channel.

13. The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

Findings:	[ST] 6.1.2 - By default, the job and ecology logs will each hold a maximum of 4,000 records; the access log can have a maximum of 12,000 records. When a maximum number of records is reached, the oldest records are overwritten. The TOE stores audit log data in a dedicated storage area of the HDD and in the evaluated configuration transfers audit data to the remote audit server as events are generated. The TOE prevents unauthorized access to the audit records by ensuring that the options to manage the audit function and the audit records are not included in the lists of available functions visible to the U.NORMAL users.

3.1.3.2 Operational Guidance

14. The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.

Findings:	[AGD] Section 3.3.2.5 specifies the means to configure IPsec for the TOE, and [AGD] Section 3.4.2 specifies the configuration of the Syslog server to use TLS.

3.1.3.3 Test

15. Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.

High-Level Test Description
Verification that the data is encrypted is satisfied by FTP_ITC.1 for the logging channel. The logging server is a syslog-ng v3.8.1 as described in the Test Setup.
Findings: PASS

3.2 Cryptographic Support (FCS)

3.2.1 FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

16. *(Modified by NIAP TD0642)*

3.2.1.1 TSS

17. The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.

18. Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described in the TSS.

19. The TSS may refer to the Key Management Description (KMD), described in Appendix F, that may not be made available to the public.

Findings:	[ST] 6.7.2 - the TOE employs KAS FFC, KAS-ECC establishment schemes conforming to NIST SP 800-56A Section 5.6.

3.2.1.2 Test

20. The evaluator shall use the key pair generation portions of "The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and “The 186-4 RSA Validation System (RSA2VS)” as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

Findings:	The TOE uses safe primes for FFC key agreement in IPsec, and KAS ECC and KAS FFC for TLS in certificate #A1837. This is consistent with the claims. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=14284

3.2.2 FCS_CKM.1(b)/DAR Cryptographic Key Generation (for Symmetric keys) [Data At Rest]

3.2.2.1 TSS

21. The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.

Findings:	[ST] Section 6.4.1 describes the use of the DRBG for key generation.

3.2.2.2 KMD

22. If the TOE is relying on random number generation from a third-party source, the KMD needs to describe the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs to include a short description of the vendor's assumption for the amount of entropy seeding the third-party DRBG. The evaluator uses the description of the RBG functionality in FCS_RBG_EXT or the KMD to determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the user data (FCS_COP.1(d)).

23. The KMD is described in Appendix F.

Findings:	The TOE relies on a third party for random number generation. The function calls to call the DRBG are provided in section 6 of the [KMD]. The entropy estimate is provided in the entropy analysis document. Based on the description given, the DRBG is capable of generating 256-bit keys which is consistent with the claims in FCS_COP.1(d). The claimed mode of encryption (CBC) is not affected by how the underlying key material is generated from the DRBG. *Confidential details are omitted in this public AAR document.*

3.2.3 FCS_CKM.1(b)/DIM Cryptographic Key Generation (for symmetric keys) [Data In Motion]

3.2.3.1 TSS

24. The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.

Findings:	[ST] Section 6.4.1 describes the use of the DRBG for key generation.

3.2.3.2 KMD

25. If the TOE is relying on random number generation from a third-party source, the KMD needs to describe the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs to include a short description of the vendor's assumption for the amount of entropy seeding the third-party DRBG. The evaluator uses the description of the RBG functionality in FCS_RBG_EXT or the KMD to determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the user data (FCS_COP.1(d)).

26. The KMD is described in Appendix F.

Findings:	The TOE relies on a third party for random number generation. The function calls to call the DRBG are provided in section 6 of the [KMD]. The entropy estimate is provided in the entropy analysis document. Based on the description given, the DRBG is capable of generating 256-bit keys which is consistent with the claims in FCS_COP.1(d). The claimed mode of encryption (CBC) is not affected by how the underlying key material is generated from the DRBG. *Confidential details are omitted in this public AAR document.*

3.2.4 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

3.2.4.1 TSS

27. The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.

Findings:	[ST] 6.4.2 - TLS and IPsec session keys are no longer needed at the end of a communication session. The REK, KEK, NVRAM Key, and DevCert Key are always needed and are never destroyed in the evaluated configuration. HDD encryption is always enabled in the evaluated configuration, so the HDD key is always needed. [ST] 6.4.2 – Also specifies that cryptographic keys and key materials stored by the TOE can be destroyed by overwriting the key with the value of a new key; the HDD key can be logically deleted should HDD encryption be disabled.

3.2.4.2 KMD

28. The evaluator shall verify the Key Management Description (KMD) includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed.

29. The evaluator shall verify the KMD includes a key lifecycle, that includes a description where key material reside, how the key material is used, how it is determined that keys and key material are no longer needed, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4 for the destruction.

Findings:	[KMD] section 8 provides a list of keys that are always needed and are never destroyed in the evaluated configuration. [KMD] section 8 also provides the description of how the HDD key can be destroyed if an Administrator: 1. sets a new HDD Key, in which it is logically overwritten with the new key, or 2. disables HDD encryption, in which case it is logically deleted. Table 5 of the same section includes information on the destruction criteria for each key. *Confidential details are omitted in this public AAR document.*

3.2.5 FCS_CKM.4 Cryptographic key destruction

(Modified by NIAP TD0261 and TD0299)

3.2.5.1 TSS

30. The evaluator shall verify the TSS provides a high level description of how keys and key material are destroyed.

31. If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.

32. The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.

Findings:	[ST] 6.4.2 – The TOE destroys cryptographic keys and key materials when no longer needed. The REK, KEK, NVRAM Key, and DevCert Key are always needed and are never destroyed in the evaluated configuration. Cryptographic keys and key materials stored by the TOE can be destroyed by overwriting the key with the value of a new key. Key destruction is further described in the separate proprietary Key Management Document (KMD).

3.2.5.2 KMD

33. The evaluator examines the KMD to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.

Findings:	The [KMD] describes how keys are introduced into volatile memory in section 5 of the [KMD], "Key purpose, protection, and derivation". Keys are destroyed in accordance with the rules provided in section 8 of the [KMD] document, "Key destruction". *Confidential details are omitted in this public AAR document.*

34. The evaluator shall check to ensure the KMD lists each type of key that is stored in non-volatile memory, and identifies the memory type (volatile or non-volatile) where key material is stored.

35. The KMD identifies and describes the interface(s) that is used to service commands to read/write memory. The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) made by the ST Author.

Findings:	The [KMD], in section 5 "Key purpose, protection, and derivation" outlines each of the keys used by the TOE and where (volatile or non-volatile memory) it is stored and whether it is stored in plaintext or not, as well as the method by which the key is destroyed (in section 8 "Key destruction"). The [KMD] specifies in section 9 that the TOE utilizes the operating system's file system operations (i.e. open(), read(), write(), close()) for access to data stored in non-volatile storage. *Confidential details are omitted in this public AAR document.*

3.2.5.3 Operational Guidance

36. There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer and how such situations can be avoided or mitigated if possible.

37. Some examples of what is expected to be in the documentation are provided here.

38. When the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-leveling and garbage collection. This may create additional copies of the key that are logically inaccessible but persist physically. In this case, to mitigate this the drive should support the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.

39. Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. To reduce this risk, the operating system and file system of the OE should support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion. If a RAID array is being used, only set-ups that support TRIM are utilized. If the drive is connected via PCI-Express, the operating system supports TRIM over that channel.

40. The drive should be healthy and contains minimal corrupted data and should be end of life before a significant amount of damage to drive health occurs, this minimizes the risk that small amounts of potentially recoverable data may remain in damaged areas of the drive.

Findings:	The [AGD] section 3.3.2.5 specifies that "Destruction of old keys is performed directly without delay in NVRAM; in Flash, it is performed by an internal microcontroller in concert with wear-leveling, bad block management, and garbage collection processes. There are no situations where key destruction may be delayed at the physical layer."

3.2.5.4 Test

41. For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

42. Test 1: Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator shall:

43. 1. Record the value of the key in the TOE subject to clearing.

44. 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

45. 3. Cause the TOE to clear the key.

46. 4. Cause the TOE to stop the execution but not exit.

47. 5. Cause the TOE to dump the entire memory of the TOE into a binary file.

48. 6. Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.

49. Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.

High-Level Test Description
Not Applicable: The ST claims that keys in volatile memory are zeroized on removal of power.
Findings: PASS

50. Test 2: Applied to each key held in non-volatile memory and subject to destruction by the TOE, except for replacing a key using the selection [a new value of a key of the

same size]. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

51. 1. Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data encryption key being deleted would cause data decryption to fail.)

52. 2. Cause the TOE to clear the key.

53. 3. Have the TOE attempt the functionality that the cleared key would be necessary for. The test succeeds if step 3 fails.

High-Level Test Description
Not Applicable: The ST claims that keys in volatile memory are zeroized on removal of power.
Findings: PASS

54. Test 3: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

55. 1. Record the value of the key in the TOE subject to clearing.

56. 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

57. 3. Cause the TOE to clear the key.

58. 4. Search the non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.

High-Level Test Description
Boot into the debug mode (using console cable) which will permit the user to extract the key blobs which are set to be replaced. Re-encrypt the TOE which replaces the keys. After the re-encryption is complete, boot into the debug mode again to extract the new keys. Ensure that the key that was replaced is, in fact, different from the previously extracted blob, yet still is the same size.
Findings: PASS

59. Test 4: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

60. 1. Record the storage location of the key in the TOE subject to clearing.

61. 2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

62. 3. Cause the TOE to clear the key.

63. 4. Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.

64. The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

High-Level Test Description
Not Applicable: The ST claims that non-volatile keys are destroyed by overwriting with a key of the same size (see above).
Findings: PASS

3.2.6 FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

3.2.6.1 Test

65. The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

Findings:	The TOE has two CAVP certificates related to data encryption for protected communication. They are AES #5315 which is used in IPsec and AES in certificate #A1837 which is used in TLS. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=9308 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=14284

3.2.7 FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

3.2.7.1 Test

66. The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSA2VS), "The Elliptic Curve Digital Signature Algorithm Validation System" (ECDSA2VS), and "The RSA Validation System" RSA2VS as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e., FIPS PUB 186-4). This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

Findings:	The TOE has the following CAVP certificates related to signature verification. For protected communications the TOE uses ECDSA and RSA in certificate #A1837; this certificate includes SigGen and SigVer. For trusted updates the TOE uses #C582, #C629 and RSA #2002; these certificates include SigVer. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=14284

	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10941 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10988 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=5347

3.2.8 FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

3.2.8.1 TSS

67. For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.

Findings:	[ST] 6.4.1 - The TOE implements random-bit generation services using a software-based DRBG that has been seeded with at least 256-bits of entropy from a third-party hardware-based TRNG and DRBG.

3.2.8.2 Entropy Description

68. The evaluator shall ensure the Entropy Description provides all of the required information as described in Appendix E. The evaluator assesses the information provided and ensures the TOE is providing sufficient entropy when it is generating a Random Bit String.

Findings:	[ENT] provides all the required information as described in Appendix E. The evaluator has ensured that the TOE is providing sufficient entropy when generating a Random Bit String.

3.2.8.3 Operational Guidance

69. The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected DRBG mechanism(s), if necessary.

Findings:	The evaluator used the guidance to put the TOE in the evaluated configuration and confirmed there were no options to select the DRBG mechanism.

3.2.8.4 Test

70. The evaluator shall perform 15 trials for the RBG implementation. If the RBG is configurable by the TOE, the evaluator shall perform 15 trials for each configuration. The evaluator shall verify that the instructions in the operational guidance for configuration of the RBG are valid.

71. If the RBG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random

bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "Generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-90A).

72. If the RBG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

73. The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

74. Entropy input: the length of the entropy input value must equal the seed length.

75. Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.

76. Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

77. Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

Findings:	CAVP #A1837 for a Hash_DRBG has been obtained and is consistent with the claims. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=14284

3.3 User Data Protection (FDP)

3.3.1 FDP_ACC.1 Subset access control

78. It is covered by assurance activities for FDP_ACF.1.

3.3.2 FDP_ACF.1 Security attribute based access control

3.3.2.1 TSS

79. The evaluator shall check to ensure that the TSS describes the functions to realize SFP defined in Table 2 and Table 3.

Findings:	[ST] Section 5.3.3 contains Table 19 and Table 20 which match those of the PP.

3.3.2.2 Operational Guidance

80. The evaluator shall check to ensure that the operational guidance contains a description of the operation to realize the SFP defined in Table 2 and Table 3, which is consistent with the description in the TSS.

Findings:	In order to comply with the SFP defined in Tables 2 and 3 of the [PP] the Administrator must configure available functions for each user. Section "Top Page > Security > Limiting Available Functions" [UG] allows the user to prevent unauthorized operations; you can specify who is allowed to access each of the machine's functions. By configuring this setting, you can limit the functions available to users. The TOE can place limitations on the use of the copier, document server, fax, scanner, printer, browser functions, and extended features. [UG] "Top Page > Security > Registering Administrators Before Using the Machine > Overview of the Administrator Privileges" provides a list of available functions to administrators. These settings coincide with Tables 2 and 3 in [PP].

3.3.2.3 Test

81. The evaluator shall perform tests to confirm the functions to realize the SFP defined in Table 2 and Table 3 with each type of interface (e.g., operation panel, Web interfaces) to the TOE.

82. The evaluator testing should include the following viewpoints:

- representative sets of the operations against representative sets of the object types defined in Table 2 and Table 3 (including some cases where operations are either permitted or denied)
- representative sets for the combinations of the setting for security attributes that are used in access control

High-Level Test Description
For table 2 and table 3 in the [PP], perform various operations which will exercise the various job types and show results consistent with the mandatory access control results as well as sample to show conformance with the claims in the Security Target.
Findings: PASS

3.4 Identification and Authentication (FIA)

3.4.1 FIA_AFL.1 Authentication Failure Handling

3.4.1.1 TSS

83. The evaluator shall check to ensure that the TSS contains a description of the actions in the case of authentication failure (types of authentication events, the number of unsuccessful authentication attempts, actions to be conducted), which is consistent with the definition of the SFR.

Findings:	[ST] 6.2.3 - The TOE counts consecutive login failures for a given login name and will lock out that user after an administrator-configured number of authentication failures attempts have been reached. The lockout can be released after a configured elapsed time, or by direct actions from the authorized administrator.

3.4.1.2 Operational Guidance

84. The evaluator shall check to ensure that the administrator guidance describes the setting for actions to be taken in the case of authentication failure, if any are defined in the SFR.

Findings:	In the [UG] under “Top Page > Security > Specifying the Policy on Login/Logout”, there are descriptions of how to release the lockout in “Releasing Password Lockout”.

3.4.1.3 Test

85. The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that the subsequent authentication attempts do not succeed by the behavior according to the actions defined in the SFR when unsuccessful authentication attempts reach the status defined in the SFR.

2. The evaluator shall check to ensure that authentication attempts succeed when conditions to re-enable authentication attempts are defined in the SFR and when the conditions are fulfilled.

3. The evaluator shall perform the tests 1 and 2 described above for all the targeted authentication methods when there are multiple Internal Authentication methods (e.g., password authentication, biometric authentication).

4. The evaluator shall perform the tests 1 and 2 described above for all interfaces when there are multiple interfaces (e.g., operation panel, Web interfaces) that implement authentication attempts.

High-Level Test Description
Modify the password lockout criteria. Then proceed with the following scenarios. 1) U.NORMAL and timed release: Using the Smart Operations Panel, lock out U.NORMAL by repeatedly providing a bad credential. Show that the account is locked out and cannot login through Smart Operations Panel or send a successful print job through Print Driver with the correct credential. Wait the prescribed period of time and then show that the U.NORMAL can log in again through Smart Operations Panel. 2) U.NORMAL and manual release: Using the WIM, lock out U.NORMAL by repeatedly providing a bad credential. Show that the account is locked out by attempting a login with the correct credential. Before the prescribed period of time ends, login as U.ADMIN and release the lock for the U.NORMAL. Show that the user can log in again through WIM. 3) U.ADMIN and timed release: Using the Smart Operations Panel, lock out U.ADMIN by repeatedly providing a bad credential. Show that the account is locked out and cannot login through Smart Operations Panel or WIM with the correct credential. Wait the prescribed period of time and then show that the U.ADMIN can log in again through any one of the interfaces. 4) U.ADMIN and manual release: Using the WIM, lock out U.ADMIN by repeatedly providing a bad credential. Show that the account is locked out by attempting a login with the correct credential. Before the prescribed period of time ends, login as MFP Supervisor through WIM and release the lock for the U.NORMAL. Show that the user can log in again through WIM.
Findings: PASS

3.4.2 FIA_ATD.1 User attribute definition

3.4.2.1 TSS

86. The evaluator shall check to ensure that the TSS contains a description of the user security attributes that the TOE uses to implement the SFR, which is consistent with the definition of the SFR.

Findings:	[ST] 6.2.1 - For each individual user, the TOE maintains the user attributes: username, password, user role and available functions list regardless of the authentication method for the user account.

3.4.3 FIA_PMG_EXT.1 Extended: Password Management

3.4.3.1 Operational Guidance

87. The evaluator shall examine the operational guidance to determine that it provides guidance to security administrators on the composition of passwords, and that it provides instructions on setting the minimum password length.

Findings:	The [UG] provides sound security guidance on password complexity policies in "Top Page > Security > Registering Administrators Before Using the Machine" under "Usable Characters for User Names and Passwords". This section of the manual provides information on the mechanics of changing the passwords. This section also provides a pointer to how to change the minimum length (under "Top Page > Settings > Settings for Administrator").

3.4.3.2 Test

88. The evaluator shall also perform the following test:

89. The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.

High-Level Test Description
Change the minimum length to be 15 characters via Smart Ops Panel. Attempt to set a password that is less than the minimum. Attempt to set a password that is the minimum length. Set a password which is different from the previously used password. Show that the user can login using that password and not with the old password. Attempt to change the minimum length to be 8 characters via WIM. Attempt to set a password that is less than the minimum. Attempt to set a password that covers all the conditions (lowercase, uppercase, numbers and all of the claimed special characters). Show that the user can login using that password and not with the old password.
Findings: PASS

3.4.4 FIA_UAU.1 Timing of authentication

3.4.4.1 TSS

90. The evaluator shall check to ensure that the TSS describes all the identification and authentication mechanisms that the TOE provides (e.g., Internal Authentication and authentication by external servers).

Findings:	[ST] 6.2.1 - The TOE authenticates users by checking the entered username/passwords credentials against the local user database or against an external authentication service (LDAP).

91. The evaluator shall check to ensure that the TSS identifies all the interfaces to perform identification and authentication (e.g., identification and authentication from operation panel or via Web interfaces).

Findings:	[ST] 6.2.1 - Users login to the TOE by entering their username/password credentials on the Operation Panel, on the Windows Image Monitor (WIM) login screen, or through a client's print driver or fax driver that has been configured to submit user credentials.

92. The evaluator shall check to ensure that the TSS describes the protocols (e.g., LDAP, Kerberos, OCSP) used in performing identification and authentication when the TOE exchanges identification and authentication with External Authentication servers.

Findings:	[ST] 6.2.1 - The TOE authenticates users by checking the entered username/passwords credentials against the local user database or against an external authentication service (LDAP).

93. The evaluator shall check to ensure that the TSS contains a description of the permitted actions before performing identification and authentication, which is consistent with the definition of the SFR.

Findings:	[ST] 6.2.1 - Only the following functions are accessible before the user is authenticated: Viewing user job lists, WIM Help, system status, the counter and information of inquiries, creation of fax reception jobs, and creation of print jobs.

3.4.4.2 Operational Guidance

94. The evaluator shall check to ensure that the administrator guidance contains descriptions of identification and authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces), which are consistent with the ST (TSS).

Findings:	The [UG] provides information on the Smart Operation Panel in section "Top Page > Introduction and Basic Operations > Names and Functions of the Control Panel". In addition, a discussion of the Web Image Monitor is provided in section "Top Page > Introduction and Basic Operations > Using Web Image Monitor". As per [AGD] section 3.3.1.2, The TOE is configured to do either local authentication labeled [Basic Authentication] or external authentical labeled [LDAP Authentication], using an LDAP Server in its operational environment. These are consistent with the TSS in the [ST]. LDAP can be configured as per the instructions provided in [AGD], (section 3.4.3 LDAP Server). Further information on configuring LDAP server can also be seen

under section “Top Page > Settings" to give "Top Page > Settings > Registering the LDAP Server” in [UG]. The total set of authentication mechanisms are summarized in [UG] in “Top Page > Security > Verifying Users to Operate the Machine (User Authentication)”.

3.4.4.3 Test

95. The evaluator shall also perform the following tests:

1. The evaluator shall check to ensure that identification and authentication succeeds, enabling the access to the TOE when using authorized data.

2. The evaluator shall check to ensure that identification and authentication fails, disabling the access to the TOE afterwards when using unauthorized data.

96. The evaluator shall perform the tests described above for each of the authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces).

High-Level Test Description
For each type of authentication mechanism For each type of authentication interface Log into the identified management interface using a known-good credential and logout. Login into the identified management interface using a known-bad credential and verify that the TOE denies access. Ensure the appropriate audit messages appear.
Findings: PASS

3.4.5 FIA_UAU.7 Protected authentication feedback

3.4.5.1 TSS

97. The evaluator shall check to ensure that the TSS contains a description of the authentication information feedback provided to users while the authentication is in progress, which is consistent with the definition of the SFR.

Findings:	[ST] 6.2.1 - When users enter their passwords on the Operation Panel, WIM login, a client’s print driver or fax driver that has been configured to submit user credentials, the TOE displays a sequence of dummy characters whose length is the same as that of the entered password.

3.4.5.2 Test

98. The evaluator shall also perform the following tests:

99. 1. The evaluator shall check to ensure that only the information defined in the SFR is provided for feedback by attempting identification and authentication.

100. 2. The evaluator shall perform the test 1 described above for all the interfaces that the TOE provides (e.g., operation panel, identification and authentication via Web interface).

High-Level Test Description
Log into the interactive management interface. Ensure the password field does not echo the password in the clear.
Findings: PASS

3.4.6 FIA_UID.1 Timing of identification

101. It is covered by assurance activities for FIA_UAU.1.

3.4.7 FIA_USB.1 User-subject binding

3.4.7.1 TSS

102. The evaluator shall check to ensure that the TSS contains a description of rules for associating security attributes with the users who succeed identification and authentication, which is consistent with the definition of the SFR.

Findings:	[ST] 6.2.1 - The user accounts maintained by the TOE include the security attributes: username, password, user role and available functions list. After successful login, users are authorized to perform functions according to their assigned user role (Normal User, MFP Administrator, or MFP Supervisor).

3.4.7.2 Test

103. The evaluator shall also perform the following test:

104. The evaluator shall check to ensure that security attributes defined in the SFR are associated with the users who succeed identification and authentication (it is ensured in the tests of FDP_ACF) for each role that the TOE supports (e.g., User and Administrator).

High-Level Test Description
Show the user has access to their designated attributes. For the MFP function set, show that changing the set alters the user's abilities.
Findings: PASS

3.5 Security management (FMT)

3.5.1 FMT_MOF.1 Management of security functions behavior

3.5.1.1 TSS

105. The evaluator shall check to ensure that the TSS contains a description of the management functions that the TOE provides as well as user roles that are permitted to manage the functions, which is consistent with the definition of the SFR.

106. The evaluator shall check to ensure that the TSS identifies interfaces to operate the management functions.

Findings:	[ST] 6.8.2 contains a description of the management functions that the TOE provides. The TOE restricts modification of TSF functions and TSF data to the authorized administrator roles. [ST] 6.8.2 states that management functions can be managed over the Operation Panel or the WIM.

3.5.1.2 Operational Guidance

107. The evaluator shall check to ensure that the administrator guidance describes the operation methods for users of the given roles defined in the SFR to operate the management functions.

Findings:	All management functions are described in a series of authorization matrices in [SEC]. Of vital importance is how to read the security settings which can be found in [SEC] “Top Page > Read This First > How to Read the Manuals” which provides the key needed to understand the privilege columns. - Document user list for fax and stored documents can be found in [SEC] under “Top Page > List of Operation Privileges for Settings Other than Initial Settings > List of Operation Privileges for Stored Files” which covers both stored documents and stored incoming faxes; - Available function list can be found in [SEC] under “Top Page > List of Operation Privileges for Address Books” (subsection “[User Management / Others][User Management]”) for the Ops Panel as well as in [SEC] under “Web Image Monitor: Address Book” (for the Web Image Monitor); - Audit log transfer settings are under [SEC] “Top Page > System Settings (Settings Screen Type: Standard)”, subsection “[Settings for Administrator]” for the Ops Panel; - Remote audit log configuration settings are only in the Web Image Monitor and are found in [SEC] under “Top Page > Web Image Monitor: Device Settings” subsection “[SYSLOG Transfer Setting]”; - Downloading the local audit log contents is found in [SEC] under “Top Page > Web Image Monitor: Device Settings” subsection “[Download Logs]”; - Setting the time is found in [SEC] under “Top Page > System Settings > Date/Time/Timer” subsection “[Timer]” for the Ops Panels and under [SEC] “Top Page > Web Image Monitor: Device Settings” subsection “[Date/Time]” for the Web Image Monitor; - Password policy is found in [SEC] “Top Page > List of Operations Privileges for Initial Settings (Settings Screen Type: Standard) > System Settings (Settings Screen Type: Standard) > Settings for Administrator” for the Ops Panel and [SEC] “Top Page > Web Image Monitor: Security” subsection “[Extended Security]”; - Auto logout for the Ops Panel is in [SEC] “Top Page > System Settings > [Date/Time/Timer]” subsection “[Timer]”; it can also be found in [SEC] “Top Page > Web Image Monitor: Device Settings” subsection “[Timer]”; - Auto-logout for the Web Image Monitor is in [SEC] “Top Page > Web Image Monitor: Webpage”; - Lockout and release (as related to locked users) can be found in [SEC] “Top Page > Web Image Monitor: Security” subsection “[User Lockout Policy]”;

- Fax received file storage is configured in [SEC] “Top Page > List of Operation Privileges for Initial Settings > Fax Settings > [Reception Settings]” for the Ops Panel; it cannot be configured in the Web Image Monitor;

- HDD encryption key is set only in the Ops Panel and the function is described in [SEC] “Top Page > System Settings > Settings for Administrator” subsection “[File Management]” as “[Machine Data Encryption Settings]”.

- Network settings can be configured as per [SEC] “Top Page > System Settings > [Network/Interface]” in the Ops Panel and under [SEC] “Top Page > Web Image Monitor: Network”;

- Device identity refers to the device certificate which is found in [SEC] “Top Page > System Settings” subsection “Settings for Administrator” as “[Register/Delete Device Certificate]” for the Ops Panel;

- Device certificates can also be modified in the Web Image Monitor under [SEC] “Top Page > Web Image Monitor: Security” subsection “[Device Certificate]”; and

- Installed TOE software can be modified using the firmware upgrade functions as restricted under [SEC] “Top Page > Web Image Monitor: Device Settings” subsection “[Firmware Update]”.

The privileges described above are all consistent with the claims made in FMT_MOF.1 in the [ST]. The default stance in the evaluated configuration ensures that the authorizations described in the matrices are being enforced. It is important to understand that out-of-the-box, these authorizations default to a permissive stance unless “Administrator Authentication Management” procedures are followed (as required by the consumer). These are described in [AGD] Section 3.3.1 Procedure 1 – Settings Specified using the Operation Panel.

The individual operations corresponding to the privilege descriptions above can be found on the Ops Panel and Web Image Monitor in a one-to-one manner. That is, the privilege matrix corresponds directly to the Ops Panel or the Web Image Monitor screen layouts. Additional information about the individual functions can be found in the [UG] “Top Page > Settings” by following the individual screen designations (e.g. “System Settings > Date/Time/Timer” for information about setting the date/time and the ops panel auto-logout). This documentation provides information on default values given, if any. For example, the ops panel auto logout is, out-of-the box, active and given a default value of 180 seconds.

Descriptions of managing the access control for stored documents and incoming stored faxes can be found in [UG] “Top Page > Document Server > Specifying Access Privileges for Documents Stored in Document Server”.

Documentation describing how to limit the functionality afforded users can be found in [UG] “Top Page > Security > Limiting Available Functions”.

Managing the machine HDD encryption key is described in [UG] under “Top Page > Settings > Settings for Administrator”. Additional information and rationale are provided in [UG] under “Top Page > Security > Encrypting Data to Prevent Data Leaks Caused by a Stolen or Disposed Machine”.

Fax reception settings are described in [AGD] under section 3.3.1.5 Fax Settings and further details provided in [UG] under “Top Page > Settings > Fax Settings > Reception Settings”.

Firmware installation instructions are provided in the Web Image Monitor help screen embedded within the TOE device.

3.5.1.3 Tests

108. The evaluator shall also perform the following tests:

109. 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can operate the management functions in accordance with the operation methods specified in the administrator guidance.

110. 2. The evaluator shall check to ensure that the operation results are appropriately reflected.

111. 3. The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management functions.

Note:	The set of attributes, operations and roles for this SFR are also replicated in the access control helper matrix for FMT_MTD.1. Please refer to that test for results. The steps outlined in FMT_MTD.1 include the verification of the administrator guide, and the checking of the operations results.

3.5.2 FMT_MSA.1 Management of security attributes

3.5.2.1 TSS

112. The evaluator shall check to ensure that the TSS contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.

Findings:	[ST] 6.8.3 describes the role-based access control rules.

3.5.2.2 Operational Guidance

113. The evaluator shall check to ensure that the administrator guidance contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.

114. The evaluator shall check to ensure that the administrator guidance describes the timing of modified security attributes.

Findings:	The security attributes defined in the SFR are username, available function list and user role. The [UG] specifies the ability to set a username in “Top Page > Introduction and Basic Operations > Registering a User in the Address Book and Specifying the Login Information”. The [UG] also specifies the ability to limit user functions in “Top Page > Security > Limiting Available Functions”. The ability to set a user role is specified in the [UG] section “Top Page > Security > Registering Administrators Before Using the Machine”. The evaluator verified that this is consistent with the definition of the SFR.

3.5.2.3 Test

115. The evaluator shall also perform the following tests:

116. 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to the security attributes in accordance with the operation methods specified in the administrator guidance.

117. 2. The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.

118. 3. The evaluator shall check to ensure that a user that is not part of an authorized role defined in the SFR is not permitted to perform operations on the security attributes.

Note:	The set of attributes, operations and roles for this SFR are also replicated in the access control helper matrix for FMT_MTD.1. Please refer to that test for results. The steps outlined in FMT_MTD.1 include the verification of the administrator guide, and the checking of the operations results.

3.5.3 FMT_MSA.3 Static attribute initialization

3.5.3.1 TSS

119. The evaluator shall check to ensure that the TSS describes mechanisms to generate security attributes which have properties of default values, which are defined in the SFR.

Findings:	[ST] 6.8.3 specifies that the default behaviour to access the document data is permissive for all authenticated normal users, except for the U.ADMIN user which cannot initiate document processing functions. The TOE maintains username and available function lists data for individual users, unauthenticated users sending document print of document fax to the TOE must be identified before the TOE processes the job.

3.5.3.2 Test

120. If U.ADMIN is selected, then testing of this SFR is performed in the tests of FDP_ACF.1.

Note:	U.ADMIN is selected in the SFR; therefore, testing can be found in FDP_ACF.1.

3.5.4 FMT_MTD.1 Management of TSF data

3.5.4.1 Operational Guidance

121. The evaluator shall check to ensure that the administrator guidance identifies the management operations and authorized roles consistent with the SFR.

Findings:	The guidance information required was identified in Section 3.5.1.2 of this AAR document. Please refer to that section for details.

122. The evaluator shall check to ensure that the administrator guidance describes how the assignment of roles is managed.

Findings:	The [UG] defines in “Top Page > Security > Registering Administrators Before Using the Machine” how administrative users are defined. The subsection “Overview of the Administrator Privileges” includes a note indicating “The administrators are distinguished from the users registered in the Address Book. A Login User name registered in the Address Book cannot be used as an administrator.”

123. The evaluator shall check to ensure that the administrator guidance describes how security attributes are assigned and managed.

Findings:	The guidance information required was identified in Section 3.5.1.2 of this AAR document. Please refer to that section for details.

124. The evaluator shall check to ensure that the administrator guidance describes how the security-related rules (.e.g., access control rules, timeout, number of consecutive logon failures,) are configured.

Findings:	The guidance information required was identified in Section 3.5.1.2 of this AAR document. Please refer to that section for details.

3.5.4.2 Test

125. The evaluator shall perform the following tests:

126. 1. The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to TSF data in accordance with the operation methods specified in the administrator guidance.

127. 2. The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.

128. 3. The evaluator shall check to ensure that no users other than users of the given roles defined in the SFR can perform operations to TSF data.

High-Level Test Description
For each of the defined operations from the Security Target, execute the operation as the approved user and show that the function can be performed. Execute the operation as one of the other users and show it cannot be performed.
Findings: PASS

3.5.5 FMT_SMF.1 Specification of Management Functions

3.5.5.1 TSS

129. The evaluator shall check the TSS to ensure that the management functions are consistent with the assignment in the SFR.

Findings:	[ST] 6.8.2 lists the management functions consistent with the SFR.

3.5.5.2 Operational Guidance

130. The evaluator shall check the guidance documents to ensure that management functions are consistent with the assignment in the SFR, and that their operation is described.

Findings:	The guidance information required was identified in Section 3.5.1.2 of this AAR document. Please refer to that section for details.

3.5.6 FMT_SMR.1 Security roles

3.5.6.1 TSS

131. The evaluator shall check to ensure that the TSS contains a description of security related roles that the TOE maintains, which is consistent with the definition of the SFR.

Findings:	[ST] 6.8.1 describes U.NORMAL and U.ADMIN roles which are consistent with the definition in the SFR.

3.5.6.2 Test

132. As for tests of this SFR, it is performed in the tests of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.

3.6 Protection of the TSF (FPT)

3.6.1 FPT_SKP_EXT.1 Extended: Protection of TSF Data

3.6.1.1 TSS

133. The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Findings:	[ST] 6.4.2 - All pre-shared keys, symmetric keys, and private keys are protected in storage and are not accessible to any user through TOE interfaces. A root encryption key is securely stored in IcKey (a Trusted Platform Module). No other plaintext keys are stored in non-volatile storage. The root encryption key is used to decrypt a key encryption key which is used to decrypt symmetric keys for encrypted storage and the Device Certificate. The IPsec PSK is stored in an encrypted partition of NVRAM. Key destruction is described in the Key Management Description.

3.6.2 FPT_STM.1 Reliable time stamps

3.6.2.1 TSS

134. The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.

Findings:	[ST] 6.6.1 - The date (year/month/day) and time (hour/minute/second) the TOE records for the audit log are derived from the system clock of the TOE. The system clock may be set locally or configured to use a network time server. Only an MFP Administrator can configure the system clock.

3.6.2.2 Operational Guidance

135. The evaluator shall check to ensure that the guidance describes the method of setting the time.

Findings:	The [UG] specifies how to configure the date and time in “Top Page > Settings > Date/Time/Timer”.

3.6.2.3 Test

136. The evaluator shall also perform the following tests:

137. 1. The evaluator shall check to ensure that the time is correctly set up in accordance with the guidance.

138. 2. The evaluator shall check to ensure that the time stamps are appropriately provided.

High-Level Test Description
Change the date and time locally. Verify that the changes result in appropriate audit messages and reflect the new settings.
Findings: PASS

3.6.3 FPT_TST_EXT.1 Extended: TSF testing

3.6.3.1 TSS

139. The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

Findings:	[ST] 6.9.1 describes the self-tests including an outline of what the tests are doing. During start-up, the TOE performs a series of integrity tests, that check that the hash on the executable files is correct and that the software has not been changed. The TOE performs integrity tests on the TPM, the MFP Control Software, the Fax Control unit, the Operation Panel Software, and the Operation Panel Applications. This is sufficient to ensure the TSF is operating correctly.

3.6.3.2 Operational Guidance

140. The evaluator shall also ensure that the operational guidance describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.

Findings:	The [UG] has a section on troubleshooting the MFP at “Top Page > Troubleshooting”. The troubleshooting guides provide tables which list the error code/message, the probable cause and the recommended solution or action. The TSS claims that in the event of an error, a Service Call (SC) is displayed. The troubleshooting section indicates there are two instances where such a Service Call will be issued: when the

	machine needs to be repaired or a malfunction has occurred. These two broad categories correspond to the claimed functional set in the TSS.

3.6.4 FPT_TUD_EXT.1 Extended: Trusted Update

3.6.4.1 TSS

141. The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR.

Findings:	[ST] 6.9.2 / Table 31 describes the digital signature mechanisms in use to verify software updates.

142. The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.

Findings:	[ST] 6.9.2 - TOE allows only the MFP Administrator to read the version of the MFP Control Software, Operation Panel Control Software, and Fax Control Unit Control Software. The MFP Administrator can read these versions using the Operation Panel or WIM from the client computer.

3.6.4.2 Operational Guidance

143. The evaluator shall check to ensure that the administrator guidance contains descriptions of the operation methods to obtain the TOE version as well as the operation methods to start update processing, which are consistent with the description of the TSS.

Findings:	The [AGD] specifies how to obtain the TOE version in section 2.2 Verifying the TOE. The [AGD] further specifies how the TOE is updated in section 2.4 Updating the TOE. The evaluator verified that this is consistent with the description in the TSS.

3.6.4.3 Test

144. The evaluator shall also perform the following tests:

145. 1. The evaluator shall check to ensure the current version of the TOE can be appropriately obtained by means of the operation methods specified by the administrator guidance.

146. 2. The evaluator shall check to ensure that the verification of the data for updates of the TOE succeeds using authorized data for updates by means of the operation methods specified by the administrator guidance.

147. 3. The evaluator shall check to ensure that only administrators can implement the application for updates using authorized data for updates.

148. 4. The evaluator shall check to ensure that the updates are correctly performed by obtaining the current version of the TOE after the normal updates finish.

149. 5. The evaluator shall check to ensure that the verification of the data for updates of the TOE fails using unauthorized data for updates by means of the operation methods specified by the administrator guidance. (The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.)

High-Level Test Description
Check the version of the TOE. As an unauthorized user, show that they have no rights to apply firmware updates. As an authorized user, apply a good and a known bad upgrade using the Web Image Monitor.
Findings: PASS

3.7 TOE Access (FTA)

3.7.1 FTA_SSL.3 TSF-initiated termination

3.7.1.1 TSS

150. The evaluator shall check to ensure that the TSS describes the types of user sessions to be terminated (e.g., user sessions via operation panel or Web interfaces) after a specified period of user inactivity.

Findings:	[ST] 6.2.3 - The TOE can terminate user sessions at the various interfaces as follow: Operation Panel: the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time (settable from 10 to 999 seconds). WIM: the user is logged out of the TOE when inactivity reaches the WIM auto logout time (settable from 3 to 60 minutes). Printer driver: the user is logged out of the TOE immediately after receiving the print data from the printer driver. Fax driver: the user is logged out of the TOE immediately after receiving the transmission information from the fax driver.

3.7.1.2 Operational Guidance

151. The evaluator shall check to ensure that the guidance describes the default time interval and, if it is settable, the method of setting the time intervals until the termination of the session.

Findings:	The [UG] in section “Top Page > Settings > Date/Time/Timer” specifies the configuration and default value (180 seconds) of the Auto Logout Timer. The [AGD] in section 3.3.2.6 WIM Auto Logout Settings specifies the configuration of the Web Image Monitor Auto Logout. Default value is 60.

3.7.1.3 Test

152. The evaluator shall also perform the following tests:

153. 1. If it is settable, the evaluator shall check to ensure that the time until the termination of the session can be set up by the method of setting specified in the administrator guidance.

154. 2. The evaluator shall check to ensure that the session terminates after the specified time interval.

155. 3. The evaluator shall perform the tests 1 and 2 described above for all the user sessions identified in the TSS.

High-Level Test Description
Operational Panel: For each of 1, 3 minutes: Change the idle timeout to this value; Log into the device; With 15 seconds before the timeout expires, verify the session is still alive by sending a keep alive as described above in the TSFI commands. This should reset the timeout clock. The purpose is to ensure the timeout is not premature. Wait 30 seconds. Verify the session is still alive by sending a keep alive. This should reset the timeout clock. The purpose is to ensure the timeout has been reset by the initial keep alive action above. Wait for the full duration of the timeout without sending any keep alives. The session should terminate. WIM: For 3 minute test: Change the idle timeout to this value; Log into the device; With 15 seconds before the timeout expires, verify the session is still alive by sending a keep alive (refresh page) as described above in the TSFI commands. This should reset the timeout clock. The purpose is to ensure the timeout is not premature. Wait 30 seconds. Verify the session is still alive by sending a keep alive. This should reset the timeout clock. The purpose is to ensure the timeout has been reset by the initial keep alive action above. Wait for the full duration of the timeout without sending any keep alives. The session should terminate. For 5 minute test: Change the idle timeout to this value, log into the device and wait for the full duration of the timeout without sending any keep alives. The session should terminate.
Findings: PASS

3.8 Trusted path/channels (FTP)

3.8.1 FTP_ITC.1/TLS Inter-TSF trusted channel

3.8.1.1 TSS

156. The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Findings:	SFR identifies the use of TLS for Syslog and SMTP which is described in [ST] 6.7.1.

3.8.1.2 Test

157. The evaluator shall also perform the following tests:

158. 1. The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

NOTE:	The TOE maintains trusted channels to the remote audit log, and SMTP servers, which are set up as per the evaluated configuration and are protected using TLS. These channels are constantly tested throughout the evaluation.

159. 2. For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.

High-Level Test Description
Invoke the trusted channel with a packet capture operating and verify that the channel has been initiated by the TOE. Show the data is not delivered in plaintext.
Findings: PASS

160. 3. The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.

High-Level Test Description
See previous test case.
Findings: PASS

161. 4. The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

High-Level Test Description
Start packet capture. For each of the given trusted channels, initiate a connection showing good behaviour. Then physically disconnect the line and wait for 2 minutes. Reconnect the line and show that the connection, when reestablished, continues to use the correct trusted protection mechanism.
Findings: PASS

162. Further assurance activities are associated with the specific protocols.

3.8.2 FTP_ITC.1/IPsec Inter-TSF trusted channel

3.8.2.1 TSS

163. The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Findings:	[ST] 6.7.3 - The TOE employs IPsec to protect communications between the TOE and external IT entities in the operational environment. In the evaluated configuration, it is used for communications with LDAP, syslog, NTP, SMTP, and FTP servers.

3.8.2.2 Test

164. The evaluator shall also perform the following tests:

165. 1. The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

NOTE:	The TOE maintains trusted channels to the NTP, FTP, LDAP, SMTP and Syslog servers, which are set up as per the evaluated configuration. They are constantly tested throughout the evaluation.

166. 2. For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.

High-Level Test Description
Invoke the trusted channel with a packet capture operating and verify that the channel has been initiated by the TOE. Show the data is not delivered in plaintext.
Findings: PASS

167. 3. The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.

High-Level Test Description
See previous test case.
Findings: PASS

168. 4. The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

High-Level Test Description
Start packet capture. For each of the given trusted channels, initiate a connection showing good behaviour. Then physically disconnect the line and wait for 2 minutes. Reconnect the line and show that the connection, when reestablished, continues to use the correct trusted protection mechanism. Test to see plaintext data traffic will occur when TOE tries to reestablish the IPsec tunnel again and fail (IKE lifetime ends during disconnection period) during a long disruption. During LDAP test, wait for TOE to try and reestablish the IPsec tunnel again, then initiate an LDAP traffic to see if the data bypasses the IPsec channel or not.
Findings: PASS

169. Further assurance activities are associated with the specific protocols.

3.8.3 FTP_TRP.1(a) Trusted path (for Administrators)

3.8.3.1 TSS

170. The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

Findings:	[ST] 6.7.1 - the TOE implements TLS 1.2 to protect communications between the TOE and remote users' client computers (print drivers, fax drivers, and WIM HTTPS sessions).

3.8.3.2 Operational Guidance

171. The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

Findings:	The [UG] provides instructions for logging into the Web Image Monitor at “Top Page > Introduction and Basic Operations > Logging in to Web Image Monitor”.

3.8.3.3 Test

172. The evaluator shall also perform the following tests:

173. 1. The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

Note:	The TOE maintains a remote trusted path to the TOE for the web interface which is set up as per the evaluated configuration. It is constantly tested throughout the evaluation.

174. 2. For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.

Note:	Reviewing the operational guidance, the evaluator believes that all applicable interfaces are invoked over a trusted path. The Web Image Monitor is the only remote administrative mechanism.

175. 3. The evaluator shall ensure, for each method of remote administration, the channel data are not sent in plaintext.

High-Level Test Description
Invoke the trusted path for each of the defined mechanisms and show the data is not in plaintext.
Findings: PASS

176. Further assurance activities are associated with the specific protocols.

4 Evaluation Activities for Conditionally Mandatory Requirements

4.1 Confidential Data on Field-Replaceable Nonvolatile Storage Devices

4.1.1 FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

4.1.1.1 KMD

177. The evaluator shall examine the Key Management Description (KMD) for a description of the methods used to protect keys stored in nonvolatile memory.

Findings:	The [KMD] describes in section 5 “Key purpose, protection, and derivation” how keys in non-volatile storage are protected. *Confidential details are omitted in this public AAR document.*

178. The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in nonvolatile memory.

Findings:	The [KMD] describes in section 5 “Key purpose, protection, and derivation” the location of all keys stored in non-volatile storage and their protection mechanisms. *Confidential details are omitted in this public AAR document.*

4.1.2 FCS_KYC_EXT.1 Extended: Key Chaining

4.1.2.1 TSS

179. The evaluator shall verify the TSS contains a high-level description of the BEV sizes – that it supports BEV outputs of no fewer 128 bits for products that support only AES-128, and no fewer than 256 bits for products that support AES-256.

Findings:	[ST] 6.5.1 - The REK is used to encrypt and decrypt a Key Encryption Key (KEK). The KEK is used to encrypt and decrypt Device Encryption Keys (DEKs) for the HDD and NVRAM. All such operations use 256-bit AES keys to protect 256-bit AES data encryption on the target devices.

4.1.2.2 KMD

180. The evaluator shall examine the KMD to ensure that it describes a high level description of the key hierarchy for all accepted BEVs. The evaluator shall examine the KMD to ensure it describes the key chain in detail. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap, submask combining, or key encryption.

Findings:	The keychain is described and illustrated in section 4 “Keychains” of the [KMD]. This description and illustration are sufficient to provide information on how sub-keys are protected. The keys in the chain are protected using key encryption as described in the [KMD] table in section 5. *Confidential details are omitted in this public AAR document.*

181. The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM)

This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the Key Chain.

Findings:	The keychain is described and illustrated in section 4 “Keychains” of the [KMD]. Keying material is protected as per the table in section 5 of the [KMD]. A review of how keys are unprotected for use is contained in section 4. The mechanisms are well described and provide the evaluator assurance that no keys could be recovered without performing a cryptographic exhaust. *Confidential details are omitted in this public AAR document.*

182. The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

Findings:	The [KMD] in section 7.1 “Key encryption” provides the key strengths in table 3. *Confidential details are omitted in this public AAR document.*

4.1.3 FDP_DSK_EXT.1 Extended: Protection of Data on Disk

4.1.3.1 TSS

(Modified by NIAP TD0176)

183. If the self-encrypting device option is selected, the device must be certified in conformance to the current Full Disk Encryption Protection Profile. The tester shall confirm that the specific SED is listed in the TSS, documented and verified to be CC certified against the FDE EE cPP.

Findings:	[ST] 5.3.3 - This option is not selected.

184. The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the Device and the point at which the encryption function is applied.

Findings:	[ST] 6.5.2 - All HDD data is encrypted with AES 256 CBC encryption by a hardware component. Partition 3 of NVRAM is encrypted software component, LPUX NVRAM Encryption Driver, with AES 256-bit encryption. HDD encryption is enabled and initialized in the evaluated configuration, as described in the guidance documentation. NVRAM encryption is initialized during manufacturing and cannot be disabled.

185. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes the interface(s) used by the TOE to invoke this functionality.

Findings:	N/A - crypto is not provided by the Operational Environment.

186. The evaluator shall verify that the TSS describes the initialization of the Device at shipment of the TOE, or by the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the Device. The evaluator shall verify the TSS describes areas of the Device that it does not encrypt (e.g., portions that do not contain confidential data boot loaders, partition tables, etc.). If the TOE supports multiple Device encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all Devices.

Findings:	[ST] 6.5.2 - NVRAM encryption is initialized during manufacturing and cannot be disabled. HDD encryption is enabled and initialized in the evaluated configuration, as described in the guidance documentation.

4.1.3.2 Operational Guidance

187. The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to enable the Device encryption function, including any necessary preparatory steps. The guidance shall provide instructions that are sufficient to ensure that all Devices will be encrypted when encryption is enabled or at shipment of the TOE.

Findings:	In [AGD], in section 3.3.1.1 System Settings, the user is instructed to navigate to the "Machine Data Encryption Settings" and ensure the data has been encrypted.

4.1.3.3 KMD

188. The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the Device, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions that do not contain confidential data, partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the Device's interface and the Device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine.

Findings:	The [KMD] indicates that the HDD encryption is provided by a hardware component and the NVRAM encryption is provided by a software driver. All data in the HDD are encrypted. Specific partitions in the NVRAM are encrypted as designated in [KMD] section "7.2 Data encryption". Encryption is enabled on the HDD in the evaluated configuration and is enabled during manufacturing for the NVRAM. The encryption engine hardware and software components are described and illustrated in section 2 of the [KMD]. This information shows the location of, and data path, between hardware components and software drivers. *Confidential details are omitted in this public AAR document.*

189. The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts all applicable Devices. The evaluator shall verify that the KMD describes the data flow from the interface to the Device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted area).

Findings:	[KMD] 7.2 - All data in the HDD are encrypted. All data in partition 3 in the NVRAM are encrypted. Encryption is enabled on the HDD in the evaluated configuration and is enabled during manufacturing for the NVRAM. At no time is data encryption bypassed. *Confidential details are omitted in this public AAR document.*

190. The evaluator shall verify that the KMD provides a description of the boot initialization, the encryption initialization process, and at what moment the product enables the encryption. If encryption can be enabled and disabled, the evaluator shall validate that the product does not allow for the transfer of confidential data before it fully initializes the encryption. The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.

Findings:	The [KMD] contains an illustration and description of the boot process in section 3. The description clearly shows the stages at which the encryption engine is initialized. Encryption is always enabled in the evaluated configuration. The developer is committed to providing the evaluator with tools and means to inspect the encrypted drive out-of-band during testing. *Confidential details are omitted in this public AAR document.*

4.1.3.4 Test

191. The evaluator shall perform the following tests:

192. Test 1. Write data to Storage device: Perform writing to the storage device with operating TSFI which enforce write process of User documents and Confidential TSF data.

193. Test 2. Confirm that written data are encrypted: Verify there are no plaintext data present in the encrypted range written by Test 1; and, verify that the data can be decrypted by proper key and key material.

194. All TSFIs for writing User Document Data and Confidential TSF data should be tested by above Test 1 and Test 2.

High-Level Test Description
Having performed available MFP jobs and configured and modified various administrative capabilities, extract the drive and forensically review to determine if any data is available for recovery.
Findings: PASS

4.2 PSTN Fax-Network Separation

4.2.1 FDP_FXS_EXT.1 Extended: Fax separation

4.2.1.1 TSS

195. The evaluator shall check the TSS to ensure that it describes:

196. 1. The fax interface use cases

197. 2. The capabilities of the fax modem and the supported fax protocols

198. 3. The data that is allowed to be sent or received via the fax interface

199. 4. How the TOE can only be used transmitting or receiving User Data using fax protocols

Findings:	[ST] 6.10.1 – identifies the ITU-T T.30 protocol and the required information.

4.2.1.2 Operational Guidance

200. The evaluator shall check to ensure that the operational guidance contains a description of the fax interface in terms of usage and available features.

Findings:	The [UG] provides an overview of the fax interface in section “Top Page > Fax”.

4.2.1.3 Test

201. The evaluator shall test to ensure that the fax interface can only be used transmitting or receiving User Data using fax protocols. Testing will be dependent upon how the TOE enforces this requirement. The following tests shall be used and supplemented with additional testing or a rationale as to why the following tests are sufficient:

202. 1. Verify that the TOE accepts incoming calls using fax carrier protocols and rejects calls that use data carriers. For example, this may be achieved using a terminal application to issue modem commands directly to the TOE from a PC modem (issue terminal command: ‘ATDT <TOE Fax Number>’) – the TOE should answer the call and disconnect.

High-Level Test Description
With a data fax modem listening, use the TOE to dial the modem and show that the connection is dropped as soon as non-FAX protocol data is received. Use the same data fax modem to dial the TOE and show that the TOE drops the call as soon as non-FAX protocol data is received. Try additional test cases: - Attempt to send a file over the data modem.
Findings: PASS

203. 2. Verify TOE negotiates outgoing calls using fax carrier protocols and rejects negotiation of data carriers. For example, this may be achieved by using a PC modem to attempt to receive a call from the TOE (submit a fax job from the TOE to <PC modem number>, at PC issue terminal command: ‘ATA’) – the TOE should disconnect without negotiating a carrier.

High-Level Test Description
Refer to previous test case.
Findings: PASS

4.3 Network Communications

(Modified by NIAP TD0393)

4.3.1 FTP_TRP.1(b) Trusted path (for Non-administrators)

4.3.1.1 TSS

204. The evaluator shall examine the TSS to determine that the methods of remote TOE access for non-administrative users are indicated, along with how those communications are protected.

Findings:	[ST] 6.7.1 - The TOE implements TLS 1.2 to protect communications between the TOE and remote users' client computers (print drivers, fax drivers, and WIM HTTPS sessions).

205. The evaluator shall also confirm that all protocols listed in the TSS in support of remote TOE access are consistent with those specified in the requirement, and are included in the requirements in the ST.

Findings:	[ST] 6.7.1 - The TOE implements TLS 1.2 in support of remote TOE access which is consistent with the selection specified in section 5.3.8.

4.3.1.2 Operational Guidance

206. The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

Findings:	The [AGD] document in section 3.3 Initial Configuration provides guidance for the use of the IPP-SSL driver when performing network print and fax operations. Following the instructions on the [AGD] section 3.3.2.5.3 sets the remote user sessions to encrypted communication only.

4.3.1.3 Test

207. The evaluator shall also perform the following tests:

208. 1. The evaluators shall ensure that communications using each specified (in the operational guidance) remote user access method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

Note:	The TOE maintains remote trusted paths to the TOE for the network print and fax functions which are set up as per the evaluated configuration. They are constantly tested throughout the evaluation.

2. For each method of remote access supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote user session without invoking the trusted path.

Note:	After reviewing the operational guidance, the non-administrative trusted paths (LAN FAX and network print) are only invoked over the trusted path.

209. 3. The evaluator shall ensure, for each method of remote access, the channel data are not sent in plaintext.

High-Level Test Description
For each of the non-administrative trusted paths, invoke the trusted path and show the data is not in plaintext.
Findings: PASS

210. Further assurance activities are associated with the specific protocols.

5 Evaluation Activities for Optional Requirements

5.1 Internal Audit Log Storage

5.1.1 FAU_SAR.1 Audit review

5.1.1.1 TSS

211. The evaluator shall check to ensure that the TSS contains a description that audit records can be viewed only by authorized users and functions to view audit records.

Findings:	[ST] 6.1.2 - Authorized administrators use the WIM to review the audit trail and to initiate transfer of audit records. The TOE prevents unauthorized access to the audit records by ensuring that the options to manage the audit function and the audit records are not included in the lists of available functions visible to the U.NORMAL users.

212. The evaluator shall check to ensure that the TSS contains a description of the methods of using interfaces that retrieve audit records (e.g., methods for user identification and authentication, authorization, and retrieving audit records).

Findings:	[ST] 6.1.2 - Authorized administrators use the WIM to review the audit trail and to initiate transfer of audit records.

5.1.1.2 Operational Guidance

213. The evaluator shall check to ensure that the operational guidance appropriately describes the ways of viewing audit records and forms of viewing.

Findings:	The instructions for downloading the local audit log contents are found in [UG] under “Top Page > Settings > Collecting Logs” subsection “Downloading the Logs”.

5.1.1.3 Test

214. The evaluator shall also perform the following tests:

215. 1. The evaluator shall check to ensure that the forms of audit records are provided as specified in the operational guidance by retrieving audit records in accordance with the operational guidance.

216. 2. The evaluator shall check to ensure that no users other than authorized users can retrieve audit records.

Findings:	Refer to test cases for FMT_MTD.1 which show appropriate means to retrieve the Audit records and show evidence of access control to authorized users.

217. 3. The evaluator shall check to ensure that all audit records are retrieved by the operation of retrieving audit records.

High-Level Test Description
Perform a series of auditable actions and show that all relevant records are captured both in the local audit log storage as well as in the remote audit server.

High-Level Test Description
Findings: PASS

5.1.2 FAU_SAR.2 Restricted audit review

5.1.2.1 Test

218. The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.

NOTE:	Refer to FMT_MTD.1, which specifies a subtest case explicitly to check access control of audit records to authorized users.

5.1.3 FAU_STG.1 Protected audit trail storage

5.1.3.1 TSS

219. The evaluator shall check to ensure that the TSS contains a description of the means of preventing audit records from unauthorized access (modification, deletion).

Findings:	[ST] 6.1.2 – The TOE prevents unauthorized access to the audit records by ensuring that the options to manage the audit function and the audit records are not included in the lists of available functions visible to the U.NORMAL users.

5.1.3.2 Operational Guidance

220. The evaluator shall check to ensure that the TSS and operational guidance contain descriptions of the interfaces to access to audit records, and if the descriptions of the means of preventing audit records from unauthorized access (modification, deletion) are consistent.

Findings:	The instructions for downloading the local audit log contents can be found in [UG] under “Top Page > Settings > Collecting Logs” subsection “Downloading the Logs”. The instructions for clearing the logs can be found in [UG] under “Top Page > Settings > Collecting Logs” subsection “Deleting All Logs”. All management functions are described in a series of authorization matrices in [SEC] which includes administrators who are permitted to download the local logs under “Web Image Monitor: Device Settings > [Download Logs]” and those permitted to clear the logs (a ‘Delete All Logs’ button) which is a function contained within “Web Image Monitor: Device Settings > [Logs]”.

5.1.3.3 Test

221. The evaluator shall also perform the following test:

222. 1. The evaluator shall test that an authorized user can access the audit records.

223. 2. The evaluator shall test that a user without authorization for the audit data cannot access the audit records.

Note:	Refer to FMT_MTD.1, which specifies a subtest case explicitly to check access control of audit records to authorized users.

5.1.4 FAU_STG.4 Prevention of audit data loss

5.1.4.1 TSS

224. The evaluator shall check to ensure that the TSS contains a description of the processing performed when the capacity of audit records becomes full, which is consistent with the definition of the SFR.

Findings:	[ST] 6.1.2 - When a maximum number of records is reached, the oldest records are overwritten.

5.1.4.2 Operational Guidance

225. The evaluator shall check to ensure that the operational guidance contains a description of the processing performed (such as informing the authorized users) when the capacity of audit records becomes full.

Findings:	In the [UG] under “Top Page > Settings > Collecting Logs”, there is an extensive description of how the log processing is performed. When the capacity of audit records becomes full, the log IDs are removed from the downloaded log and can be detected by the user.

5.1.4.3 Test

226. The evaluator shall also perform the following tests:

227. 1. The evaluator generates auditable events after the capacity of audit records becomes full by generating auditable events in accordance with the operational guidance.

228. 2. The evaluator shall check to ensure that the processing defined in the SFR is appropriately performed to audit records.

High-Level Test Description
Download an existing log from the TOE. Perform a series of audited actions. Download the same log file from the TOE and show that the oldest record has been overwritten.
Findings: PASS

5.2 Image Overwrite

5.2.1 FDP_RIP.1(a) Subset residual information protection

5.2.1.1 TSS

229. The evaluator shall examine the TSS to ensure that the description is comprehensive in describing where image data is stored and how and when it is overwritten.

Findings:	[ST] 6.11.1 describes where image data is stored and how and when it is overwritten. During the processing of jobs, image data is stored on the HDD. When such data is no longer needed by the user or the TOE, residual data can be overwritten using the Auto Erase Memory function.

5.2.1.2 Operational Guidance

230. The evaluator shall check to ensure that the operational guidance contains instructions for enabling the Image Overwrite function.

Findings:	This is described in [AGD] section 3.3.1.1 System Settings, specifically the Auto Erase Memory Setting, which must be configured to On and can select the level of erasure between DoD, NSA or Random Numbers.

5.2.1.3 Test

231. The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.

NOTE:	FMT_SMF.1 does not define tests for FDP_RIP.1(a) and therefore the evaluator defined a test.

High-Level Test Description
Show that the TOE is capable of overwriting used memory.
Findings: PASS

6 Evaluation Activities for Selection-based Requirements

6.1 Confidential Data on Field-Replaceable Nonvolatile Storage Devices

6.1.1 FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

6.1.1.1 TSS

232. The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for encryption.

Findings:	[ST] 6.5.1 and 6.5.2 identify the key size used for encryption as 256-bit AES keys and the mode as CBC.

6.1.1.2 Operational Guidance

233. If multiple encryption modes are supported, the evaluator examines the guidance documentation to determine that the method of choosing a specific mode/key size by the end user is described.

Findings:	No such configuration is permitted.

6.1.1.3 Test

234. The following tests are conditional based upon the selections made in the SFR.

235. AES-CBC Tests

236. AES-CBC Known Answer Tests

237. There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

238. KAT-1. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key.

239. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.

240. KAT-2. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys.

241. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption.

242. KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N].

243. To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.

244. KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128].

245. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

246. AES-CBC Multi-Block Message Test

247. The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.

248. The evaluator shall also test the decrypt functionality for each mode by decrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.

249. AES-CBC Monte Carlo Tests

250. The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:

251. # Input: PT, IV, Key

252. for i = 1 to 1000:

253. if i == 1:

CT[1] = AES-CBC-Encrypt(Key, IV, PT)

PT = IV

else:

CT[i] = AES-CBC-Encrypt(Key, PT)

PT = CT[i-1]

The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

AES-GCM Test

The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

128 bit and 256 bit keys

Two plaintext lengths. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.

Three AAD lengths. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.

Two IV lengths. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.

The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

XTS-AES Test

The evaluator shall test the encrypt functionality of XTS-AES for each combination of the following input parameter lengths:

256 bit (for AES-128) and 512 bit (for AES-256) keys

273. Three data unit (i.e., plaintext) lengths. One of the data unit lengths shall be a non-zero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported. The third data unit length shall be either the longest supported data unit length or 2^{16} bits, whichever is smaller.

274. The evaluator shall test the encrypt functionality using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt.

275. The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally.

276. The evaluator shall test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTS-AES encrypt with XTS-AES decrypt.

Findings:	AES 256 CBC with validation certificate AES #3921 is used for HDD encryption. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=5346 This CAVP certificate maps to a hardware encryption chip used for full disk encryption. The CAVP certificate shows the module was tested for AES-CBC with 256-bit keys which is consistent with the claim. AES 256 CBC with validation certificate AES #4560 is used for NVRAM encryption. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=1732 This CAVP certificate maps to a software encryption driver for the NVRAM component. It was tested for AES-CBC with 256-bit keys which is consistent with the claim.

6.1.2 FCS_COP.1(f) Cryptographic operation (Key Encryption)

6.1.2.1 TSS

277. The evaluator shall verify the TSS includes a description of the key encryption function(s) and shall verify the key encryption uses an approved algorithm according to the appropriate specification.

Findings:	[ST] 6.5.1 - AES 256 is used in CBC mode which is consistent with the approved selection.

6.1.2.2 KMD

278. The evaluator shall review the KMD to ensure that all keys are encrypted using the approved method and a description of when the key encryption occurs is provided.

Findings:	Section 7.1 of the [KMD] “Key encryption” provides information about the method used. There is a description of the point at which key decryption occurs such that the encrypted keys are suitable for use. Section 7.1 of the [KMD] further specifies that keys are encrypted at the time of generation. *Confidential details are omitted in this public AAR document.*

6.1.2.3 Test

279. The evaluator shall use tests in FCS_COP.1(d) to verify encryption.

6.2 Protected Communications

6.2.1 FCS_IPSEC_EXT.1 Extended: IPsec selected

6.2.1.1 FCS_IPSEC_EXT.1.1

(Modified by NIAP TD0157)

6.2.1.1.1 TSS

280. The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.

281. As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.

Findings:	[ST] 6.7.3 - As an SPD, four individual entries and one default entry of protect can be set by an administrator. Beginning with the first entry the packet is compared, and if it matches the entry, IPsec communication is performed. If the packet does not match the first entry, subsequent entries are tested until there is a match. If no entries match the packet, the default entry will be compared, and if it does not match, the packet is discarded. The algorithms are listed in Table 29.

6.2.1.1.2 Operational Guidance

282. The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

Findings:	The [SEC] guide provides information on how to construct the SPD entries in section "Top Page > Enhanced Network Security > Configuring IPsec Settings > IPsec Settings".

	In the [AGD], a discussion of the order of the rules is provided in section 3.3.2.5.2 Installing a certificate on an IPsec Server. Specifically, '"Settings 1" to "Settings 4" are applied in order when connecting to IPsec, and if any connection cannot be established, the settings of "Default Settings" are applied.'

283. The evaluator uses the guidance documentation to configure the TOE to carry out the following tests:

a) Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and (if configurable) allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.

High-Level Test Description
Configure IPsec tunnels to either encrypt, bypass or drop data, by using the IPsec configuration screen. Test to show that the appropriate action is taken when the tunnel is configured and activated.
Findings: PASS

b) Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.

NOTE:	The TOE's mechanism for implementing an SPD is simplistic and was fully tested in the previous test case. Either the IP is permitted, or it is not.

6.2.1.2 FCS_IPSEC_EXT.1.2

6.2.1.2.1 TSS

284. The evaluator checks the TSS to ensure it states that the VPN can be established to operate in tunnel mode and/or transport mode (as selected).

Findings:	[ST] 6.7.3 - IPsec is operated in transport mode, as set by the administrator.

6.2.1.2.2 Operational Guidance

285. The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

Findings:	Section 3.3.2.5.3 in the [AGD] specifies the use of transport mode.

6.2.1.2.3 Test

286. The evaluator shall perform the following test(s) based on the selections chosen:

1. (conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures an IPsec Peer to operate in tunnel mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.

Test not applicable:	Tunnel mode is not claimed for the TOE.

2. (conditional): If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec Peer to operate in transport mode. The evaluator configures the TOE and the IPsec Peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.

NOTE:	Only transport mode is claimed for the TOE. The High-Level Test Description for FCS_IPSEC_EXT.1.1 Test 1 specifies the testing done and the result of the testing.

6.2.1.3 FCS_IPSEC_EXT.1.3

6.2.1.3.1 TSS

287. The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no “rules” are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

Findings:	[ST] 6.7.3 - If no entries match the packet, the default entry will be compared, and if it does not match, the packet is discarded.

6.2.1.3.2 Operational Guidance

288. The evaluator checks that the operational guidance provides instructions on how to construct the SPD and uses the guidance to configure the TOE for the following tests.

Findings:	The [SEC] guide provides information on how to construct the SPD entries in section “Top Page > Enhanced Network Security > Configuring IPsec Settings > IPsec Settings” in the “Security Policy” row of the “Encryption key auto exchange settings

	items" subsection. This row is the construction of the SPD including the Apply, Bypass and Discard settings. The evaluator used these settings in the tests below.

6.2.1.3.3 Test

289. The evaluator shall perform the following test:

290. The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE's interfaces.

NOTE:	Test Case 1 for FCS_IPSEC_EXT.1.1 was constructed to cover this test as well. Refer to the High-Level Test Description for FCS_IPSEC_EXT.1.1 Test 1.

6.2.1.4 FCS_IPSEC_EXT.1.4

6.2.1.4.1 TSS

291. The evaluator shall examine the TSS to verify that the symmetric encryption algorithms selected (along with the SHA-based HMAC algorithm, if AES-CBC is selected) are described. If selected, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(g) Cryptographic Operations (for keyed-hash message authentication).

Findings:	[ST] 6.7.3 – Table 29 specifies the algorithms consistent with SFRs.

6.2.1.4.2 Operational Guidance

292. The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE to use the algorithms selected by the ST author.

Findings:	The [AGD] specifies in section 3.3.2.5.3 Cryptographic Settings that AES-128-CBC or AES-256-CBC should be used as well as SHA256, SHA384 or SHA512. This is consistent with the [ST].

6.2.1.4.3 Test

293. The evaluator shall perform the following tests:

294. The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the selected algorithms, and attempt to establish a connection using ESP. The connection should be successfully established for each algorithm.

High-Level Test Description
Configure the TOE to use a specific IKE phase 2 ciphersuite. Show that it can successfully connect to a similarly configured peer.

High-Level Test Description
Findings: PASS

6.2.1.5 FCS_IPSEC_EXT.1.5

6.2.1.5.1 TSS

295. The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.

Findings:	[ST] 6.7.3 - Only IKEv1 is implemented.

6.2.1.5.2 Operational Guidance

296. The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the following test if IKEv2 is selected.

Findings:	IKEv2 is not claimed for the TOE.

6.2.1.5.3 Test

297. (conditional): If IKEv2 is selected, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.

Test not applicable:	The ST does not claim IKEv2 for the TOE.

6.2.1.6 FCS_IPSEC_EXT.1.6

6.2.1.6.1 TSS

298. The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.

Findings:	[ST] 6.7.3 - AES 128 CBC and AES 256 CBC are specified.

6.2.1.6.2 Operational Guidance

299. The evaluator ensures that the operational guidance describes the configuration of the mandated algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to configure the TOE to perform the following test for each ciphersuite selected.

Findings:	The [AGD] specifies in section 3.3.2.5.3 Cryptographic Settings that AES-128-CBC or AES-256-CBC should be used as well as SHA256, SHA384 or SHA512. This is consistent with the [ST]. Note that phase 1 and phase 2 settings are both specified in this section but with the names used by the TOE to identify the difference.

6.2.1.6.3 Test

300. The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.

High-Level Test Description
Configure the TOE to use a specific IKE phase 1 ciphersuite. Show that it can successfully connect to a similarly configured peer.
Findings: PASS

6.2.1.7 FCS_IPSEC_EXT.1.7

6.2.1.7.1 TSS

301. The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.

Findings:	[ST] 6.7.3 - An administrator can select whether to use main mode or aggressive mode. In the evaluated configuration, only main mode is used.

6.2.1.7.2 Operational Guidance

302. If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance.

Findings:	The [AGD] specifies how to disable aggressive mode for all tunnels in section 3.3.2.5.1 IPSEC.

6.2.1.7.3 Test

303. The evaluator shall also perform the following test:

304. (conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. This test is not applicable if IKEv1 is not selected above in the FCS_IPSEC_EXT.1.5 protocol selection.

High-Level Test Description
Configure the TOE to permit IKEv1 to initiate a connection to a peer which is offering aggressive mode. Show the connection fails. Configure the non-TOE peer to initiate an aggressive mode connection to the TOE. Show the connection fails.
Findings: PASS

6.2.1.8 FCS_IPSEC_EXT.1.8

6.2.1.8.1 Operational Guidance

305. The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing so are located in the operational guidance. If time-based limits are supported, the evaluator ensures that the values allow for Phase 1 Sas values for 24 hours and 8 hours for Phase 2 Sas. Currently there are no values mandated for the number of packets or number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

306. When testing this functionality, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant Sas). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered."

Findings:	The [SEC] provides this information in section "Top Page > Enhanced Network Security > Configuring IPsec Settings > IPsec Settings". Only time-based rekeying is permitted and the valid range is 300 seconds to 48 hours for both Phase 1 and Phase 2 SAs.

6.2.1.8.2 Test

307. Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

1. (Conditional): The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is renegotiated.

Test not applicable:	The ST does not claim volume-based rekey.

2. (Conditional): The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.

High-Level Test Description
Configure the Phase 1 SA to be 86400 seconds (24 hours) (and set P2 to be 21600s as required by guidance) and show that the TOE will rekey P1 before this time limit.
Findings: PASS

3. (Conditional): The evaluator shall perform a test similar to Test 1 for Phase 2 Sas, except that the lifetime will be 8 hours instead of 24.

High-Level Test Description
Configure the Phase 1 SA to be 86400 seconds (24 hours) and set P2 to be 28800s (8 hours) and show that the TOE will rekey P2 before this time limit.
Findings: PASS

6.2.1.9 FCS_IPSEC_EXT.1.9

6.2.1.9.1 TSS

308. The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.

Findings:	[ST] 6.7.3 – In IKEv1, supported DH group is 14.

6.2.1.9.2 Test

309. The evaluator shall also perform the following test (this test may be combined with other tests for this component, for instance, the tests associated with FCS_IPSEC_EXT.1.1):

310. For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.

Note	DH group 14 is the only permitted group and IKEv1 is the only permitted IKE version. These combinations have been successfully used for all of the IPsec test cases.

6.2.1.10 FCS_IPSEC_EXT.1.10

6.2.1.10.1 TSS

311. The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in the requirement.

Findings:	[ST] 6.7.3 – peer authentication supports RSA and pre-shared key authentication. RSA is specified in Table 29.

6.2.1.10.2 Test

312. The evaluator shall also perform the following test:

313. For each supported signature algorithm, the evaluator shall test that peer authentication using that algorithm can be successfully achieved and results in the successful establishment of a connection.

High-Level Test Description
Configure the TOE IPSec connection to use RSA certificates and show the connection is successful.

High-Level Test Description
Findings: PASS

6.2.2 FCS_TLS_EXT.1 Extended: TLS selected

6.2.2.1 TSS

314. The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

Findings:	[ST] 6.7.1 – Ciphersuites are listed and match those selected in the SFR. The guidance provides specification of the use of TLS 1.2.

6.2.2.2 Test

315. The evaluator shall also perform the following test:

316. 1. The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

High-Level Test Description
Using a TLS probe, connect to the TOE as a server using the claimed ciphersuites. Using a TLS test server, force the TOE to connect as a client using the claimed ciphersuites.
Findings: PASS

317. 2. The evaluator shall setup a man-in-the-middle tool between the TOE and the TLS Peer and shall perform the following modifications to the traffic:

318. *(Modified by NIAP TD0474)* a) [Conditional: TOE is a server] Modify a byte in the data of the client's Finished handshake message, and verify that the server rejects the connection and does not send any application data.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE using a TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 ciphersuite. Modify the client's Finished handshake message and show that the TOE will terminate the connection before Application Data flows.
Findings: PASS

319. b) [Conditional: TOE is a client] Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello

handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.

High-Level Test Description
Using a Lightship developed TLS server, listen for the TOE connection. Modify the Server Hello handshake message and show that the TOE will terminate the connection if the ciphersuite does not match an expected value. The offered ciphersuite will be TLS_RSA_WITH_NULL_MD5.
Findings: PASS

320. c) [Conditional: TOE is a client] If a DHE or ECDHE ciphersuite is supported, modify the signature block in the Server's KeyExchange handshake message, and verify that the client rejects the connection after receiving the Server KeyExchange.

High-Level Test Description
Using a Lightship developed TLS server, respond to the Client Hello with a modified signature block in the Server KeyExchange. The TOE rejects the connection.
Findings: PASS

321. d) [Conditional: TOE is a client] Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data.

High-Level Test Description
Using a Lightship developed TLS server, provide a handshake with a modified Server Finished message. The TOE sends a fatal alert and does not send any application data.
Findings: PASS

6.2.3 FCS_HTTPS_EXT.1 Extended: HTTPS selected

6.2.3.1.1 TSS

322. The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack.

Findings:	[ST] 6.7.1 - TLS client authentication is not supported.

6.2.3.1.2 Test

323. Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

6.2.4 FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

6.2.4.1.1 Test

324. The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

Findings:	Refer to Table 5 in the Security Target for CAVP certificates #A1837 and HMAC #3515 appropriate for FCS_COP.1(g). https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=14284 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=9308 Certificate #A1837 indicates wolfCrypt v4.1.1's HMAC implementation was tested with SHA2-256 and SHA2-384 which is consistent with the claims for TLS. Certificate HMAC #3515 specifies that the Ricoh Cryptographic Module for IPsec v1.00's HMAC implementation was tested with SHA2-256, SHA2-384 and SHA2-512 which is consistent with the claims for IPsec.

6.2.5 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

6.2.5.1.1 TSS

325. The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported, and that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the first selection in the FIA_PSK_EXT.1.3 requirement. If the assignment is used to specify conditioning, the evaluator will confirm that the TSS describes this conditioning.

Findings:	[ST] 6.7.3 - The pre-shared key can be any length from 1 to 32 characters, and is composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). Text-based pre-shared keys of 22 characters is supported. The pre-shared key is configurable with an ASCII text string, and is conditioned using a SHA-256 hash.

326. If "bit-based pre-shared keys" is selected, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

Findings:	Bit-based pre-shared keys is not selected.

6.2.5.1.2 Operational Guidance

327. The evaluator shall examine the operational guidance to determine that it provides guidance on the composition of strong text-based pre-shared keys, and (if the

selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.

Findings:	[AGD] section 3.3.2.5.3 specifies that “PSK Text” is limited (truncated) to 32 characters; is composed of any combination of upper and lower-case characters, numbers and special characters that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. It is recommended that long “PSK Text” composed of all permitted characters should be chosen as this is considered more secure.

6.2.5.1.3 Test

328. The evaluator shall also perform the following tests:

1. The evaluator shall compose at least 15 pre-shared keys of 22 characters that cover all allowed characters in various combinations that conform to the operational guidance, and demonstrates that a successful protocol negotiation can be performed with each key.

High-Level Test Description
Modify the PSK in the TOE and show that the new PSK can be used to successfully negotiate the IPsec session. In addition, test the minimum length and maximum length of a PSK and show they are accepted. Test a key with an invalid length and show it is not accepted.
Findings: PASS

2. [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.

NOTE:	Please refer to previous test case.

3. [conditional]: If the TOE supports bit-based pre-shared keys but does not generate such keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

Test Not Applicable:	The TOE does not support bit-based keys.

4. [conditional]: If the TOE supports bit-based pre-shared keys and does generate such keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

Test Not Applicable:	The TOE does not support bit-based keys.

6.3 Trusted Update

6.3.1 FCS_COP.1(c)/L1 Cryptographic operation (Hash Algorithm)

6.3.1.1 TSS

329. The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

Findings:	[ST] sections 6.9.1 and 6.9.2 identify the hashing functions in use for digital signature verification.

6.3.1.2 Operational Guidance

330. The evaluator checks the operational guidance documents to determine that any configuration that is required to be done to configure the functionality for the required hash sizes is present.

Findings:	No such configuration is required.

6.3.1.3 Test

331. The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

332. The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.

333. Short Messages Test - Bit-oriented Mode

334. The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

335. Short Messages Test - Byte-oriented Mode

336. The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

337. Selected Long Messages Test - Bit-oriented Mode

338. The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

339. Selected Long Messages Test - Byte-oriented Mode

340. The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

341. Pseudorandomly Generated Messages Test

342. This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

Findings:	During start-up the TOE uses SHA hash implementation to verify the TOE's firmware. This includes the TPM implementation which has CAVP certificate #C715. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=31111

6.3.2 FCS_COP.1(c)/L2 Cryptographic operation (Hash Algorithm)

6.3.2.1 TSS

343. The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

Findings:	[ST] sections 6.9.1 and 6.9.2 identify the hashing functions in use for digital signature verification.

6.3.2.2 Operational Guidance

344. The evaluator checks the operational guidance documents to determine that any configuration that is required to be done to configure the functionality for the required hash sizes is present.

Findings:	No such configuration is required.

6.3.2.3 Test

345. The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be

hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test mode.

346. The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.

347. Short Messages Test - Bit-oriented Mode

348. The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

349. Short Messages Test - Byte-oriented Mode

350. The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

351. Selected Long Messages Test - Bit-oriented Mode

352. The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

353. Selected Long Messages Test - Byte-oriented Mode

354. The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

355. Pseudorandomly Generated Messages Test

356. This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

Findings:	The TOE has various hash functions which support trusted update signatures and trusted updates. This includes the following: libgwguard, v0.9.8a, SHS #3231 RICOH Cryptographic Library 2 (Java), v1.0, #C582 RICOH Cryptographic Library C, v1.2, #C629 For protected communications, CAVP certificates that cover the validation of SHA algorithms used with HMAC are: SHS #4269 and #A1837.

7 Security Assurance Requirements (APE_REQ)

7.1 Class ASE: Security Target evaluation

357. No additional assurance activities

7.2 Class ADV: Development

7.2.1 ADV_FSP.1 Basic functional specification

7.2.1.1 TSS

358. The evaluator shall confirm identifiable external interfaces from guidance documents and examine that TSS description identifies all the interfaces required for realizing SFR.

Findings:	There are only two external management interfaces provided that can be used to realize the management SFRs: the Operation Panel of the multi-function printer (MFP) and Web Image Monitor (WIM). Both external management interfaces are described in the TSS of the [ST] and in the guidance documents.

359. The evaluator shall confirm identification information of the TSFI associated with the SFR described in the TSS and confirm the consistency with the description related to each interface.

Findings:	The evaluator was able to conduct sufficient and complete testing using the existing guidance documentation and information contained in the TSS. The evaluator confirms each TSFI contains identification information and is consistent with each corresponding interface description.

360. The evaluator shall check to ensure that the SFR defined in the ST is appropriately realized, based on identification information of the TSFI in the TSS description as well as on the information of purposes, methods of use, and parameters for each TSFI in the guidance documents

Findings:	The [ST] defines the TOE's interfaces in Section 2.2.2 as follows: Operation Panel of the Multi-Function Printer (MFP) Web Image Monitor (WIM) Client Printer driver or fax driver IPsec Interface TLS Interface PSTN Fax Line The guidance documents align with the defined interfaces.

361. The assurance activities specific to each SFR are described in Section 4, and also applicable SFRs from Appendix B , Appendix C , and Appendix D , and the evaluator shall perform evaluations by adding to this assurance component.

Findings:	As shown in this document, the assurance activities from the [PP] have been performed.

7.3 Class AGD: Guidance Documents

7.3.1 AGD_OPE.1 Operational user guidance

7.3.1.1 Operational Guidance

362. The contents of operational guidance are confirmed by the assurance activities in Section 4, and applicable assurance activities in Appendix B , Appendix C , and Appendix D , and the TOE evaluation in accordance with the CEM.

363. The evaluator shall check to ensure that the following guidance is provided:

364. Procedures for administrators to confirm that the TOE returns to its evaluation configuration after the transition from the maintenance mode to the normal Operational Environment.

Findings:	By definition, maintenance mode falls outside of the evaluated configuration. In order to re-enter the evaluated configuration, the administrator can use the [AGD] to verify that the settings described in section 3.3 Initial Configuration are set properly.

7.3.2 AGD_PRE.1 Preparative procedures

7.3.2.1 Operational Guidance

365. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

Findings:	The [AGD] describes the models in section 1.3.2 Evaluated Software and Hardware. This list covers all models described in the [ST] in section 2.3.

7.4 Class ALC: Life-cycle Support

7.4.1 ALC_CMC.1 Labelling of the TOE

7.4.1.1 Operational Guidance

366. The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. The evaluator shall ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the appropriate administrative guidance) as specified in the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Findings:	The evaluator checked the TOE made available for independent testing and ensured that it includes the TOE name and version number and that these are consistent with the ST and all guidance documents. The product name is also consistent with the vendor Website.

7.4.2 ALC_CMS.1 TOE CM coverage

7.4.2.1 Operational Guidance

367. The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

Findings:	The TOE identification is in Section 1.2 in the [ST] and Section 1.3.2 of the [AGD].

7.5 Class ATE: Tests

7.5.1 ATE_IND.1 Independent testing - Conformance

7.5.1.1 Test

368. The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

369. The Test Plan identifies the product models to be tested, and for those product models not included in the test plan but included in the ST, the test plan provides a justification for not testing the models. This justification must address the differences between the tested models and the untested models, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. In case the ST describes multiple models (product names) in particular, the evaluator shall consider the differences in language specification as well as the influences, in which functions except security functions such as a printing function, may affect security functions when creating this justification. If all product models claimed in the ST are tested, then no rationale is necessary.

370. The test plan describes the composition of each product model to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each model either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE.

371. The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include the goal of the particular procedure, the test steps used to achieve the goal, and the expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

Findings:	The evaluator constructed a test plan and an equivalency argument. The equivalency argument provides the rationale for the selection of model used for actual testing. In addition, evidence was provided by the vendor showing internal QA testing covering all models. The evaluator test plan provided the necessary configuration of the TOE beyond what was required in the guidance documentation, such as configuration of external entities and any special test equipment that was needed to fulfil this. Each test case provided a step-by-step way to conduct the test, the expected results and the actual results (which were contained in external documents). Where any failures occurred, the actual results provided a journal of the activity performed until a 'pass' was achieved.

7.6 Class AVA: Vulnerability Assessment

7.6.1 AVA_VAN.1 Vulnerability survey

7.6.1.1 Test

372. As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in printing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report.

373. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability.

374. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Findings:	The following sources of public vulnerabilities were considered in formulating the specific list of flaws to be investigated by the evaluators. Hypothesis sources for public vulnerabilities were: - https://www.ricoh.com/products/security/mfp/bulletins/ - https://www.ricoh.com/info/ - NIST National Vulnerabilities Database (NVD): https://web.nvd.nist.gov/view/vuln/search - https://www.ricoh.com/products/security/vulnerabilities/ - CISA - Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog - CVE Mitre: https://cve.mitre.org/index.html

- CVEdetails.com - https://www.cvedetails.com/vulnerability-search.php

- Google

Type 1 Hypothesis searches were conducted on August 15, 2023, and included the following search terms:

- RICOH IM 2500/3000/3500/4000/5000/6000 version JE-1.10-H
- LPUX6.0 OS (customized NetBSD 6.0.1)
- wolfCrypt, v4.1.1
- WolfSSL v4.1.0t
- Web Image Monitor version 5.0.1
- Intel Atom x5-E3930
- ARM Cortex-A9 Quad Core
- MB8AL1062MH-GE1
- Boot SHA-1 Module
- Libgwguard
- RICOH Cryptographic Module for IPSec, v1.0
- ST33TPHF2ESPI
- RICOH Cryptographic Library

All potential vulnerabilities were analysed for exploitability in the TOE. The public search result can be found in Section 2 of the Vulnerability Assessment report. In addition to public searches, Type 3 Hypotheses Evaluation Team Generated are reported in Section 3. The evaluator also developed penetration tests in an effort to test and exploit potential weaknesses that were identified as a result of the search term analysis, or flaws identified by scanning tools, and other sources. Any vulnerability that was deemed to be exploitable in the TOE was patched by the vendor. At the time of writing the evaluator determined that the TOE in the evaluated configuration is not affected by any known vulnerabilities.