Xerox® VersaLink™ C625/B625 with HDD

Assurance Activity Report

Version 1.2

May 2024

Document prepared by

www.lightshipsec.com

Table of Contents

1 INTRODUCTION 3
1.1 Evaluation Identifiers 3
1.2 Evaluation Methods 3
2 TOE DETAILS 5
2.1 Overview 5
2.2 TOE Models 5
2.3 Reference Documents 5
2.4 Summary of SFRs 6
3 EVALUATION ACTIVITIES FOR SFRS 9
3.1 Security Audit (FAU) 9
3.2 Cryptographic Support (FCS) 13
3.3 User Data Protection (FDP) 38
3.4 Identification and Authentication (FIA) 44
3.5 Security management (FMT) 51
3.6 Protection of the TSF (FPT) 56
3.7 TOE Access (FTA) 59
3.8 Trusted path/channels (FTP) 60
4 SECURITY ASSURANCE REQUIREMENTS (APE_REQ) 65
4.1 Class ASE: Security Target evaluation 65
4.2 Class ADV: Development 65
4.3 Class AGD: Guidance Documents 65
4.4 Class ALC: Life-cycle Support 66
4.5 Class ATE: Tests 67
4.6 Class AVA: Vulnerability Assessment 68

1 Introduction

1 This Assurance Activity Report (AAR) documents the evaluation activities performed by Lightship Security for the evaluation identified in Table 1: Evaluation Identifiers. 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	Xerox Corporation
TOE	Xerox® VersaLink™ C625/B625 with HDD Software Version: 119.024.003.11705 / 119.025.003.11705
Security Target	Xerox® VersaLink™ C625/B625 with HDD Security Target, v1.1
Protection Profile	Protection Profile for Hardcopy Devices, v1.0
	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 *This TD is applicable as IPSec is claimed for the TOE.* TD0176 FDP_DSK_EXT.1.2 - SED Testing *This TD is not applicable as SED drives are not in scope.* TD0219 NIAP Endorsement of Errata for HCD PP v1.0 (Errata #1, June 2017)

	This TD is applicable to the TOE and the Errata is included in the Test Plan.
	TD0253 Assurance Activities for Key Transport *This TD is not applicable to the TOE as Key Transport under FCS_COP.1(i) is not claimed.*
	TD0261 Destruction of CSPs in flash *This TD applies to the TOE.*
	TD0299 Update to FCS_CKM.4 Assurance Activities *This TD applies to the TOE.*
	TD0393 Require FTP_TRP.1(b) only for printing *This TD applies to the TOE.*
	TD0474 Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1 *This TD applies to the TOE.*
	TD0494 Removal of Mandatory SSH Ciphersuite for HCD *This TD applies to the TOE.*
	TD0562 - Test activity for Public Key Algorithms *This TD applies to the TOE.*
	TD0642 FCS_CKM.1(a) Requirement; P-384 keysize moved to selection *This TD applies to the TOE. This TD supersedes NIAP TD0074.*

2 TOE Details

2.1 Overview

The TOE is a hardcopy device that copies and prints with scan and fax capabilities, commonly known as Multi-Function Device (MFD), Multi-Function Printer (MFP) or simply printer. The TOE is deployed within office environments for general copy/print/scan/fax use by non-administrative users.

2.2 TOE Models

1 The TOE includes the models listed in the table below. The TOE models vary in print speeds.

Table 3: TOE models

Model	Firmware Version	CPU / OS
VersaLink™ C625	119.024.003.11705	ARM Cortex A53 Yocto Linux 3.1
VersaLink™ B625	119.025.003.11705	

2.3 Reference Documents

Table 4: List of Reference Documents

Ref	Document
[ST]	Xerox® VersaLink™ C625/B625 with HDD Security Target, v1.1
[PP]	Protection Profile for Hardcopy Devices, v1.0 Protection Profile for Hardcopy Devices, v1.0, Errata #1
[KMD]	Xerox® VersaLink® B415 / C415 / 625 / C625 Key Management Description, Document Version: 1.4
[ENT]	Xerox® VersaLink™ B625, C625, B415, C415 Entropy Description, Document Version: 1.9
[CCGE]	Canadian Common Criteria Program Guidance for Evaluators, v5.0, December 2022
[SIG]	Secure Installation and Operation of your Xerox® VersaLink® C415, C625 Multifunction Printer Xerox® VersaLink® B415, B625 Multifunction Printer, v1.3, April 2024
[SAG]	Xerox® VersaLink® C620/B620 Single Function and VersaLink® C625/B625/C415/B415 Multifunction Printers System Administrator Guide, v1.2, September 2023 (702P09150)
[UG]	Xerox® VersaLink® B625 Multifunction Printer User Guide, v1.2, September 2023 (702P09148) Xerox® VersaLink® C625 Color Multifunction Printer User Guide, v1.1, September 2023 (702P09147)

Ref	Document
[SC]	Smart Card Installation and Configuration Guide for Xerox®, AltaLink® / VersaLink® Series, v1.0, March 25, 2024

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_STG_EXT.1	Extended: External Audit Trail Storage
FAU_STG.1	Protected 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)	Cryptographic Key Generation (Symmetric keys)
FCS_CKM.4(a)	Cryptographic Key Destruction
FCS_CKM_EXT.4	Extended: Cryptographic Key Material Destruction
FCS_COP.1(a)	Cryptographic Operation (Symmetric Encryption/Decryption)
FCS_COP.1(b)	Cryptographic Operation (for Signature Generation and Verification)
FCS_COP.1(c)	Cryptographic operation (Hash Algorithm)
FCS_COP.1(d)	Cryptographic operation (AES Data Encryption/Decryption)
FCS_COP.1(g)	Cryptographic Operation (for Keyed-hash message authentication)
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
FCS_IPSEC_EXT.1	Extended: IPsec selected
FCS_HTTPS_EXT.1	Extended: HTTPS selected
FCS_KYC_EXT.1	Extended: Key Chaining
FCS_TLS_EXT.1	Extended: TLS selected
FCS_SSH_EXT.1	Extended: SSH selected
FDP_ACC.1	Subset Access Control

Requirement	Title
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
FDP_RIP.1(b)	Subset residual information protection
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User attribute definition
FIA_PMG_EXT.1	Extended: Password Management
FIA_UAU.1	Timing of authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition
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	Inter-TSF trusted channel
FTP_TRP.1(a)	Trusted Path (for Administrators)

Requirement	Title
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

3 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] 6.2.1 specifies "The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to logged-in users, and each log entry contains a timestamp. The audit log also tracks user identification and authentication, administrator actions (including creation and modification of users and associated roles, as well as changes to the time), and failure of trusted channels. Each log entry contains a time stamp, the type of event, the user that cause the event (where applicable), and the event outcome. For failure to establish a trusted communication channel, the log entry also contains the reason for the failure." The evaluator verifies that the auditable events and recorded information are consistent with the SFR.

3.1.1.2 Operational Guidance

4 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 [SIG] in the Section "Audit Log" describes the audit logs and the information captured in the audit log; the recorded information is consistent with the SFR.

3.1.1.3 Test

5 The evaluator shall also perform the following tests:

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

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

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

Findings:	The evaluator performs actions to generate audit events identified in Table 1 of the [PP] throughout the testing of the associated SFRs and confirms that the required audit events are generated. For the FIA_UAU.1 auditable events, the evaluator ensures that the test for FIA_UAU.1 exercises all the I&A mechanisms claimed in the TSS and verifies that audit events are generated for all use of the I&A mechanisms.

3.1.2 FAU_GEN.2 User identity association

9 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

10 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] 6.2.2 specifies that "The TOE has the ability to transfer, or "push" the audit log file to a designated file server in the operational environment. This is possible via the SFTP protocol only. The audit log transfer can be set up to send daily audit log file transmissions at a specific time, or a 'send now' function can be utilized to transfer audit logs immediately." The evaluator verified that the TSS includes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. The TSS in [ST] Section 6.8.4 describes "SSH/SFTP is used to transfer audit logs to a remote log server".

11 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] 6.2.3 describes that "The TOE can store a maximum of 15,000 audit log entries. The TOE overwrites oldest events first if the maximum is reached. When the TOE reaches 13,500 entries (90% full) an email warning is sent to a set of administrator defined email addresses. Subsequent warnings will be emailed after every 15,000 entries if the audit log has not been cleared." The verified that audit log may be downloaded from MFP through the Embedded Web Server (EWS) or the Control Panel and only the Administrator has authorized access to the audit log. Section 6.2.2 states that "The audit log transfer can be set up to send daily audit log file transmissions at a specific time, or a 'send now' function can be utilized to transfer audit logs immediately."

3.1.3.2 Operational Guidance

12 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:	The [SIG] Section "SFTP Filing" describes how to configure the trusted channel for audit transfer, as well as any requirements on the audit server and TOE configuration.

3.1.3.3 Test

13 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
The evaluator establishes a successful connection to the SFTP syslog server and verifies that the audit log transfer is encrypted.
Findings: PASS

3.1.4 FAU_STG.1 Extended: External Audit Trail Storage

3.1.4.1 TSS

14 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] 6.2.3 describes that the audit log may be downloaded from the MFP through EWS or the Control Panel. The System Administrator must be logged in to download the local audit log and is the only user with authorized access to the audit log. The audit log cannot be modified. The audit log may be deleted by the System Administrator via the purge function described at section 6.10.2. Access control which prevents unauthorized access to the audit log is described in section 6.3.

3.1.4.2 Operational Guidance

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

Findings:	The [SIG] Section "Audit Log" describes how the system administrator downloads the audit log and protocol logs for review. The audit records are restricted from unauthorized access as visibility to audit features requires System Administrator authentication per section "Secure Installation and Set-up in the Evaluated Configuration" of the [SIG]. The [SAG] Section "Audit Log" provides instructions for downloading audit logs both through the EWS and Control Panel.

3.1.4.3 Test

16 The evaluator shall also perform the following tests:

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

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

High-Level Test Description
Log into the EWS as the ‘admin’ user. Go to the Audit Log section using the TSFI command above and verify the admin user has full access to audit settings and information. Logout of the EWS as the ‘admin’ user and log back in as the ‘user1’ user with “Logged-In User” permissions (default). Try to go to the same Audit Log section as before and verify that the ‘user1’ user cannot access the audit log settings.
Findings: PASS

3.1.5 FAU_STG.4 Prevention of audit data loss

3.1.5.1 TSS

19 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] 6.2.3 states ”The TOE can store a maximum of 15,000 audit log entries. The TOE overwrites oldest events first if the maximum is reached. When the TOE reaches 13,500 entries (90% full) an email warning is sent to a set of administrator defined email addresses. Subsequent warnings will be emailed after every 15,000 entries if the audit log has not been cleared.”

3.1.5.2 Operational Guidance

20 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:	The [SIG] Section “Audit Log” describes the audit log processing for sending a warning email to the administrator when the log is at 90% full.

3.1.5.3 Tests

21 The evaluator shall also perform the following tests:

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

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

High-Level Test Description
The evaluator attempts to fill the audit logs and verifies that the TOE generates an email alert once the log is 90% full and completely full. The evaluator then confirms the log is rotated once full.
Findings: PASS

3.2 Cryptographic Support (FCS)

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

24 *(Modified by NIAP TD0642)*

3.2.1.1 TSS

25 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.

26 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.

27 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] 6.6.1 describes how the TOE complies with the 800-56A and 800-56B and identifies the relevant sections in the standard which include sections on key establishment. “(a)FFC DH Group 14 (2048-bit MODP) per NIST SP 800-56Ar3 section 5.6.1.1.1 (b)RSA 2048 per NIST SP 800-56Br2 section 6 (c)ECDSA P256, P-384 and P-521 per NIST SP 800-56Ar3 section 5.6.1.2” The evaluator also verified that the TSS does not identify any TOE-specific extensions not described in the NIST publication or any alternative implementation.

3.2.1.2 Test

28 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.

Note:	The test assurance activity for FCS_CKM.1(a) is covered by the CAVP certificate A845.

3.2.2 FCS_CKM.1(b) Cryptographic Key Generation (symmetric keys)

3.2.2.1 TSS

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

Findings:	[ST] 6.6.1 Specifies that “The TOE cryptographic module implements random bit generation services using CTR_DRBG (AES) seeded with 256-bits of entropy from a hardware noise source as further described in the separate proprietary Entropy Description document.”

3.2.2.2 KMD

30 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)).

31 The KMD is described in Appendix F.

Findings:	Table 5 in Section 4 of the [KMD] indicates that the TOE incorporates its own DRBG seeded with 256-bits of entropy. Section 6.6.1 and 6.6.2 in the TSS indicates that the TOE uses CTR-DRBG and performs encryption/decryption of the user data (FCS_COP.1(d)) using AES in CBC mode and key size of 256 bits. *Confidential details are omitted in this public AAR document.*

3.2.3 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

3.2.3.1 TSS

32 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] 6.6.1 Table 18 lists all key and key materials along with description of how each key is stored, how it is protected (where applicable), when the key is no longer needed, how and when the key is expected to be destroyed.

3.2.3.2 KMD

33 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.

Findings:	Table 4 of the [KMD] identifies the keys and key materials used by the TOE and describes where they reside, and when they are no longer needed. *Confidential details are omitted in this public AAR document.*

34 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:	Table 4 of the [KMD] includes a key lifecycle. The table lists all keys and key material, how they are used, where they reside, end-of-life, and destruction method. Section 3.2 of the [KMD] includes a detailed description of key destruction. The evaluator verified that the [KMD] matches the claims made in FCS_CKM.4. *Confidential details are omitted in this public AAR document.*

3.2.4 FCS_CKM.4(a) Cryptographic key destruction

(Modified by NIAP TD0261 and TD0299)

3.2.4.1 TSS

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

36 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.

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

Findings:	[ST] 6.6.1 specifies that "Keys and keying material are securely deleted when no longer needed. Keys in volatile memory are destroyed by removal of power to the memory. For keys in non-volatile memory, when 'securely deleted' the material is overwritten with a single overwrite of the values (0x35 or 0x97)." The same section also states that "There are no known configurations or circumstances that do not conform to the key destruction requirement."

3.2.4.2 KMD

38 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:	Table 4 in Section 3.3 of the [KMD] describes how the keys stored in volatile memory are derived and used. *Confidential details are omitted in this public AAR document.*

39 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.

Findings:	Table 4 in the [KMD] lists each type of key stored in the TOE and identifies the memory type where key material is stored. *Confidential details are omitted in this public AAR document.*

40 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:	Section 3.2 of the [KMD] describes and identifies the different storage media types that the TOE utilizes to service commands to read/write memory and the types of memory. The evaluator verified that the [KMD] description supports the selection(s) made by the ST Author. *Confidential details are omitted in this public AAR document.*

3.2.4.3 Operational Guidance

41 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.

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

43 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.

44 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.

45 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 [SIG] section “Special Configuration Notes” states that there are no situations where key destruction may be delayed at the physical layer.

3.2.4.4 Test

46 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.

47 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:

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

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

50 3. Cause the TOE to clear the key.

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

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

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

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

55 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.

56 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.)

57 2. Cause the TOE to clear the key.

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

59 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:

60 1. Record the value 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 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.

64 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:

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

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

67 3. Cause the TOE to clear the key.

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

69 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
Using backchannel (serial access) verify the keys subject to deletion by overwrite by the TOE. Then proceed with generating new keys. View the same storage location to verify that the instances of the previously known key value are not found.
Findings: PASS

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

3.2.5.1 Test

70 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.

Note:	The test assurance activity for FCS_COP.1(a) is covered by the CAVP certificates A845 and A846.

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

3.2.6.1 Tests

71 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.

Note:	The test assurance activity for FCS_COP.1(b) is covered by the CAVP certificate A845.

3.2.7 FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

3.2.7.1 TSS

72 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] 6.6.4 describes cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512 that are used for TLS, IPsec, SSH, Storage encryption and trusted update (digital signature verification).

3.2.7.2 Operational Guidance

73 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:	The [SIG] Section “FIPS 140 Mode” and Section “Special Configuration Notes” page 21 include instructions for configuring the hash sizes.

3.2.7.3 Test

74 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.

75 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.

76 Short Messages Test - Bit-oriented Mode

77 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.

78 Short Messages Test - Byte-oriented Mode

79 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.

80 Selected Long Messages Test - Bit-oriented Mode

81 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 $1 \leq i \leq m$. For SHA-512, the length of the i-th message is 1024 + 99*i, where $1 \leq i \leq m$. 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.

82 Selected Long Messages Test - Byte-oriented Mode

83 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 $1 \leq i \leq m/8$. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where $1 \leq i \leq m/8$. 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.

84 Pseudorandomly Generated Messages Test

85 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.

Note:	The test assurance activity for FCS_COP.1(c) is covered by the CAVP certificate A845.

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

3.2.8.1 TSS

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

Findings:	The TSS in [ST] 6.6.2 describes key sizes (128-bits, 256-bits) and mode (CBC, GCM) used for encryption.

3.2.8.2 Operational Guidance

87 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:	The [SIG] Section “Data Encryption” indicates that by default the MFP uses AES-CBC-256. No additional cryptographic settings are configurable in the TOE for data encryption.

3.2.8.3 Test

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

89 **AES-CBC Tests**

90 <u>AES-CBC Known Answer Tests</u>

91 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.

92 **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.

93 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.

94 **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.

95 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.

96 **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].

97 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.

98 **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].

99 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.

100 AES-CBC Multi-Block Message Test

101 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.

102 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.

103 AES-CBC Monte Carlo Tests

104 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:

105 # Input: PT, IV, Key

106 for i = 1 to 1000:

107 if i == 1:

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

109 PT = IV

110 else:

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

112 PT = CT[i-1]

113 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.

114 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.

115 AES-GCM Test

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

117 128 bit and 256 bit keys

118 **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.

119 **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.

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

121 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.

122 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.

123 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.

124 XTS-AES Test

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

126 256 bit (for AES-128) and 512 bit (for AES-256) keys

127 **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.

128 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.

129 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.

130 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.

Note:	The test assurance activity for FCS_COP.1(d) is covered by the CAVP certificate A845.

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

3.2.9.1 Test

131 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.

Note:	The test assurance activity for FCS_COP.1(g) is covered by the CAVP certificate A845.

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

3.2.10.1 TSS

132 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:	The TSS in [ST] 6.6.1 describes that “The TOE cryptographic module implements random bit generation services using CTR_DRBG (AES) seeded with 256-bits of entropy from a hardware noise source” The evaluator verified that this statement is consistent with the selection in FCS_RBG_EXT.1.2.

3.2.10.2 Entropy Description

133 The evaluator shall ensure the Entropy Description provides all 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:	The Entropy Description provides all required information and has been approved for this evaluation.

3.2.10.3 Operational Guidance

134 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 [SIG] Section “FIPS 140 Mode” includes a statement that DRBG selection is not configurable in the TOE.

3.2.10.4 Test

135 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.

136 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).

137 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.

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

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

140 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.

141 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.

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

Note:	The test assurance activity for FCS_RBG_EXT.1 is covered by the CAVP certificate A845.

3.2.11 FCS_IPSEC_EXT.1 Extended: IPsec selected

3.2.11.1 FCS_IPSEC_EXT.1.1

(Modified by NIAP TD0157)

3.2.11.1.1 TSS

143 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.

144 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] 6.8.5 describes that the TOE implements an IPsec Security Policy Database (SPD) and allows configuration to discard, bypass, and protect packets. The SPD which consists of these policies is consulted during the processing of all traffic, both inbound and outbound. As a packet is analyzed, the policies are consulted in order and the first matched policy will be used to process the traffic, and the associated action applied. For the evaluated configuration, only inbound connections are supported for reception and handling of print jobs; outbound connections for transmission of scan jobs are not supported. A final policy is configured such that any non-matching packet results in the packet being discarded. The algorithms are described in section 6.8.5 in the [ST].

3.2.11.1.2 Operational Guidance

145 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 [SIG] Section "IPsec" provides the instructions for configuring the SPD rules for packets processing and covers all 3 cases and the ordering of rules. The [SIG] details are consistent with the TSS and the evaluator followed these instructions to configure the SPD for testing.

3.2.11.1.3 Test

146 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
Create a BYPASS, BLOCK and PASS policy and verify that these policies are enacted in order.
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.

Findings:	Refer to Test 1.

3.2.11.2 FCS_IPSEC_EXT.1.2

3.2.11.2.1 TSS

147 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] 6.8.5 states that "Both transport and tunnel mode are supported and are configuration options when configuring up IPsec."

3.2.11.2.2 Operational Guidance

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

Findings:	The [SIG] in Section “IPsec” describes the IPsec settings configurable in the TOE including the settings for tunnel or transport mode.

3.2.11.2.3 Test

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

150 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.

High-Level Test Description
The evaluator configures tunnel mode for IPsec on the TOE and successfully connects using tunnel mode. The evaluator then configures transport mode on the TOE then successfully connects using transport mode.
Findings: PASS

151 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.

Findings:	FCS_IPSEC_EXT.1.1 Test 1 shows the results of this test.

3.2.11.3 FCS_IPSEC_EXT.1.3

3.2.11.3.1 TSS

152 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] 6.8.5 — The TSS describes that packets are processed against the SPD. For the evaluated configuration, “A final policy is configured such that by default any non-matching packet results in the packet being discarded.”

3.2.11.3.2 Operational Guidance

153 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 [SIG] Section “IPsec” describes the IPsec settings that are configurable in the TOE.

3.2.11.3.3 Test

154 The evaluator shall perform the following test:

155 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.

Findings:	All the actions were tested in FCS_IPSEC_EXT.1.1 Test 1.

3.2.11.4 FCS_IPSEC_EXT.1.4

3.2.11.4.1 TSS

156 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] 6.8.5 states that “The IPsec ESP protocol is implemented in conjunction with AES-CBC-128 and AES-CBC-256 together with the following SHA-based HMAC algorithms: HMAC-SHA2-256 and HMAC-SHA-384.” identified in FCS_COP.1(g).

3.2.11.4.2 Operational Guidance

157 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 [SIG] Section “IPsec” describes the IPsec settings that are configurable in the TOE.

3.2.11.4.3 Test

158 The evaluator shall also perform the following tests:

159 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
The evaluator successfully connects to the TOE via IPsec using each ESP algorithm claimed.
Findings: PASS

3.2.11.5 FCS_IPSEC_EXT.1.5

3.2.11.5.1 TSS

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

Findings:	[ST] 6.8.5 — The TSS states that the TOE implements IKEv1.

3.2.11.5.2 Operational Guidance

161 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:	The [SIG] Section “IPsec” includes instructions for configuring the IPsec settings. The TOE is configured to use IKEv1.

3.2.11.5.3 Test

162 (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.

Findings:	N/A. IKEv2 is not selected.

3.2.11.6 FCS_IPSEC_EXT.1.6

3.2.11.6.1 TSS

163 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] 6.8.5 states that the TOE uses AES-CBC-128, AES-CBC-256 for encrypting the IKEv1 payload.

3.2.11.6.2 Operational Guidance

164 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 [SIG] Section “IPsec” describes the settings for configuring the mandated algorithms.

3.2.11.6.3 Test

165 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
The evaluator successfully connects to the TOE via IPsec using each IKE algorithm claimed.
Findings: PASS

3.2.11.7 FCS_IPSEC_EXT.1.7

3.2.11.7.1 TSS

166 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] 6.8.5 — The TSS description includes a statement that “IKEv1 is implemented with main mode only for phase 1 key exchanges. Aggressive mode is not supported.”

3.2.11.7.2 Operational Guidance

167 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 [SIG] Section “IPsec” describes the IPsec settings configurable in the TOE. The mode is not configurable in the TOE; it is set by default.

3.2.11.7.3 Test

168 The evaluator shall also perform the following test:

169 (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
The evaluator attempts to connect to the TOE using IPsec and confirms that this attempt is dropped by the TOE.
Findings: PASS

3.2.11.8 FCS_IPSEC_EXT.1.8

3.2.11.8.1 Operational Guidance

170 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.

171 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 [SIG] Section "IPsec" describes the IPsec settings for configuring the SA lifetimes for IKEv1. The section contains instructions for configuring the SA. Time-based limits are supported and allow for Phase 1 SA values of 24 hours and 8 hours for Phase 2 SAs. The evaluator followed the [SIG] instructions for configuring the SA lifetimes during testing.

3.2.11.8.2 Test

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

173 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.

Findings:	This test is not applicable because number of bytes is not implemented by the TOE.

174 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.

175 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
The evaluator verifies that the Phase 1 and Phase 2 SAs are renegotiated after 24 and 8 hours, respectively.
Findings: PASS

3.2.11.9 FCS_IPSEC_EXT.1.9

3.2.11.9.1 TSS

176 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] 6.8.5 states that "DH Group 14(2048-bit MODP), DH Group 19 (256-bit Random ECP), and DH Group 20 (384-bit Random ECP) are the only DH groups allowed."

3.2.11.9.2 Test

177 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):

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

High-Level Test Description
The evaluator successfully connected to the TOE using each of the supported DH groups.
Findings: PASS

3.2.11.10 FCS_IPSEC_EXT.1.10

3.2.11.10.1 TSS

179 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] 6.8.5 — The TSS contains a description of the IKE peer authentication process which uses RSA algorithm as well as pre-shared keys. “The TOE can be configured to perform peer authentication using RSA certificates along the DH mode configured (DH group 14) during IKE Phase 2. If the TOE is configured to use RSA, the TOE will perform peer authentication using a device authentication certificate and a server validation certificate. The administrator can configure the TOE to use either RSA digital certificates or pre-shared keys for peer authentication by creating an IP policy rule in the TOE’s IP Security Policy.”

3.2.11.10.2 Test

180 The evaluator shall also perform the following test:

181 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
The evaluator successfully establishes an IPsec connection using RSA digital certificates.
Findings: PASS

3.2.12 FCS_HTTPS_EXT.1 Extended: HTTPS selected

3.2.12.1.1 TSS

182 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] 6.8.2 —The TSS describes that "The TOE's EWS interface is accessed via HTTPS, in this case the TOE is a HTTPS/TLS server. TOE users access EWS via a web browser and authenticate as described section 6.1. TLS client authentication is not supported."

3.2.12.1.2 Test

183 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.

3.2.13 FCS_KYC_EXT.1 Extended: Key Chaining

3.2.13.1 TSS

184 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] 6.7.2 – specifies that "The TOE generates a 256-bit BEV for disk encryption."

3.2.13.2 KMD

185 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:	[KMD] Section 3.1 describes how the key chain process functions in detail. The BEV is generated by the TOE DRBG which is then transformed into the DEK by means of a SHA-256 hash (which neither adds nor subtracts any cryptographic strength). *Confidential details are omitted in this public AAR document.*

186 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:	[KMD] Section 3.1 describes how the key chain process functions and includes a diagram. The key chain process shows no point where the chain could be broken; the effective strength of the BEV is maintained throughout the key chain and the BEV is protected within the TPM. *Confidential details are omitted in this public AAR document.*

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

Findings:	[KMD] Section 3.1 states the generated BEV is 256-bits and the chain is extended with a SHA-256 hash (which neither adds nor subtracts any cryptographic strength). *Confidential details are omitted in this public AAR document.*

3.2.14 FCS_TLS_EXT.1 Extended: TLS selected

(Modified by NIAP TD0474)

3.2.14.1 TSS

188 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] 6.8.3 - The TSS describes that the TOE implements TLS 1.2 and lists supported ciphersuites that are identical to the listing in the SFR. [SIG] section “Transport Layer Security (TLS):” contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.

3.2.14.2 Test

189 The evaluator shall also perform the following test:

190 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
The evaluator attempted a TLS connection using each of the claimed TLS ciphersuites. For each attempt, the evaluator observes a successful connection.
Findings: PASS

191 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:

192 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.

193 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.

194 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.

195 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
The evaluator attempts a TLS connection to the TOE with a modified byte in the client's handshake message and verifies that the connection fails. The evaluator attempts a TLS connection from the TOE to a TLS server offering a ciphersuite in the Server Hello message that is not supported by the TOE and verifies that the connection fails. The evaluator attempts a connection from the TOE to a TLS server with a modified signature block in the Server's Key Exchange message and verifies that the connection fails. The evaluator attempts a connection from the TOE to a TLS server with a modified Server Finished message and verifies that the connection fails.
Findings: PASS

3.2.15 FCS_SSH_EXT.1 Extended: SSH selected

3.2.15.1 FCS_SSH_EXT.1.1

None

3.2.15.2 FCS_SSH_EXT.1.2

3.2.15.2.1 TSS

196 The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSH_EXT.1.5, and ensure that password-based authentication methods are also allowed.

Findings:	[ST] 6.8.4 identifies the supported public key algorithms ssh_rsa, ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384. Password-based authentication methods are also allowed. All public key algorithms supported by the TOE are found in FCS_SSH_EXT.1.5.

3.2.15.2.2 Test

197 The evaluator shall also perform the following tests:

198 1. The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance.

199 2. Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.

High-Level Test Description
The evaluator successfully establishes an SSH connection using password-based authentication. The evaluator then successfully establishes an SSH connection using public key algorithm.
Findings: PASS

3.2.15.3 FCS_SSH_EXT.1.3

3.2.15.3.1 Test

200 The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.

High-Level Test Description
The evaluator attempts an SSH connection for less than the large packet threshold and verifies the connection succeeds. The evaluator then attempts an SSH connection with a packet greater than the large packet threshold and verifies the connection fails. An audit event is generated for the failed connection.
Findings: PASS

3.2.15.4 FCS_SSH_EXT.1.4

3.2.15.4.1 TSS

201 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms 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 SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

Findings:	[ST] 6.8.4 - The TSS description indicates “SSH/SFTP is used to transfer audit logs to a remote log server.” The evaluated verified that this description does not specify optional characteristics and the identified encryption algorithms are identical to those identified in the SFR. [SIG] section “Audit Log:” contains instructions on configuring the TOE so that SSH/SFTP conforms to the description in the TSS. No additional configuration is needed for conformance.

3.2.15.4.2 Test

202 The evaluator shall also perform the following test:

203 The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

High-Level Test Description
The evaluator connected to the SFTP server using each of the claimed encryption algorithms.
Findings: PASS

3.2.15.5 FCS_SSH_EXT.1.5

(Modified per NIAP TD0562)

3.2.15.5.1 TSS

204 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the public key algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the public key algorithms 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 SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

Findings:	[ST] 6.8.4 identifies the supported public key algorithms. The public key algorithms specified in the TSS are identical to those listed in the component (ssh_rsa, ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384.). This description does not specify optional characteristics. [SIG] section “Audit Log:” contains instructions on configuring the TOE so that SSH/SFTP conforms to the description in the TSS. No additional configuration is needed for conformance.

3.2.15.5.2 Test

205 The evaluator shall also perform the following test:

206 The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

High-Level Test Description
The evaluator established an SSH connection using each of the public key algorithms.
Findings: PASS

3.2.15.6 FCS_SSH_EXT.1.6

3.2.15.6.1 TSS

207 The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that that list corresponds to the list in this component. The evaluator shall also check the operational guidance to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).

Findings:	[ST] 6.8.4 – Data integrity algorithms used for SSH connections are hmac-sha2-256 and hmac-sha2-512. This list is consistent with the integrity algorithms claimed in FCS_SSH_EXT.1.6. [SIG] section “Audit Log:” contains instructions on configuring the TOE so that SSH/SFTP conforms to the description in the TSS. No additional configuration needed for conformance.

3.2.15.6.2 Test

208 The evaluator shall also perform the following test:

209 The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

High-Level Test Description
The evaluator established an SSH connection using each of the integrity algorithms.
Findings: PASS

3.2.15.7 FCS_SSH_EXT.1.7

210 *(Modified per NIAP TD0494)*

3.2.15.7.1 Operational Guidance

211 The evaluator shall check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.

Findings:	The [SIG] Section “SFTP Filing” includes a statement that the SSH cryptographic algorithms are not configurable in the TOE.

3.2.15.7.2 Test

212 The evaluator shall also perform the following test:

213 1. [Conditional: TOE is a client] The evaluator shall configure an SSH server to permit all allowed key exchange methods. For each allowed key exchange method, the evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt succeeds.

High-Level Test Description
The evaluator established an SSH connection using each of the key exchange methods.
Findings: PASS

214 2. [Conditional: TOE is a server] The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.

215 3. [Conditional: TOE is a server] For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.

Findings:	Tests 2 and 3 are not applicable because the TOE only acts as an SSH client.

3.3 User Data Protection (FDP)

3.3.1 FDP_ACC.1 Subset access control

216 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

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

Findings:	[ST] 6.3.2 provides a high-level description of the access control SFP. [ST] 5.3.3 contains Table 13 and Table 14 which match those of the [PP]

3.3.2.2 Operational Guidance

218 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. [SAG] Section “User Permissions” allows the administrator 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, scanner, printer, fax, email and other features.

3.3.2.3 Test

219 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.

220 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
Verify that Unauthenticated users can send a print job to the TOE but need valid user credentials on the LUI to release the job. Verify that Normal users can create a print job, a scan job, a fax job, and a copy job. Verify that Admin users can create and delete all job types. Verify that Job Owner users can create all jobs and delete their own jobs.
Findings: PASS

3.3.3 FDP_DSK_EXT.1 Extended: Protection of Data on Disk

3.3.3.1 TSS

221 *(Modified by NIAP TD0176)*

222 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:	N/A - This option was not selected.

223 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] 6.7.1 states that the TOE makes use of block-level software encryption and the Mocana cryptographic library to perform transparent disk encryption.

224 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 – The TOE includes a single cryptographic module: Mocana Cryptographic Library (v7.0.0f) that it uses for all cryptographic services.

225 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] 6.7.1 states that the drive encryption is enabled by default as shipped from the factory. Details on the disk encryption implementation and unencrypted/encrypted partitions are provided in the KMD.

3.3.3.2 Operational Guidance

226 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:	[SIG] Section “Data Encryption” describes that encryption is enabled by default. There is no additional setup to enable encryption.

3.3.3.3 KMD

227 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:	[KMD] Section 2.1 includes a high-level block diagram of the TOE architecture and a table of the encrypted/unencrypted partitions and mount points. Section 2.2 describes the data encryption engine and provides details of its implementation. The description includes a diagram showing the main components within the TOE. *Confidential details are omitted in this public AAR document.*

228 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:	Table 5 in Section 4 of the [KMD] includes a statement that encryption is enabled by default. [KMD] Section 2 explains the boot process and data encryption/decryption process. In addition, section 2 of the [KMD] identifies the unencrypted disk partitions. *Confidential details are omitted in this public AAR document.*

229 The evaluator shall verify 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:	[KMD] Section 2.3 describes the boot initialization process. Encryption is enabled by default. *Confidential details are omitted in this public AAR document.*

3.3.3.4 Test

230 The evaluator shall perform the following tests:

231 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.

232 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.

233 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
Connect to the TOE via serial cable and start a Tera Term session. Login as root.

High-Level Test Description
Send a Secure Print Job to the TOE. Copy a string from the job's binary data and search the string with the TOE disk encrypted and decrypted. Send a Delayed Fax Job from the TOE. Copy a string from the job's binary data and search the string with the TOE disk encrypted and decrypted. Send a Copy Job from the TOE that is unable to print, due to lack of resources (no paper). Copy a string from the job's binary data and search the string with the TOE disk encrypted and decrypted. Send a Scan Job from the TOE with the Build Option enabled. Copy a string from the job's binary data and search the string with the TOE disk encrypted and decrypted.
Findings: PASS

3.3.4 FDP_FXS_EXT.1 Extended: Fax separation

3.3.4.1 TSS

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

235 1. The fax interface use cases

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

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

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

Findings:	The evaluator verified that the TSS in [ST] 6.9.1 describes the fax interface, how it is used, the supported fax protocols, what data can be transmitted via the fax interface, and how the TOE prevents interconnection between the PSTN and the internal network.

3.3.4.2 Operational Guidance

239 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 [SIG] Section "Embedded Fax" describes the settings for the fax interface.

3.3.4.3 Test

240 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:

241 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.

242 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
Use the ATDT command in a Tera Term session with the modem to send a data carrier fax call to the TOE. Verify the TOE disconnects without negotiating a carrier. Send a fax call from the TOE and answer the call with the ATA command from the modem. Verify the TOE disconnects without negotiating a carrier.
Findings: PASS

3.3.5 FDP_RIP.1(a) Subset residual information protection

3.3.5.1 TSS

243 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:	The evaluator verified that the TSS in [ST] 6.10.1 provides a comprehensive description of the Image Overwrite function. The immediate image overwrite security function can also be invoked manually by the system administrator. A standard image overwrite, overwrites all files written to temporary storage areas of the HDD; a full image overwrite, overwrites those files as well as fax mailbox/dial directory and scan to mailbox data. The description also covers when image data is overwritten.

3.3.5.2 Operational Guidance

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

Findings:	The [SIG] Section "Immediate Image Overwrite" describes the settings for configuring Image Overwrite function.

3.3.5.3 Test

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

3.3.6 FDP_RIP.1(b) Subset residual information protection

3.3.6.1 TSS

246 The evaluator shall examine the TSS to ensure that the description is comprehensive in describing what customer-supplied data is to be purged, where it is stored, and how it is made unavailable.

Findings:	The evaluator verified that the TSS in [ST] 6.10.2 describes the purge function and covers all data to be purged including all jobs that are actively in progress or that are stored on the TOE for later processing; all customer data stored in address books and accounting database. The TOE will reformat the hard drive at the completion of the purge function.

3.3.6.2 Operational Guidance

247 The evaluator shall check to ensure that the operational guidance contains instructions for initiating the Purge Data function.

Findings:	The [SIG] Section “Erase Customer Data” redirects Administrators to follow the instructions in “Erase Customer Data” Section of the [SAG] in order to restore the device to factory-installed values.

3.3.6.3 Test

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

3.4 Identification and Authentication (FIA)

3.4.1 FIA_AFL.1 Authentication Failure Handling

3.4.1.1 TSS

249 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] 6.1.2 - Authentication failures handled by the TOE on EWS and Control Panel interfaces are described. The information includes the number of unsuccessful authentication attempts to trigger a lockdown and the duration of this lockdown.

3.4.1.2 Operational Guidance

250 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:	The [SIG] Section “Authentication Failure Handling” describes the settings for authentication failure handling.

3.4.1.3 Test

251 The evaluator shall also perform the following tests:

252 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.

253 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.

254 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).

255 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
After 4 minutes and 30 seconds of inactivity, attempt to log into the TOE's EWS using the correct password. The attempt should fail. This is to confirm the lockout did not expire prematurely.
After 5 minutes of inactivity, log into the TOE device EWS using the correct password. The attempt should succeed.
Repeat above for LUI.
Using the EWS, log into the TOE device 5 times using an incorrect password. On the sixth attempt, log in correctly and verify that the threshold has been reached and that the user cannot log in.
Using the LUI log into the TOE with the correct password for the locked-out user. Verify that the user cannot log in.
After 5 minutes of inactivity, log into the TOE device LUI using the previously locked out user with the correct password. The attempt should succeed.
Change lockout period time to 10 minutes. Continue testing to verify that the change is applied.
Using the LUI log into the TOE device 5 times using an incorrect password. On the sixth attempt, log in correctly and verify that the threshold has been reached and that the user cannot log in.
Using the LUI log into the TOE with another user with the correct password after 5m 30s. Verify that the LUI is locked out for all users with the new threshold.
Using the EWS log into the TOE with a non-locked out user with the correct password. Verify that the user is not locked out of the EWS.
After 10 minutes, using LUI, log into the TOE with the previously locked user with the correct password. The attempt should succeed.
Findings: PASS

3.4.2 FIA_ATD.1 User attribute definition

3.4.2.1 TSS

256 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] 6.3.1 – The TSS describes that the TOE maintains username, password and role security attributes for each individual user. This is consistent with the SFR definition.

3.4.3 FIA_PMG_EXT.1 Extended: Password Management

3.4.3.1 Operational Guidance

257 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 [SIG] Section "Authentication Passwords" provides instructions for password management including password composition and minimum password length.

3.4.3.2 Test

258 The evaluator shall perform the following tests:

259 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
Update the 'testuser' user with the password "test". Log into the EWS as the admin and update the password policy to "Level 2: Elevated". The minimum password length will be changed to 8 characters and will require a capital letter and a numerical character. Log out of the admin account and log back in with the "testuser" account. When prompted to enter a new password, try the password "Password". This should fail, as expected. Try the password "Passw0rd". This should work, as expected. Repeat the same process as above but change the password policy on the EWS to "Level 3: High". This will require 15 characters and all character types. Try the password 'Passw0rd!@#$123'. This should work, as expected. Change the password policy back to "Level 1: Basic" and test the following passwords to verify that they are accepted: qwertyuiop[]\ 1234567890-= asdfghjkl;' zxcvbnm,./ ZXCVBNM<? ASDFGHJKL:" QWERTYUIOP{}\| !@#$%^&*()_+ The passwords above were selected to represent all supported characters as specified by the [ST]. Attempt to use the illegal character '>' in the password and verify that this rejected.
Findings: PASS

3.4.4 FIA_UAU.1 Timing of authentication

3.4.4.1 TSS

260 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] 6.1.1 – the TSS describes local authentication, network authentication (LDAP server), smart card authentication (Windows Domain Controller).

261 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] 6.1.1 – The TOE performs identification and authentication at the Control Panel and the EWS.

262 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] 6.8.5 – The TOE uses IPsec for communication with the Windows domain controller for Smart Card authentication and Kerberos over IPsec to protect this communication. [ST] 6.8.3 - The TOE uses TLS for communication with LDAP server.

263 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] 6.1.1 – The TSS specifies that “The only operations permitted prior to successful identification and authentication are job requests received via printing protocols” .

3.4.4.2 Operational Guidance

264 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:	[SIG] Section “Authentication” describes the methods of authentication used by the TOE to include local or internal authentication and external authentication with remote LDAP server. [SAG] sections "Configuring Network Authentication Settings" and "Configuring Local Authentication Settings" also cover that the LUI and the WebUI authenticate users with username/password mechanism, and the LUI can also perform smart card authentication.

3.4.4.3 Test

265 The evaluator shall also perform the following tests:

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

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

268 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
Log into the identified management interface using a known-good credential and logout. Attempt to log into the identified management interface using a known-bad credential and verify that the operator cannot log into the TOE. Ensure the appropriate audit messages appear.
Findings: PASS

3.4.5 FIA_UAU.7 Protected authentication feedback

3.4.5.1 TSS

269 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] 6.1.3 – The TSS specifies that “When a user enters a password, asterisks are displayed to obscure the password.”. This is consistent with the claim made in FIA_UAU.7.

3.4.5.2 Test

270 The evaluator shall also perform the following tests:

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

272 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 EWS interface. Ensure the password field only echos asterisks, as claimed by the [ST]. Log into the LUI interface. Ensure the password field only echos asterisks, as claimed by the [ST].
Findings: PASS

3.4.6 FIA_UID.1 Timing of identification

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

3.4.7 FIA_USB.1 User-subject binding

3.4.7.1 TSS

274 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:	The TSS in [ST] 6.3.1 describes the rules for associating security attributes with users. The level of access for the authenticated users is based on their assigned role. This is consistent with the claims made in FIA_USB.1.

3.4.7.2 Test

275 The evaluator shall also perform the following test:

276 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
Log into the TOE and verify each defined role and their privileges for U.ADMIN and U.NORMAL.
Findings: PASS

3.4.8 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

3.4.8.1 TSS

277 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] 6.8.5 – The TOE supports text-based pre-shared keys of 22 characters. The text-based pre-shared key sequence entered by the user is initially conditioned using a SHA-256 hash and then encrypted with AES 256 algorithm. This is consistent with the claims made in FIA_PSK_EXT.1.

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:	The evaluator verified that the ST claims text-based pre-shared keys and no other pre-shared key to use for IPsec.

3.4.8.2 Operational Guidance

278 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:	[SIG] Section "Authentication Passwords" provides guidance on the composition of strong text-based password and allowable length. [SAG] section "Creating a New Action" under "IPsec" specifies to use complex and long key for improved security when configuring pre-shared key for IPsec authentication.

3.4.8.3 Test

279 The evaluator shall also perform the following tests.

280 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.

281 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.

282 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.

283 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.

High-Level Test Description
Test 15 different pre-shared keys in an IPsec connection and verify that each connection is successful. 15 PSKs, each 22 characters in length: 1. n3Buqe$4ep6AfazafrAtra 2. Hb$^3rJ#WEcRk80s%BvCP3 3. ^-YTPGH*2vJh5-e^6D89-J 4. 8^Hmh6vd@!YvW*T&Y7Fz!D 5. !CnSE^ttn2Dtn*d*5%LpyL 6. PnNjN&7qvARC#XcPKx83xs 7. pFST!s!jsS%B6G)7eCBv6k

High-Level Test Description
8. WX!dNwADCtV(CBY)pH88rD 9. zC6$eGCGP4Z@vu5d$t@Yap 10. (a6qSJV2P%*WkSPLdb#C)@ 11. pcDZ3vG)83QBt2eSBc!T)A 12. m8)fT@@57sS-N-yVY4zjr(13. 2SGw$jaADst9#npQK9U(C! 14. kdqkLXBYNPZg2hWW&W9F2* 15. jTufwx$UxA_5b%MeT*BwM4 Test with the pre-shared key 'ThisIsA32CharacterKey!ForTesting' to verify that the 32 character maximum value is successful. Test with the pre-shared key '12345678901234' to verify that the 14 character minimum value is successful. Try inputting an empty pre-shared key on the TOE and verify that this fails. Try inputting an 13 character pre-shared key on the TOE and verify that this fails. Try inputting a pre-shared key which exceeds the maximum length limit of 32 characters and verify that this fails to be accepted.
Findings: PASS

3.5 Security management (FMT)

3.5.1 FMT_MOF.1 Management of security functions behavior

3.5.1.1 TSS

284 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.

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

Findings:	[ST] 6.4.1 references Table 16 for a description of the management functions provided by the TOE. The table outlines the operations that can be performed for each management function and makes clear that only the system administrator can access the listed management functions. The EWS and LUI interfaces are used to manage the TSF and are defined in section 6.1.1 of the [ST]. This is consistent with the claims made in FMT_MOF.1.

3.5.1.2 Operational Guidance

286 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:	The following sections in the [SIG] describe the operation methods for the admin to operate the management functions:

	- “Secure Installation and Set-up in the Evaluated Configuration” - “Evaluated Configuration” - “Secure Operation of Device Services/Functions Part of the Evaluated Configuration” The remaining management functions are described in the [SAG] in sections “Software Upgrade Files”, “Configuring Email Settings at The Control Panel” and “SMTP Server”. All the management functions described in the [ST] are covered in the sections of the [SIG] and [SAG] above.

3.5.1.3 Test

287 The evaluator shall also perform the following tests:

288 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.

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

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

High-Level Test Description
For these events the evaluator performed the actions necessary to generate the audit event and confirmed the event was successfully generated. The activities were performed in **FMT_MOF.1** for management functions.
Findings: PASS

3.5.2 FMT_MSA.1 Management of security attributes

3.5.2.1 TSS

291 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] 6.3.2 and 6.4.1 describe the role-based access control rules. This is consistent with the claims made for FMT_MSA.1.

3.5.2.2 Operational Guidance

292 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.

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

Findings:	The [SIG] sections “Authentication Passwords”, “‘Administrator Password” and “Authorization” describe the possible operations on security attributes. Except for the login password that can be modified by the owning user, all security attributes are

	managed by U.ADMIN. The description also covers the timing of modified security attributes.

3.5.2.3 Test

294 The evaluator shall also perform the following tests:

295 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

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

297 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.

High-Level Test Description
Log into the EWS as the ‘admin’ user. Navigate to the User Roles section and create a new role. Assign ‘testuser’ to the role. Create another new role. Once it is created, delete the new role. Verify that the ‘admin’ user can query the new role, modify the new role, and delete the new role. Logout of the EWS as the ‘admin’ user. Log into the EWS as the ‘testuser’ user and verify that this user cannot reach the User Roles section.
Findings: PASS

3.5.3 FMT_MSA.3 Static attribute initialization

3.5.3.1 TSS

298 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] 6.3.2 describes the access configuration for the different types of jobs and the security attributes that have default values. Certain users can access the TOE without authentication and perform print jobs while other types of access require different security attributes such U.NORMAL and U.ADMIN. This is consistent with the claims made for FMT_MSA.3.

3.5.3.2 Test

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

3.5.4 FMT_MTD.1 Management of TSF data

3.5.4.1 Operational Guidance

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

Findings:	[SIG] Section ”Secure Operation of Device Services/Functions Part of the Evaluated Configuration” and “Evaluated Configuration”, and [SAG] Section “Setting Copy Presets” describe the management of TSF data. This covers all TSF data and management operations identified in Table 15 of the [ST].

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

Findings:	The [SIG] Section “Authorization” describes how the role assignment is managed.

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

Findings:	The [SIG] Section “Authorization” describes how security attributes are assigned and managed.

303 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 [SIG] describes the security-related rules. It covers the access control rules in the “Authentication Passwords” section; timeout is covered in the section “Session Inactivity Timeout” and user lockout is described in the section “Authentication failure handling”.

3.5.4.2 Test

304 The evaluator shall perform the following tests:

305 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.

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

307 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
Log into the EWS using a U.NORMAL account and verify that the following functions are performed accordingly: Modify login password for the authenticated user: **Covered by tests in FMT_MOF.1** Send a Print Job (EWS): **Covered by tests in FDP_ACF.1 and FTP_TRP.1(b)** Send a Copy Job (LUI): **Covered by tests in FDP_ACF.1** Send a Fax Job (EWS and LUI): **Covered by tests in FDP_ACF.1**

High-Level Test Description
Send a Scan Job (EWS and LUI): **Covered by tests in FDP_ACF.1** Log into the EWS using a U.ADMIN account and verify that the following functions are performed accordingly: Modify, Change default for authenticated user roles to copy, print, scan, or fax: **Covered by tests in FMT_MSA.1** Modify login password for the System Administrator: **Covered by tests in FMT_MOF.1** Query or Modify the behavior of Audit Log settings: **Covered by tests in FCS_SSH_EXT.1 and FAU_STG_EXT.1** Modify, query, or delete X.509 (TLS) certificates: **Covered by tests in FCS_CKM.4** Modify, query, or delete IP filter table rules: **Covered by tests in FMT_MOF.1** Modify, query, or delete email addresses for fax forwarding. Verify that the U.NORMAL user does not have the ability to perform any of the admin functions listed above.
Findings: PASS

3.5.5 FMT_SMF.1 Specification of Management Functions

3.5.5.1 TSS

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

Findings:	The TSS in [ST] 6.4.1 references Table 16 for the management functions, so the TSS description is consistent with the SFR.

3.5.5.2 Operational Guidance

309 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 following sections in the [SIG] describe the operations defined in the SFR: - “Secure Installation and Set-up in the Evaluated Configuration” - “Evaluated Configuration” - “Secure Operation of Device Services/Functions Part of the Evaluated Configuration” The remaining management functions are described in the [SAG] in sections “Software Upgrade Files”, “Configuring Email Settings at The Control Panel” and “SMTP Server”. The management functions are consistent with the assignment in the SFR.

3.5.6 FMT_SMR.1 Security roles

3.5.6.1 TSS

310 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:	The TSS in [ST] 6.3.1 describes U.ADMIN and U.NORMAL roles defined by the SFR.

3.5.6.2 Test

311 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_KYP_EXT.1 Extended: Protection of Key and Key Material

3.6.1.1 KMD

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

Findings:	All keys in non-volatile memory are encrypted using the DEK. The TOE uses the TPM to store the BEV which is used to create the DEK.

313 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 TOE uses the TPM to store the BEV which is used to create the DEK. All other keys are stored encrypted by the DEK on either the eMMC or the HDD.

3.6.2 FPT_SKP_EXT.1 Extended: Protection of TSF Data

3.6.2.1 TSS

314 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] 6.6.1 - The TSS in Table 18 describes how all cryptographic keys are stored and protected in the TOE. “The TOE does not allow users or the System Administrator, through any customer provided interface, to view or obtain any pre-shared key, private key, or symmetric key.” Pre-shared keys, symmetric keys and private keys are protected using encryption.

3.6.3 FPT_STM.1 Reliable time stamps

3.6.3.1 TSS

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

Findings:	[ST] 6.2.4 specifies that “During initial device configuration the initial date and time are set. The TOE maintains the date and time to provide reliable timestamps. The TOE can also be configured to synchronize time with an NTP server in the operational environment.”

3.6.3.2 Operational Guidance

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

Findings:	The [SIG] Sections “Date and Time” and “NTP” describe the methods of setting the time on the TOE.

3.6.3.3 Test

317 The evaluator shall also perform the following tests:

318 1. The evaluator shall check to ensure that the time is correctly set up in accordance with the guidance or external network services (e.g., NTP).

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

High-Level Test Description
Set the time manually and save settings. Create an audit record to verify that the time stamp is appropriately provided. Using the TSFI command above, change the date/time manually. Setup an NTP server to synchronize the time with the TOE. Synchronize the TOE with the NTP server and verify that the time syncs correctly and that the timestamps are accurate.
Findings: PASS

3.6.4 FPT_TST_EXT.1 Extended: TSF testing

3.6.4.1 TSS

320 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] Section 6.5.1 describes the self-tests ran during the TOE start-up: Cryptographic Module Verification and Trusted Boot. The TSS includes an argument that these tests are sufficient to demonstrate that the TSF is operating correctly by verifying the TSF's code integrity along with verifying the correct operation of the cryptographic modules.

3.6.4.2 Operational Guidance

321 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 [SIG] Section "Special Configuration Notes" describes the possible errors that may result from the self-tests that are run by the TSF.

3.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

3.6.5.1 TSS

322 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:	The TSS in [ST] 6.5.2 describes that the TOE performs signature verification to verify software for update. This is consistent with the SFR.

323 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:	The TSS in [ST] 6.5.2 specifies that "The System Administrator may view the current version of TOE firmware via EWS or the Control Panel and may initiate updates to TOE firmware via EWS."

3.6.5.2 Operational Guidance

324 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 evaluator verified that the [SIG] Section "Secure Acceptance" describes the operation methods to obtain the TOE version via EWS and Control Panel. The [SAG] Section "Software Upgrade Files" describes the operation methods for update processing. The evaluator confirmed that the descriptions are consistent with the description of the TSS.

3.6.5.3 Test

325 The evaluator shall also perform the following tests:

326 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.

327 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.

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

329 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.

330 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
Get the current version of the TOE. Attempt to install a legitimate version of the TOE and verify that this succeeds. After the installation, get the current version of the TOE and ensure it is consistent with the newly installed version. Modify the DLM Signature of the DLM file to verify that the TOE rejects this update due to an invalid DLM.
Findings: PASS

3.7 TOE Access (FTA)

3.7.1 FTA_SSL.3 TSF-initiated termination

3.7.1.1 TSS

331 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:	The TSS in [ST] 6.1.2 describes that user session timeout for both the LUI (operation panel) and EWS (Web Interfaces) can be configured by the administrator and include a default setting.

3.7.1.2 Operational Guidance

332 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 [SIG] Section “Session Inactivity Timeout” describes the settings for configuring user session timeout for both the LUI and EWS. The default settings are 60 seconds for the LUI and 60 minutes for EWS.

3.7.1.3 Test

333 The evaluator shall also perform the following tests:

334 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.

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

336 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
For 1 minute (Local UI) and 6 minutes (Web UI): Change the idle timeout to this value; Log into the device; Wait for the full duration of the timeout without sending any keep alives. The session should terminate. For 2 minutes (Local UI) and 10 minutes (Web UI): Change the idle timeout to this value; Log into the device; 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 Inter-TSF trusted channel

3.8.1.1 TSS

337 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:	The TSS in [ST] 6.8 describes the trusted channels communication between the TOE and other authorized IT identities. The TOE uses TLS for communication with LDAP server, SSH for communication with external audit server, and IPsec for communication with a domain controller for smart card authentication. The evaluator confirmed that the operational guidance, [SIG] section "Special Configuration Notes", contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

3.8.1.2 Test

338 The evaluator shall also perform the following tests:

339 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.

340 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.

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

342 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
The evaluator successfully connects to the audit server via SSH and observes via a packet capture that the communication is encrypted (already captured under FAU_STG_EXT.1). The evaluator then disconnects the audit server and attempts a connection to the audit server and verifies that the attempt fails, and the packet capture shows that no plaintext data was sent. The evaluator then observes the TOE's audit trail for an audit event for the failure to establish the session. The evaluator then reconnects the audit server and attempts a connection to the audit server from the TOE. The evaluator observes via the packet capture that the communication is encrypted. The evaluator successfully authenticates to the TOE as a smart card user and observes via a packet capture that the TOE communicates with the domain controller and LDAP server via IPsec and the communication is encrypted. The evaluator then disconnects the domain controller and LDAP server and attempts to authenticate to the TOE as a smart card user and verifies that the attempt fails, and the packet capture shows that no plaintext data was sent. The evaluator then observes the TOE's audit trail for an audit event for the failure to establish the session. The evaluator then reconnects the domain controller and LDAP server and successfully authenticates to the TOE as a smart card user. The evaluator observes via the packet capture that the communication is encrypted. The evaluator successfully authenticates to the TOE as an LDAP user and observes via a packet capture that the TOE communicates with the LDAP server via LDAPS(TLS) and the communication is encrypted. The evaluator then disconnects the LDAP server and attempts to authenticate to the TOE as an LDAP user and verifies that the attempt fails, and the packet capture shows that no plaintext data was sent. The evaluator then observes the TOE's audit trail for an audit event for the failure to establish the session. The evaluator then reconnects the LDAP server and successfully authenticates to the TOE as an LDAP user. The evaluator observes via the packet capture that the communication is encrypted. The evaluator successfully connects to the remote file repository via TLS and observes via a packet capture that the communication is encrypted. The evaluator then disconnects the remote file repository and attempts a connection to the remote file repository and verifies that the attempt fails, and the packet capture shows that no plaintext data was sent. The evaluator then observes the TOE's audit trail for an audit event for the failure to establish the session. The evaluator then reconnects the remote file repository and attempts a connection to the remote file repository from the TOE. The evaluator observes via the packet capture that the communication is encrypted. The evaluator successfully connects to the SMTP server via TLS and observes via a packet capture that the communication is encrypted. The evaluator then disconnects the SMTP server and attempts a connection to the SMTP server and verifies that the attempt fails, and the packet capture shows that no plaintext data was sent. The evaluator then observes the TOE's audit trail for an audit event for the failure to establish the session. The evaluator then reconnects the SMTP server

High-Level Test Description
and attempts a connection to the SMTP server from the TOE. The evaluator observes via the packet capture that the communication is encrypted.
Findings: PASS

343 Further assurance activities are associated with the specific protocols.

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

3.8.2.1 TSS

344 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] 6.8.1 and 6.8.3 describe that EWS is used for remote administration and access to EWS is protected via TLS/HTTPS. This is consistent with the requirement that TLS/HTTPS be used to protect communication between the TOE and remote administrators.

3.8.2.2 Operational Guidance

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

Findings:	The [SIG] Section “Establishing a Remote Session” describes how to establish remote administrative sessions to the EWS via HTTPS. The [SAG] Section “Accessing the Embedded Web Server as a System Administrator” provides instructions for establishing remote access to the EWS. The TOE uses TLS/HTTPS for access to EWS.

3.8.2.3 Test

346 The evaluator shall also perform the following tests:

347 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.

348 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 session without invoking the trusted path.

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

High-Level Test Description
Engage Wireshark over the appropriate interface. Log into the trusted path.

High-Level Test Description
Examine Wireshark and verify that the trusted path sends encrypted traffic after any initial plaintext protocol negotiation occurs.
Findings: PASS

350 Further assurance activities are associated with the specific protocols.

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

351 *(Modified by NIAP TD0393)*

3.8.3.1 TSS

352 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] 6.8 describes that the TOE implements TLS 1.2 in support of remote TOE access to EWS; uses IPsec to protect communication with all remote print clients.

353 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] 6.8 describes that the TOE implements TLS 1.2 in support of remote TOE access to EWS; uses IPsec to protect communication with all remote print clients which are consistent with the selection specified in section 5.3.8.

3.8.3.2 Operational Guidance

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

Findings:	The [SIG] Section “Establishing a Remote Session” describes how to establish remote user sessions. [SIG] Section “Transport Layer Security (TLS)” provides instructions for configuring TLS. The TOE uses TLS/HTTPS for access to EWS. [SIG] Section “IPsec” indicates that the TOE uses IPsec to secure print job communications.

3.8.3.3 Test

355 The evaluator shall also perform the following tests:

356 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.

357 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.

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

High-Level Test Description
Engage Wireshark over the appropriate interface. Log into the trusted path. Examine Wireshark and verify that the trusted path sends encrypted traffic after any initial plaintext protocol negotiation occurs.
Findings: PASS

359 Further assurance activities are associated with the specific protocols.

4 Security Assurance Requirements (APE_REQ)

4.1 Class ASE: Security Target evaluation

360 No additional assurance activities

4.2 Class ADV: Development

4.2.1 ADV_FSP.1 Basic functional specification

4.2.1.1 TSS

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

362 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.

363 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.

364 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:	The evaluator reviewed the guidance documentation to catalog the identifiable TSFIs. The TSS identifies the external interfaces that implement the security features of the TOE including the user/administrator interfaces WebUI also called EWS and the LUI, as well as the protocol interfaces to external IT entities including audit log server, LDAP server, Windows domain controller, and print clients via SSH/SFTP, HTTPS, TLS and IPsec. The TSS describes how the TOE implements each SFR. The description of security behavior at the TSFIs is consistent with the SFR claims.

4.3 Class AGD: Guidance Documents

4.3.1 AGD_OPE.1 Operational user guidance

4.3.1.1 Operational Guidance

365 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.

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

367 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:	The [SIG] in Section "FIPS 140 Mode" describes how the administrator can confirm that the TOE is in its evaluated configuration and in the [SIG] Section "Special Configuration Notes" specifies for the administrator to periodically review the configuration and verify that the proper evaluated configuration is maintained.

4.3.2 AGD_PRE.1 Preparative procedures

4.3.2.1 Operational Guidance

368 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:	All MFP platforms claimed in the ST are covered by the guidance provided.

4.4 Class ALC: Life-cycle Support

4.4.1 ALC_CMC.1 Labelling of the TOE

4.4.1.1 Operational Guidance

369 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:	Table 1 in the [ST] identifies the Xerox printer model devices and firmware/software version that meets the requirements of the [ST]. The TOE devices provided for testing are labeled with the model numbers included in the [ST] and the firmware/software version is consistent with the [ST]. Xerox advertises the Xerox VersaLink printers and the information in the [ST] is sufficient to distinguish the TOE product from the other Xerox products.

4.4.2 ALC_CMS.1 TOE CM coverage

4.4.2.1 Operational Guidance

370 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 ST and AGD identifies all hardware and firmware components that comprise the TOE. The evaluator confirmed that the multi-function printer device models that were provided for testing were the models covered in the TOE Description section of the [ST] and that these printer devices had the firmware of the versions specified in Table 1: Evaluation identifiers in the [ST]. The evaluator also confirmed that the cryptographic module claimed in the CAVP certificates is included in the TOE.

4.5 Class ATE: Tests

4.5.1 ATE_IND.1 Independent testing - Conformance

4.5.1.1 Test

371 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.

372 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.

373 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.

374 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 models 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.

4.6 Class AVA: Vulnerability Assessment

4.6.1 AVA_VAN.1 Vulnerability survey

4.6.1.1 Test

375 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.

376 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.

377 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: - Xerox Bulletins: https://security.business.xerox.com/en-us/documents/bulletins/ - Xerox Products – VersaLink C625: https://security.business.xerox.com/en-us/products/versalink-c625-2/ - Xerox Products – VersaLink B625: https://security.business.xerox.com/en-us/products/versalink-b625/ - NIST National Vulnerabilities Database: https://nvd.nist.gov/vuln/search - Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ - CISA - Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog - CVEdetails.com: https://www.cvedetails.com/vulnerability-search.php - CCCS - Alerts and advisories: https://cyber.gc.ca/en/alerts-advisories - Apache: https://httpd.apache.org/security/vulnerabilities_24.html Type 1 Hypothesis searches were conducted several times during the course of the evaluation, and were last performed on March 12, 2024, and included the following search terms:

	- VersaLink C625/B625 with HDD (version 119.024.003.11705 / 119.025.003.11705) - Yocto Linux 3.1.2 - Mocana 7.0.0f - Apache 2.4.46 - openldap 2.4.59 - libssh2 1.10.0 - ARM Cortex-A53 Dual Core - Infineon SLB9672 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. 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.