Security Target for the Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet Gateway product

Document No. 1531-002-D000

Version 0.41, 5 January 2009

Prepared for:

General Dynamics Canada
1020 - 68th Avenue NE
Calgary, Alberta
Canada T2E 8P2

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
55 Metcalfe St., Suite 1600
Ottawa, Ontario
K1P 6L5

Security Target for the Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet Gateway product

Document No. 1531-002-D000

Version 0.41, 5 January 2009

<Original> Approved by:

Project Engineer (ST Author):	Steve Jackson / Grant Gibbs	5 January 2009
Project Manager:	Mark Gauvreau	5 January 2009
Program Director:	Erin Connor	5 January 2009
	(Signature)	(Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

1.1.1 ST Title:

Security Target for the Tactical Network-layer Gateway (2E2 IA): a GD Canada MESHnet Gateway product

1.1.2 ST Version Number:

Version 0.41

1.1.3 ST Publication Date:

5 January 2009

1.1.4 ST Authors:

Steve Jackson and Grant Gibbs, EWA-Canada.

1.2 TOE IDENTIFICATION

This document is the Security Target (ST) for the General Dynamics Canada Ltd (GDC) Tactical Network-layer Gateway (TNG) as detailed in Table 1.

Product	Firmware Version	Hardware Version
TNG (Headquarters (HQ))	2E2 IA	CORE: 723975-908 ISDN: 723974-908 DTMF: 723973-903
TNG Equipment Management System (TEMS)	TNG SysMan Release 2E2 IA	N/A

Table 1 - TOE Identification Details

These products are collectively termed the TNG.

This ST defines the security and assurance requirements for a combined hardware, firmware and software TOE which includes the TNG hardware and firmware as well as management software (TNG Equipment Management System (TEMS)).

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005 (CCMB-2005-08-001, CCMB-2005-02-002, and CCMB-2005-02-003).

1.3 OVERVIEW

The TNG is part of a family of products that provide secure routers for connecting networks (referred to as MESHnet). The connected networks may transmit a variety of information via the TNG including both voice and data. The transmitted information may include both secure and insecure data or voice transmissions.

1.4 CC CONFORMANCE

The TOE is conformant with the identified functional requirements specified in Part 2 of the CC. The TOE is also conformant to the assurance requirements for Evaluation Assurance Level (EAL) 2, as specified in Part 3 of the CC, with the following augmentation:

- ALC_FLR.1 – Basic Flaw Remediation

1.5 CONVENTIONS

1.5.1 Operations

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets and italicised text, e.g., [*selected item*].
- Assignment: Indicated by surrounding brackets and regular text, e.g., [assigned item].
- Refinement: Indicated by underlined text, e.g., refined item for additions or strikethrough text, e.g., ~~refined item~~ for deleted items.
- Iteration: Indicated by assigning a number at the functional component level, e.g., "FDP_ACC.1(1), Subset access control" and "FDP_ACC.1(2) Subset access control".

The markings are relative to the requirements statements in the CC.

1.6 TERMINOLOGY

The following terminology is used in this ST:

Attack Potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Controlled Subject	Entity under control of the TOE Security Policy (TSP).

2 TARGET OF EVALUATION DESCRIPTION

2.1 PHYSICAL DESCRIPTION

The TNG is system-independent gateway system. There are four types of objective Network Access Units (oNAUs) which can be combined together to create a TNG installation:

a. TNG(Core): oNAU providing Ethernet network connections;
Note: TNG(Core) can also be configured to run either OSPF or BGP-4.

b. TNG(ISDN): oNAU providing the Integrated Services Digital Network (ISDN) Primary Rate and Basic Rate interfaces;

c. TNG(DTMF): oNAU providing Dual Tone Multi-Frequency (DTMF) interfaces; and

d. TNG(Fw): oNAU providing firewall functionality for data at an application-level as well as and as opposed to merely a secure router configuration. The firewall application on the oNAU provides for access control of communications and information flow using application-level proxy and packet filtering functionality. This component of TNG is considered to be outside the Target of Evaluation (TOE) boundary. Refer to separate Security Target for the Sidewinder G2 Security Appliance Models EAL4+ with Medium PP Compliance, version 7.0.0.02).

In general, the TNG has two separate elements, which can be deployed together, or separately:

a. TNG(HQ): consisting of the TNG(Core), TNG(ISDN) and TNG(DTMF) oNAUs; and

b. TNG(Fw).

However, nothing precludes a different mix of oNAUs to suit deployment needs, nor the use of a TNG oNAU standalone (TNG(DTMF) is an example of this).

Figure 1 depicts a typical TNG(HQ) configuration of 3 TNG oNAUs and a management terminal.

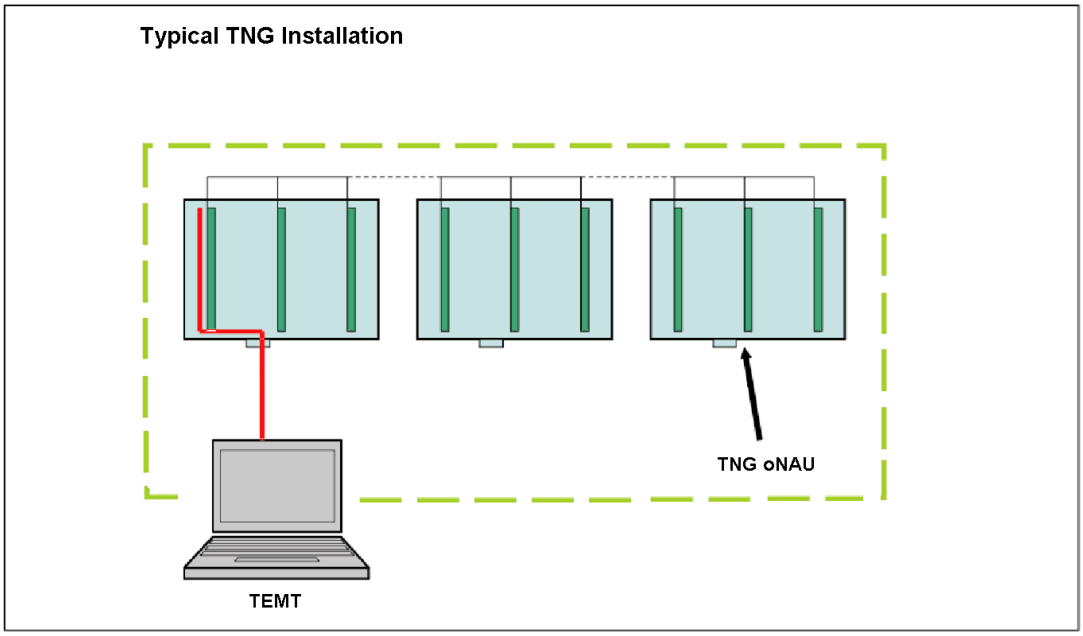

Figure 1 - Typical TNG Installation

2.2 EVALUATED CONFIGURATION

The evaluated configuration of the TOE consists of one or more TNG devices (hardware and software), plus the TEMS software. The IT environment supporting the evaluated configuration of the TOE consists of a Panasonic Toughbook workstation running the Windows 2000 Professional (Service Pack 4) operating system. However, any hardware platform capable of running this operating system could be used in the IT environment as the management workstation hosting the TEMS software. The TOE developer provides detailed guidance for the secure configuration of the management workstation (TEMT).

2.3 LOGICAL DESCRIPTION

The logical interfaces providing connectivity with the two TNG-supported networks and interfaces are described below and shown in Figure 2.

2 wire DTMF	TNG provides configurable Dual Tone Multi-Frequency (DTMF) ports for connecting 2-wire telephones.
Ethernet	TNG provides configurable 10/100/1000 Mbps Ethernet ports for interconnection with data devices and other networks.
ISDN BRI	TNG provides configurable Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) ports for ISDN telephones. It can also be connected to BRI network with the BRI interface acting as a local subscriber (ISDN terminal) or gateway interface (similar to PRI).
ISDN PRI	TNG provides configurable ISDN Primary Rate Interface (PRI) ports (E1, TacISDN, STANAG 4578, and QSig) for interconnect with other networks and communications systems.
TNG(Fw)	Through its Ethernet interface, TNG will maintain an interface with the application-level firewall [TNG(Fw)].

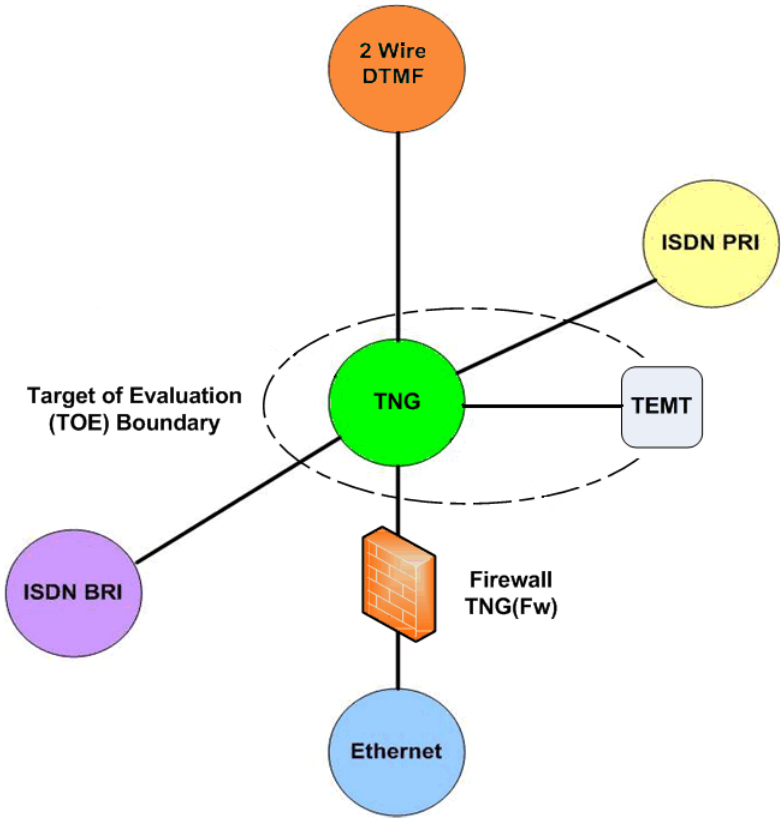

Figure 2 - TOE Boundary[1]

TNG traffic can be comprised of any combination of the following types:

a. Management Data;

b. User Data; and

c. Voice:

(1) Secure; and

(2) Non-secure.

The TNG is gateway equipment and as such, it is located on the edge of the physical security perimeter (of any of its potentially connected systems). TNG is therefore subject to the policies and physical security procedures of the system(s) to which it is connected; specifically the system on which it is acting as a border device. Hence, physical security measures are the responsibility of the system in which it is deployed.

With respect to enforcing security aspects for user and voice data, as the TNG only provides interconnections with other systems for externally-generated (to TNG) user data (i.e., it does not

[1] Circuit switched connections are voice or data capable, depending upon how a call is set-up, e.g. data pipes. Further, it should be noted that the firewall is only relevant for packet-switched data; data passed via a circuit-switched connection does not pass through the firewall.

communicate directly with these end systems), originating/receiving systems are responsible for enforcing the (transmission, network, and cryptographic) security of items (b) and (c) above.

As specified further within this ST, the TNG is responsible for:

a. protecting the confidentiality and integrity of TNG management data (item (a) above); and

b. providing channel separation for data traffic, and voice traffic (secure and non-secure).

In both Figure 1 and Figure 2, the TNG Equipment Management Terminal (TEMT) is shown as interfacing with the TNG and residing on the TOE boundary. This is because the TEMT hosts the TEMS software which forms part of the TOE. However the TEMT hardware and operating system are excluded from the TOE boundary and are part of the IT environment.

A minimal TEMT build will include the following components/applications:

- Microsoft Windows 2000 Service Pack 4 with hotfixes and patches
- HP ProtectTools Authentication Services
- TNG Equipment Management Applications (TEMS and TNG(Fw))
- SSH Software & Certification Authority Key Material
- Microsoft .NET Framework version 1.1 & 2.0

2.3.1 Features Included In TOE

The TOE performs the following security functions:

2.3.1.1 Administration and Security Management

The TEMS performs the TNG management functions. It is connected to the TNG via a dedicated system management connection (see Figure 1) on the TEMT, which is cryptographically set-up and protected using the SSH Version 2 protocol. The TEMS interacts with relevant OS functionality to ensure that every authorized administrator is successfully identified and authenticated before they are permitted to perform any management functions on the TOE.

Returning to the primary objective of direct TNG platform management, subject to the connected systems, the TNG(HQ)/TEMS interconnect will be used to manage and/or provide:

a. the following gateway interfaces:

(1) Ethernet;

(2) ISDN PRI; and

(3) ISDN BRI.

b. the following user telephone interfaces:

(1) ISDN BRI, and

(2) 2-wire DTMF;

c. the following TNG system management functions:

(1) audit log file management;

(2) SSH key management;

(3) firmware upgrade;

(4) NIAC configuration;

(5) PMA lists for connected Ethernet network;

(6) Frequently Called Number Lists;

(7) status reports;

(8) Built-in-Test (BIT);

(9) interface configuration; and

(10) datapipe configuration.

2.3.1.2 Audit

Audit logging is performed by the TNG, and data is stored in memory and written to hard disk for subsequent off-load to external IT systems. Events and data that are recorded consist of the following:

a) Blocked/Dropped Calls (logged by: TNG(HQ));

b) Time of Call (logged by: TNG(HQ));

c) Calling Line Identifier (logged by: TNG(HQ));

d) Local login attempts to TNG (logged by: TNG(HQ));

e) Failed login attempts to TNG (logged by: TEMS);

f) Successful login attempts to the TEMT (logged by TEMS);

g) Log-off from the TEMT (logged by: TEMS);

h) Creation, deletion, or alteration of access rights and privileges (logged by: TEMS);

i) Creation, deletion, or alteration of passwords (logged by: TEMS);

j) Authentication failures (logged by: TNG(HQ));

k) Firmware updates (logged by: TNG(HQ));

l) Setting of the timestamp clock (logged by: TNG(HQ));

m) Download of audit records to the TEMT (logged by: TNG(HQ));

n) TNG configuration change (logged by: TNG(HQ));

o) Login of TEMT to TNG (logged by: TNG(HQ)); and

p) Log-off of TEMT from TNG (logged by: TNG(HQ)).

2.3.1.3 Cryptography

TNG provides cryptographic interfaces for its own use. It employs the SSH v2 protocol for establishing encrypted communications channels used in administering the TNG(HQ). Establishment of the secured-channels occurs using asymmetric keys pre-generated by the end-user's Certificate Authority (CA) and then pre-loaded by the developer or the end-user. As part of

the SSH protocol, symmetric keys are established and used for the duration of the session. Digital signatures (hash algorithms and asymmetric keys & algorithms) are used by the TNG to validate Installation and Role asymmetric key pairs prior to use or update, and software/firmware loads when updating.

2.3.1.4 Information Flow Control

Traffic flow from between connected network nodes is controlled by information flow control policies (refer to section 2.4). These policies control the flow of traffic based upon administratively configured rule sets and information embedded within the traffic itself. All management traffic is subject to the TNG's authenticated information flow policy which requires the use of cryptographic support mechanisms for both authentication and protection of the management information flows.

2.3.1.5 Access Control

The TNG uses Microsoft Windows accounts to implement a role-based access control capability. The features and functions available to authorized users are based on the Microsoft Windows account which is used. Refer to section 2.4.2 for additional details.

2.3.1.6 TOE Self-Protection

The TNG is a hardware device that protects itself by primarily offering a minimal logical interface to its connected networks. The TNG operating system is a specific-purpose OS that has been hardened and configured to provide no general purpose programming capability. All network traffic from one network zone to another passes through the TOE; however, no protocol services are provided for end-user communication with the security appliance itself. The TOE also preserves its configuration for a trusted recovery in the event that the configuration has been modified and not saved or if the TNG has been shutdown ungracefully.

2.3.1.7 Trusted Channel / Path

The TNG shall provide a trusted channel between the TEMT and the TNG(HQ) for local administration of those TNG oNAUs by TNG Managers and TNG Administrators. As well, trusted channels (secure chat) are provided between TEMTs in peer TOEs.

2.4 TOE SECURITY FUNCTIONAL POLICIES

2.4.1 Unauthenticated Information Flow SFP

For the UNAUTHENTICATED INFORMATION FLOW SFP, the subjects under control of this policy, are the TOE interfaces that connect to unauthenticated end-users (IT entities) on an internal or external network while sending information through the TOE to other destinations on the internal or external network.

The information flowing between subjects in the policy consists of traffic with attributes, defined in FDP_IFF.1.1, including source and destination addresses.

The rules that define the SFP are found in FDP_IFF.1.2.

For TNG(HQ) oNAU configurations, ports are configured with the security mode (Secure/Non-Secure) and data is routed through VLANs. In Secure mode, all Non-Secure traffic is discarded; in Non-Secure mode all Secure traffic is discarded. Separate VLANs are used for:

- Secure and Non-Secure traffic passing between TNG interfaces;
- User data and management traffic; and
- Voice traffic.

Packets without the appropriate VLAN identification (either absent or misrouted) are discarded.

2.4.2 Authenticated User Access Control SFP

The TNG incorporates a role-based access control capability that defines tasks that are allowed to be performed by authorized (management) users. The TNG oNAUs do not perform authentication, as any user who has successfully authenticated to the TEMT and is able to run the TEMS, is able to request the establishment of a SSH session with a particular agent. For example; the TEMS (running on the TEMT) permits a TNG Administrator to perform FW upgrades, but prevents a TNG Manager from performing this function. The TEMS GUI prevents a TNG Manager from accessing the FW upgrade function. Therefore, a request to the oNAU to establish an SSH session to the FW Upgrade agent on the oNAU) will only come from a TNG Administrator. Authentication to the TEMT (as TNG Administrator or TNG Manager) is accomplished via the standard Microsoft Windows authentication process. The TEMS software (on the TEMT) is only accessible to these two accounts. Additionally as noted in the example earlier in this section, the TEMS GUI restricts access to some functionality to only one of the accounts.

When a TNG oNAU receives a request from the TEMT to open an SSH session, the TNG oNAU negotiates an SSH session with the TEMT using the appropriate NetBSD account. Each management agent on the oNAU is associated with a specific NetBSD user account (local management account) who then relay requests to other agents (e.g. firmware update or key update account). Management data is transferred between the TEMS and the applicable TNG oNAU via these SSH sessions. All data transfers between the TEMT and the TNG(HQ) oNAUs are protected by the SSH session

Operating system user account types on the oNAUs cannot be created, modified or deleted except by firmware update. The use of digital signatures in the TNG firmware (FW) process ensures the authenticity and integrity of new TNG FW loads. As noted above, all management operations between the TEMT and the TNG(HQ) are preceded by SSH session initiation requests and followed by validation of operations after the session is established.

On the TEMT, creation, modification and deletion of any of its user accounts is based on the standard Windows operating system controls. For operation of the TEMS, TNG (Windows) accounts include:

a. TNG Manager: TEMS application specific Power User used for TNG(HQ) (and TNG(Fw)) day-to-day management functions, excluding for TNG(HQ) firmware upgrade; and

b. TNG Administrator: Administrator user, has control over all TEMT aspects including all functions contained in the TNG(HQ) management applications, i.e., those functions assigned to the TNG Manager as well as firmware upgrade capability. The TNG Administrator is also considered to be the TNG Security Auditor. This pertains specifically to the ability to access the Windows Security Event log on the TEMT.

TNG(HQ) user accounts are part of the NetBSD secure configuration. They are used to control external access to the OS and the rights and privileges of the daemons that perform the various tasks.

3 TOE SECURITY ENVIRONMENT

3.1 SECURE USAGE ASSUMPTIONS

The TNG will be employed in military environments where it will be required to correctly route a combination of sensitive and non-sensitive traffic (data and voice) between its interconnected networks.

While the TNG is currently intended for use in a military environment, it has the potential for use in a commercial environment where ruggedised equipment is called for (e.g., tactical police communications).

The following usage assumptions are made about the intended environment of the TOE.

A.AVAILABILITY	Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.
A.CONNECT	The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.
A.GOOD_ADMIN	The administrators will be competent and will adhere to the applicable TOE guidance; however they are capable of error.
A.NO_BYPASS	It is assumed that information cannot flow between the connected networks unless it passes through the TOE.
A.NO_GEN_PURPOSE	There are no general-purpose computing or storage repository capabilities available on the TNG(HQ) portion of the TOE.
A.NO_MAINT_PORT	It is assumed that the maintenance port (COM1) on the TNG(HQ) portion of the TOE will not be used while the TNG(HQ) is in operational service.
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

3.2 THREATS

The threats listed below are addressed by the TOE. The threat agents consist of unauthorized persons or external IT entities that are not authorized to use the TOE as well as authorized administrators of the TOE who either make errors in configuring the TOE or act maliciously towards the TOE. The threat agent is assumed to be a motivated attacker with an attack potential of BASIC. The resources used by the attacker are assumed to include attack tools that are publicly available as well as bespoke tools. The assets that are subject to attack are the oNAUs that comprise the TNG and the TEMT.

T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

T.ADMIN_ROGUE	An administrator's intentions may become malicious resulting in user or TOE Security Functions (TSF) data being compromised.
T.AUDIT_COMP	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.CRYPTO_COMP	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.
T.FLAWED_TOE	Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
T.MALICIOUS_USER	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted). This threat class includes malicious software threats (e.g., viruses, Trojans, etc.).
T.MASQUERADE	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.
T.MISSED_ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.POOR_TEST	Insufficient testing to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behaviour being undiscovered thereby causing potential security vulnerabilities.
T.SPOOFING	A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended TOE session.
T.UNAUTH_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNAUTH_PEER	An unauthorized IT entity may attempt to establish a security association with the TOE.
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.
T.USER_ERROR	A user error could lead to the incorrect operation of the TOE (e.g., hardware or software fault).

3.3 ORGANIZATIONAL SECURITY POLICIES

There are no organizational security policies with which the TOE must comply.

Application Note: Organizational security policies may be defined by the end-user of the TOE. The TOE developer provides procedural security recommendations to the purchaser of the TOE.

4 SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

The following are the IT security objectives for the TOE:

O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure configuration and management of the TOE.
O.ADMIN_ROLE	The TOE will provide administrator roles to isolate administrative actions, and to make the administrative functions available locally.
O.AUDIT_DATA	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information and alert the administrator to identified potential security violations.
O.GOOD_TESTING	The TOE will undergo appropriate security functional testing that demonstrates that the TSF satisfy the security functional requirements.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MANAGE_CHANGE	The configuration of, and all changes to, the TOE and its development evidence will be analyzed, tracked and controlled throughout the TOE's development.
O.MEDIATE_INFO	The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.
O.PEER_AUTH	The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
O.SELF_PROTECT	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure.
O.SOUND_DESIGN	The TOE will be designed using sound design principles and techniques. The TOE design, design principles and design techniques will be adequately and accurately documented.
O.SOUND_TOE	The implementation of the TOE will be an accurate instantiation of its design, and is adequately and accurately documented.

O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
O.TRUSTED_PATH	The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.
O.USER_GUIDANCE	The TOE will provide users with the information necessary to correctly use the security mechanisms.
O.VULN_ANAL_TEST	The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE and does not allow attackers to violate the TOE's security policies.

For a detailed mapping between threats and the IT security objectives listed above see Section 8.1 of the Rationale.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The security objectives for the IT Environment of the TOE are listed below. In each case the objective is formulated to satisfy one of the assumptions from Section 3.1 of the ST.

OE.AVAILABILITY	Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.
OE.CONNECT	The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.
OE.GOOD_ADMIN	The administrators will be competent and will adhere to applicable TOE guidance; however they are capable of error.
OE.NO_BYPASS	Information cannot flow between the connected networks unless it pass through the TOE.
OE.NO_GEN_PURPOSE	The are no general purpose computing or storage repository capabilities such as compilers, editors or user applications available on the TNG portion of the TOE.
OE.NO_MAINT_PORT	The maintenance port (COM1) on the TNG(HQ) portion of the TOE will not be used while the TNG(HQ) is in operational service.
OE.PHYSICAL	The IT environment provides the TOE with appropriate physical protection, commensurate with the value of the IT assets protected by the TOE.

For a detailed mapping between threats, assumptions, and the non-IT security objectives listed above see Section 8.1 of the Rationale.

5 IT SECURITY REQUIREMENTS

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance requirements from Part 3 of the CC.

5.1.1 Overview

5.1.1.1 Content

The security functional requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 2.

CC Part 2 Security Functional Components	
Identifier	**Name**
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_DAU.1	Basic data authentication
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_ITT.1	Basic internal transfer protection
FIA_AFL.1(1)	Authentication failure handling (TNG)
FIA_ATD.1(1)	User attribute definition (TOE)
FIA_UAU.2(1)	User authentication before any action (TOE)
FIA_UID.2(1)	User identification before any action (TOE)
FMT_MOF.1(1)	Management of security functions behaviour (enable/disable)
FMT_MOF.1(2)	Management of security functions behaviour (enable only)
FMT_MOF.1(3)	Management of security functions behaviour (TNG

CC Part 2 Security Functional Components	
Identifier	**Name**
	Administrator)
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1(1)	Management of TSF data (audit logs except Windows Security Audit log)
FMT_MTD.1(2)	Management of TSF data (Windows Security Audit log)
FMT_MTD.3	Secure TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.2	TSF data transfer separation
FPT_RVM.1(1)	Non-bypassability of the TSP (TOE)
FPT_SEP.1(1)	TSF domain separation (TOE)
FPT_STM.1(1)	Reliable time stamps (TOE)
FTP_TRP.1	Trusted path

Table 2 – TOE Security Functional Requirements

5.1.1.2 Strength of Function

The minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism shall be SOF-basic. The rationale for this selected level is presented in Section 8.4.

The minimum strength of function level for the TOE security functions applies to the TOE's authentication mechanisms which form part of the F.I&A security function which in turn meets the requirements of the FIA_UAU.2(1) security functional requirement.

In addition to the mandated strength of function level for the TOE, strength of function requirements are levied on the TOE environment by the following security functional requirements:

- FIA_UAU.2(2); and
- FIA_SOS.1.

5.1.2 Security Functional Requirements

5.1.2.1 FAU_ARP.1 Security alarms

FAU_ARP.1 The TSF shall take [the following action(s):

a) record the security relevant event into the log; and optionally

depending on the nature of the alarm

b) utilize SNMP traps to report events to the management function; and

c) provide a visual and/or audible alarm on the management terminal]

upon detection of a potential security violation.

5.1.2.2 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit;

c) [Blocked/Dropped Calls;

d) Successful and failed local login attempts to TNG(HQ);

e) Successful login attempts to the management terminal;

f) Logout from the management terminal;

g) Creation, deletion, or alteration of access rights and privileges (on TEMT);

h) Creation or alteration of passwords (on TEMT);

i) Authentication failures;

j) Firmware updates (on TNG(HQ));

k) Setting of the timestamp clock (on TNG(HQ));

l) Download of TNG(HQ) audit records to the TEMT; and

m) Selected configuration change (on TNG(HQ)).].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST:

[management terminal commanding the event].

Application Note: *In operation, the passwords for the TNG Manager and TNG Administrator shall not be changed.*

5.1.2.3 FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application *Some audit event records are in response to system generated events. In*

Notes: *these cases there is no user identity associated with the auditable event.*

For audit records on the TEMS the phrase "the user that caused the event" refers to either the TNG Administrator or TNG Manager operating system accounts.

5.1.2.4 FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*].

5.1.2.5 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [only the Security Auditor] with the capability to read [all logged data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: *Only the Security Auditor (TNG Administrator) has access to all of the log information. However on the TEMT workstation, the TNG Manager has access to the TNG log archives and the Windows system and application logs. The TNG Manager does not have access to the Windows security log on the TEMT workstation.*

5.1.2.6 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.2.7 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorized modifications to the audit records in the audit trail.

5.1.2.8 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [*overwrite the oldest stored audit records*] and [overwrite the earlier records in the same order as they were originally recorded] if the audit trail is full.

5.1.2.9 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [the specified cryptographic operations in column one (Cryptographic Operations) in Table 3 - Cryptographic Algorithms] in

accordance with ~~a~~ the specified cryptographic algorithms [specified in column two (Cryptographic Algorithm) of Table 3 - Cryptographic Algorithms] and cryptographic key sizes [specified in column three (Cryptographic Key Size) of Table 3 - Cryptographic Algorithms] that meet the ~~following:~~ [algorithm standards identified in column four (Applicable Standard) of Table 3 - Cryptographic Algorithms].

Cryptographic Operation	Cryptographic Algorithm	Cryptographic Key Size	Applicable Standard
Encryption	Advanced Encryption Standard (AES)	256 bits	FIPS 197, *Advanced Encryption Standard (AES)*
Hashing	Secure Hash Algorithm (SHA-1)	none	FIPS 180-2, *Secure Hash Standard*

Table 3 - Cryptographic Algorithms

5.1.2.10 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [AUTHENTICATED USER ACCESS CONTROL SFP] on

a) [TNG Manager (TNG);

b) TNG Administrator (TEMT);

c) Firmware upgrade;

d) Maintenance; and

e) all TNG users].

Application Note: *There are two User (Role) Accounts – TNG Administrator (for TEMT/TEMS including the firmware upgrade function) and TNG Manager (for most other TEMS functions).*

5.1.2.11 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [AUTHENTICATED USER ACCESS CONTROL SFP] to objects based on the ~~following~~ [object requester being an authorized user].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) [a user account for the claimed user ID exists;

b) the presented authentication credential is valid and matches that required for the claimed user ID;

c) if the authenticated user is the (Security Auditor | TNG Administrator), access will be granted to the Windows Security audit

logs;

d) if the authenticated user is the TNG Manager or TNG Administrator, access will be granted to the TNG log file archive directory; and

e) all management operations are preceded by SSH session initiation requests and are validated after the session is established].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

a) [user account types on the TNG(HQ) cannot be created, modified, or deleted;

b) user accounts on the TNG(HQ), associated with TEMT accounts (TNG Manager, TNG Administrator) are only available through authenticated SSH sessions and are otherwise denied access; and

c) On the TNG(HQ), absence of an explicit rule permitting the access in a policy file (basically, any access which is not explicitly permitted, is denied)].

5.1.2.12 FDP_DAU.1 Basic data authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of:

a) [TNG(HQ) firmware through the application of a hashing mechanism and digital signature; and

b) All firmware loads and updates by utilising a hashing mechanism and digital signature.]

FDP_DAU.1.2 The TSF shall provide [the TNG Administrator and the TNG Manager] with the ability to verify evidence of the validity of the indicated information.

5.1.2.13 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW SFP] on:

a) [subjects: each IT entity that sends and receives information through the TOE;

b) information: traffic sent through the TOE from one subject to another; and

c) operations: pass or drop information].

5.1.2.14 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [UNAUTHENTICATED INFORMATION FLOW SFP] based on the following types of subject and information security attributes:

a) [subject security attributes: port/VLAN identification, port configuration, (secure/non-secure, mixed); and

b) Information security attributes: flow type (voice/data) and data type (user/management traffic)].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) [in Non-Secure mode all non-Secure traffic is allowed; in Secure mode all Secure traffic is allowed].

FDP_IFF.1.3 The TSF shall enforce the [no additional information flow control rules].

FDP_IFF.1.4 The TSF shall provide the following [user/management traffic shall be separated via VLAN, secure/non-secure user traffic shall be separated via VLAN, voice/data traffic shall be separated via VLAN].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules:

a) [none].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

a) [In Secure mode, all Non-Secure traffic is discarded; in Non-Secure mode all Secure traffic is discarded. Packets without the appropriate VLAN identification (either absent or misrouted) are discarded].

5.1.2.15 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [ACCESS CONTROL SFP and/or INFORMATION FLOW CONTROL SFP] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [

The digital signature of this new image, once downloaded to the alternate image area, is checked by the current image and if verified, this new image is activated and becomes the current image. Lack of a digital signature or failure to verify the digital signature aborts this final activation action.]

5.1.2.16 FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the [AUTHENTICATED USER ACCESS CONTROL SFP] to prevent the [*disclosure*, *modification*, *and loss of use*] of user data when it is transmitted between physically-separated parts of the TOE.

5.1.2.17 FIA_AFL.1(1) Authentication failure handling (TNG)

FIA_AFL.1.1(1) The TSF shall detect when [*one*] unsuccessful authentication attempt occurs related to [any claimed user ID attempting to authenticate to the TNG].

FIA_AFL.1.2(1) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall:

a) [generate an audit log record]

Application Note: *Administrators (using TEMS on the TEMT) do not authenticate directly with the TNG(HQ). Rather the TEMS application authenticates to the TNG(HQ) using the TNG(HQ) account appropriate to the administrative action that has been requested.*

5.1.2.18 FIA_ATD.1(1) User attribute definition (TOE)

FIA_ATD.1.1(1) The TSF shall maintain the following list of security attributes belonging to ~~individual users~~ user accounts associated with the following TEMT Windows accounts:

a) [TNG Manager and TNG Administrator:

Role]

Application Note: *The TEMS user interface determines which administrative functions are available to which TEMT account.*

On the TNG(HQ) user accounts cannot be created, modified or deleted except by firmware update. The TEMS application will login to the TNG(HQ) using an account determined by the administrative function being requested by the TEMS application.

5.1.2.19 FIA_UAU.2(1) User authentication before any action (TOE)

FIA_UAU.2.1(1) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: *Under normal operations users do not identify or authenticate to the TNG(HQ). This function is performed on their behalf by the TEMS application. However, the TNG(HQ) operating systems is a customized version of the UNIX OS which maintains a list of user accounts and requires identification and authentication before permitting any actions on behalf of the user.*

5.1.2.20 FIA_UID.2(1) User identification before any action (TOE)

FIA_UID.2.1(1) The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Application Note: *Under normal operations users do not identify or authenticate to the TNG(HQ). This function is performed on their behalf by the TEMS application. However, the TNG(HQ) operating systems is a customized version of the UNIX OS which maintains a list of user accounts and requires identification and authentication before permitting any actions on behalf of the user.*

5.1.2.21 FMT_MOF.1(1) Management of security functions behaviour (enable/disable)

FMT_MOF.1.1(1) The TSF shall restrict the ability to [*enable and disable*] the following functions:

a) [user account "active" (enable and disable only); and

b) audit]

to [the TNG Manager and TNG Administrator accounts].

Application Note: *The TNG Manager account cannot enable or disable the TNG Administrator account.*

5.1.2.22 FMT_MOF.1(2) Management of security functions behaviour (enable only)

FMT_MOF.1.1(2) The TSF shall restrict the ability to [*enable*] the following functions:

a) [delete unarchived log file;

b) delete unexported log file; and

c) access rights and privilege definitions (creation, deletion, and alteration).]

to [the TNG Manager and TNG Administrator accounts].

5.1.2.23 FMT_MOF.1(3) Management of security functions behaviour (TNG Administrator)

FMT_MOF.1.1(3) The TSF shall restrict the ability to [*enable*] the function [TOE firmware update] to [the TNG Administrator account].

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [AUTHENTICATED USER ACCESS SFP] to restrict the ability to [*change_default, query, modify, delete*] the security attributes [defined in FDP_IFF.1.1] to the [TNG Manager and TNG Administrator accounts].

5.1.2.24 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.2.25 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [AUTHENTICATED USER ACCESS SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [TNG Manager and TNG Administrator accounts] to specify alternative initial values to override the default values when an object or information is created.

5.1.2.26 FMT_MTD.1(1) Management of TSF data (audit logs except Windows Security Audit log)

FMT.MTD.1.1(1) The TSF shall restrict the ability to [*query, delete, clear*] the [all audit logs except the Windows Security Audit log] to [the TNG Administrator and TNG Manager accounts].

5.1.2.27 FMT_MTD.1(2) Management of TSF data (Windows Security Audit log)

FMT.MTD.1.1(2) The TSF shall restrict the ability to [*query, delete, clear*] the [Windows Security Audit log] to [the TNG Administrator account (i.e. the TNG Security Auditor role)].

5.1.2.28 FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

5.1.2.29 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) [start-up and shutdown;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) modify and set the time and date; and

e) archive, create, delete, empty, and review the audit log.]

5.1.2.30 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role~~s~~ [TNG Manager and TNG Administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with the TNG Manager and TNG Administrator role~~s~~.

Application Note: *The terms TNG Administrator and TNG Manager refer to both users and roles. They act as users in the sense that accounts exist with these names on the operating system which hosts the TEMS. Human users must know the password for one of these accounts in order to gain access to the*

TEMS software. They also act as roles in the sense that the features available depend on whether a human user has connected with the TNG Administrator or TNG Manager account. The TOE has been developed to meet the specifications of a specific government agency who has decided that given the physical and personnel security measures in place, associating individual human users with their actions on the TOE is not a requirement. Therefore the requirements of FMT_SMR.1.2 are met since the TNG Administrator user is always associated with the TNG Administrator role while the TNG Manager user is always associated with the TNG Manager role. Similarly the requirements of FAU_GEN.2 are met since auditable events (on the TEMT) will be associated with either the TNG Administrator user or the TNG Manager user.

5.1.2.31 FPT_ITT.2 TSF data transfer separation

FPT_ITT.2.1 The TSF shall protect TSF audit data from [*disclosure, modification*] when it transmitted between ~~separate parts of the TOE~~ the:

a) TNG(HQ) and the TEMT.

FTP_ITT.2.2 The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

5.1.2.32 FPT_RVM.1(1) Non-bypassability of the TSP (TOE)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.2.33 FPT_SEP.1(1) TSF domain separation (TOE)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.2.34 FPT_STM.1(1) Reliable time stamps (TOE)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.2.35 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communications path between itself and [*local*] ~~users~~ TNG Administrators and TNG Managers that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [*local users*] to initiate communications via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for:

a) [initial user TNG Administrator and TNG Manager authentication; and

b) the issuance of all management commands.]

5.2 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

This section describes the security functional requirements which must be provided by the IT environment in which the TOE operates. These requirements consist of functional components drawn from Part 2 of the CC.

5.2.1 Overview

CC Part 2 Security Functional Components	
Identifier	**Name**
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FIA_AFL.1(2)	Authentication failure handling (TEMT)
FIA_ATD.1(2)	User attribute definition (IT Environment)
FIA_SOS.1	Verification of secrets
FIA_UAU.2(2)	User authentication before any action (IT Environment)
FIA_UID.2(2)	User identification before any action (IT Environment)
FIA_UAU.6	Re-authenticating (IT Environment)
FPT_RVM.1(2)	Non-bypassability of the TSP (IT Environment)
FPT_SEP.1(2)	TSF domain separation (IT Environment)
FPT_STM.1(2)	Reliable time stamps (IT Environment)

Table 4 – Security Functional Requirements for the IT Environment

5.2.2 Security Functional Requirements

5.2.2.1 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The ~~TSF~~ IT Environment shall provide the ability to perform [*searches*] of audit data based on:

a) [User identity; and

b) Type (success or failure), date, time, category, event identifier and computer].

5.2.2.2 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The ~~TSF~~ IT Environment shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [event type]; and

b) [no additional attributes].

5.2.2.3 FIA_AFL.1(2) Authentication failure handling (TEMT)

FIA_AFL.1.1(2) The ~~TSF~~ IT Environment shall detect when [*six*] unsuccessful authentication attempts occur related to [any claimed user ID attempting to authenticate to the TEMT].

FIA_AFL.1.2(2) When the defined number of unsuccessful authentication attempts has been met or surpassed, the ~~TSF~~ IT Environment shall:

a) [generate an audit log record; and

b) lock out the user account which was attempting to login to the TEMT for a period of sixty minutes, unless the account being locked is the TNG Administrator account.]

5.2.2.4 FIA_ATD.1(2) User attribute definition (IT Environment)

FIA_ATD.1.1(2) The ~~TSF~~ IT Environment shall maintain the following list of security attributes belonging to ~~individual users~~ the following user accounts:

a) [TNG Manager and TNG Administrator accounts:

User ID and password.]

5.2.2.5 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The ~~TSF~~ IT Environment shall provide a mechanism to verify that secrets meet [the minimum password length and complexity requirements specified in the TNG guidance documents for both the TNG Administrator and the TNG Manager accounts].

5.2.2.6 FIA_UAU.2(2) User authentication before any action (IT Environment)

FIA_UAU.2.1(2) The ~~TSF~~ IT Environment shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.2.7 FIA_UID.2(2) User identification before any action (IT Environment)

FIA_UID.2.1(2) The ~~TSF~~ IT Environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.2.8 FIA_UAU.6 Re-authenticating (IT Environment)

FIA_UAU.6.1 The ~~TSF~~ IT Environment shall re-authenticate ~~the user~~ TNG Administrators and TNG Managers under the conditions [after 20 minutes of inactivity].

5.2.2.9 FPT_RVM.1(2) Non-bypassability of the TSP (IT Environment)

FPT_RVM.1.1 The ~~TSF~~ IT Environment shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to

proceed.

5.2.2.10 FPT_SEP.1(2) TSF domain separation (IT Environment)

FPT_SEP.1.1(2) The ~~TSF~~ IT Environment shall maintain a security domain for ~~its own~~ the TOE's execution that protects ~~it~~ the TOE from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2) The ~~TSF~~ IT Environment shall enforce separation between the security domains of subjects in the TSC.

5.2.2.11 FPT_STM.1(2) Reliable time stamps (IT Environment)

FPT_STM.1.1(2) The ~~TSF~~ IT Environment shall be able to provide reliable time stamps for ~~its own~~ use by the TOE.

Application Note: *The word 'reliable' in the above requirement means that the order of the occurrence of auditable events is preserved. Reliable time stamps, which include both date and time, are especially important for TOEs comprised of greater than one component. This requirement was refined to make it clear that the IT Environment provides time stamps for the use of the TOE.*

5.3 TOE SECURITY ASSURANCE REQUIREMENTS

5.3.1 Overview

The security assurance requirements for the TOE consist of the requirements corresponding to the EAL2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Remediation.

5.3.2 Security Assurance Requirements

The assurance components are summarized in the following table:

Assurance Class	Assurance Components	
	Identifier	**Name**
Configuration Management	ACM_CAP.2	Configuration items
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_FLR.1	Basic flaw remediation

Assurance Class	Assurance Components	
	Identifier	**Name**
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5 – Security Assurance Requirements (EAL2+)

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements defined in Section 5. The functions and functional requirements are cross-referenced in Table 12. The assurance measures and assurance requirements are cross-referenced in Table 13.

6.1 TOE SECURITY FUNCTIONS

6.1.1 Overview

The TOE security functions that were introduced in Section 2.3.1 are further elaborated in this section. The major functions (e.g., audit) are decomposed to more clearly define their functionality.

6.1.2 Administration and Security Management

F.HMI

The TOE supports the following interfaces for administrative access:

a) serial port for local connections to a TEMT.

Administrative access to the TOE is restricted to authorised administrators. Access control shall be provided through a set of defined profiles (roles) that permit specific administrative activities to be performed.

Each administrative user has an associated set of attributes, which are maintained by the TNG Administrator.

The TOE only accepts secure values for security attributes.

Tasks that are restricted to the TNG Administrator and/or TNG Manager are:

a) start-up and shutdown;

b) management of TOE interfaces;

c) manipulation of security attributes;

d) creation, deletion, modification, and viewing of user attribute values;

e) enable, disable, determine and modify the behaviour of the Audit function;

f) modification, deletion, creation and querying of information flow policy rules including as a minimum:

configuring communications interfaces as secure and rejecting all non-secure traffic, and

configuring communications interfaces as non-secure and rejecting all secure traffic;

g) configuration of the time source for the time and date used to form the time stamps;

h) archive, create, delete, empty, and review the audit logs; and

i) recovery of the TOE to a secure state.

6.1.3 Audit

F.AUDIT

The TOE provides an audit management capability for use by authorized users (i.e., TNG Administrator as the Security Auditor).

The TOE is capable of generating:

a) auditable events; and

b) audit records.

The TOE provides the TNG Administrator (as Security Auditor) with the capability to configure auditable events with respect to the Windows Security Log. The TNG Manager can also access and manipulate the Windows System/Application logs and archived TNG logs.

Each auditable event generates an audit record.

The TOE generates an alarm when the storage capacity of the audit log has been exceeded.

The TOE provides the TNG Administrator (as Security Auditor) and the TNG Manager with a searching capability for audit log analysis.

The TOE provides the TNG Administrator (as Security Auditor) and the TNG Manager with the capability to:

a) manage audit log storage;

b) back-up (archive) audit log data; and

c) delete archived audit log data files.

The TEMT configures and sends update requests to the oNAUs, and the oNAUs download event log files to the TEMT on an as-requested or as-configured basis. Details of trap events are recorded in local logs and may be sent back to an associated TEMT (via SSH sessions) if so configured in the trap itself. The logs sent back from the oNAUs to the TEMT are exported/imported in ASCII Text Format in order to be readable and parsable by the Windows text editor. For auditability purposes, a flag or delimiter within the file denoting the event as “security” is used. Windows Notepad can then be used to search the standard Windows logs (security, application, system), search through the events and allow viewing. Note that the specific events listed in Section 2.3.12 when recorded in log files from associated TNG(HQ) oNAUs and stored/archived on the TEMT will also contain this “security” flag, and thus can also be parsed and viewed.

6.1.4 Cryptography

F.CRYPTO

Within the TNG SSH v2 is implemented using signed asymmetric keys, all of which are generated and controlled through a Certification Authority (CA). These sessions, provide confidentiality and authentication and are used for assurance of data separation (management vs user) and are enacted between the TEMT and its associated TNG(HQ) oNAUs, or between TEMTs on peer TOEs. In TNG(HQ) oNAUs, all management operations are funnelled through a FW interface which directs SSH session initiation requests to the appropriate agents within the oNAU and validates the operation (after session establishment) by performing stateful inspection of packets. In TEMTs, the TNG Manager account controls/initiates SSH session via the TEMS.

Digital signature checks verify application of the TNG master private key to other key pairs, public keys, TNG FW upgrades or new TNG software applications.

The TOE performs data encryption/decryption of management data using the Advanced Encryption Standard (AES) algorithm with a minimum key size of 256 bits

The reference standards for the TOE's cryptographic operations are listed in Table 3 of section 5.1.2.9.

6.1.5 Information Flow Control

F.INFO_FLOW_CTRL

The TNG information flow control security functional policies are defined at section 2.4.

6.1.6 Access Control

F.ACCESS_CTRL

The TNG user access control security functional policies are defined at section 2.3.

6.1.7 TOE Self-Protection

F.DOMAIN

The TOE maintains a security domain, within its enclosure, for its own execution that protects it from interference and tampering by untrusted subjects.

The TOE is configured so that no general-purpose software (unapproved by those responsible for the TNG) runs on the system.

On startup, the TOE checks its boot partition to ensure that no changes have been made.

The TOE enforces separation between the security domains of subjects in the TSF Scope of Control (TSC) by assigning each to a physical and logical input/output interface and by segregating and

	protecting security-critical data in a configuration file.
F.REF_MEDIATE	The TNG(HQ) modules (oNAUs) authenticate all management commands. The privileges and access are statically defined for each process and this can only be changed by loading a new FW image.
F.TIME	The TOE provides reliable time stamps for its own use which includes audit record creation.

6.1.8 Trusted Channel / Path

F.TRUSTED_COMMS The TOE provides two types of encrypted communications, trusted channel and trusted path, where:

a) trusted channel refers to the encrypted connection between the TOE and a trusted IT entity; and

b) trusted path refers to the encrypted connection used to authenticate an administrator (TNG Manager or TNG Administrator) with the TOE.

Trusted paths and trusted channels:

a) are logically distinct from other communication paths;

b) provide assured identification of their end points; and

c) are protected by encryption to guard against disclosure and by cryptographic signature to detect modifications

Either the TOE or the trusted IT entities are able to initiate communication via the trusted channel.

The trusted path is used for all local TNG Administrator authentication functions.

6.2 ASSURANCE MEASURES

A description of each of the TOE assurance measures follows.

M.ID	The TOE incorporates a unique version identifier that can be displayed to the user.

M.CMSYS	The TOE was developed and is maintained using a documented Configuration Management (CM) system, with automated generation support, to ensure that only authorised changes are made to the TOE configuration items and implemented in the evaluated version of the TOE and to support the generation of the TOE. The organization, operation and usage of the CM system are described in a CM plan, which describes the method used to uniquely identify the configuration items, describes the automated tools and their usage in the system, and identifies CM records that are to be retained as evidence that the CM system is operating in accordance with the plan and that all configuration items have been and are being effectively maintained under the CM system. A list that uniquely identifies and describes all configuration items that comprise the TOE, all TOE documentation, all configuration items required to create the TOE (i.e., implementation representation), security flaws and the evaluation evidence required by the assurance components of the ST, is maintained. The procedures used to accept modified or newly created configuration items as part of the TOE are documented in an acceptance plan.
M.GETTOE	The developer uses a documented and controlled process and procedures for shipping a packaged TOE, identified by serial number, to a customer. The delivery documentation describes all procedures and technical measures that are necessary to maintain security and detect modifications or any discrepancy between the developer's master copy and the version received at the user site. The documentation describes how the procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.
M.SETUP	Documented procedures describe all the steps necessary for the secure installation, generation, and start-up of the TOE. Application of these procedures to the TOE results in a secure configuration.
M.SPEC	The development documentation contains a: a) functional specification, and b) high level TOE design. The informal, internally consistent, functional specification describes the TSF and it: a) contains a description of the purpose and method of use of all external TSF interfaces, and, for each, designates the interface as security-enforcing or security-supporting;

b) describes, for security-enforcing external TSF interfaces, the functional specification describes the security-enforcing effects and security-enforcing exceptions, and the direct error messages that result from security-enforcing effects and exceptions, and

c) completely represents the TSF and includes rationale that the TSF is completely represented.

The informal, internally consistent, high-level design describes the structure of the TOE in terms of subsystems. The high-level design:

a) describes the design of the TOE in sufficient detail to determine what subsystems of the TOE are part of the TSF; and

b) identifies all subsystems in the TSF, and designates them as either security-enforcing or security-supporting as described below:

for security-enforcing subsystems, the high-level design describes the structure of the subsystem, the design of the security-enforcing behaviour and summarizes any non-security-enforcing behaviour.

the high-level design summarizes the behaviour for security-supporting subsystem. The high-level design describes any interactions between the security-enforcing subsystems of the TSF and summarizes all other interactions between subsystems of the TSF.

M.TRACE Correspondence mappings demonstrate that the security functionality detailed in the TOE functional specification is upwards traceable to this ST and downwards traceable to the high level design. For each adjacent pair of provided TSF representations, a correspondence analysis demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

M.DOCS Documentation is provided in the form of operational guidance for the administrator and for the user.

The administrator guidance:

a) describes the administrative functions and interfaces available to the administrator of the TOE;

b) describes how to administer the TOE in a secure manner;

c) contains warnings about functions and privileges that should be controlled in a secure processing environment;

d) identifies all assumptions regarding user behaviour that are relevant to secure operation of the TOE; and

e) describes all security parameters under the control of the administrator, indicating secure values as appropriate, and describes each type of

security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

The administrator guidance is consistent with all other documentation supplied for evaluation, and describes all security requirements for the IT environment that are relevant to the administrator.

The user guidance:

a) describes the functions and interfaces available to the non-administrative users of the TOE;

b) describes the use of user-accessible security functions provided by the TOE;

c) contains warnings about user-accessible functions and privileges that should be controlled in a secure processing environment;

d) clearly presents all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

The user guidance is consistent with all other documentation supplied for evaluation, and describes all security requirements for the IT environment that are relevant to the user.

Flaw remediation guidance (which forms part of the user guidance) is provided to describe how TOE users report to the developer any suspected security flaws in the TOE.

The flaw remediation guidance also describes a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

The flaw remediation guidance identifies the specific points of contact for all reports and enquiries about security issues involving the TOE.

M.FLAWREM Flaw remediation procedures, addressed to TOE developers, establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to these flaws.

The flaw remediation procedures documentation describes the procedures used to track all reported security flaws in each release of the TOE.

The flaw remediation procedures:

a) require that a description of the nature and effect of each flaw be provided, as well as the status of finding a correction to that flaw;

b) require that corrective actions be identified for each of the security flaws and the flaw remediation procedures documentation describes the methods used to provide flaw information, corrections, and guidance on corrective actions to TOE users; and

c) describe the means by which the developer receives reports and enquiries of suspected security flaws in the TOE from TOE users. The procedures for processing reported security flaws:

ensure that reported flaws are corrected and the correction issued to TOE users, and

provide safeguards that corrections to these security flaws do not introduce any new flaws.

M.TESTCOV	An analysis of the TOE's test coverage demonstrates the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. This analysis demonstrates that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
M.TEST	A suitably configured TOE has been evaluated in a controlled networked environment to confirm that TOE functionality operates as specified, and that the product can remediate a representative set of well-known vulnerabilities from each of the vulnerability classes claimed by the developer. TOE functionality has also been evaluated in a real-world environment, using a representative set of network systems configured with known vulnerabilities. The TOE includes developer test documentation which consists of test plans, test procedure descriptions, expected test results and actual test results. The test documentation is sufficient to determine that the developer has systematically tested the TOE against both the functional specification and the high level design.
M.VULNER	The TOE includes vulnerability documentation which describes the strength of function analysis along with an analysis of obvious vulnerabilities in the TOE.

7 PROTECTION PROFILE CLAIMS

This ST does not make any Protection Profile claims.

8 RATIONALE

8.1 SECURITY OBJECTIVES RATIONALE

8.1.1 Threats and TOE Security Objectives

Table 6 provides a bi-directional mapping of Security Objectives to Threats. It shows that each of the threats is addressed by at least one of the objectives, and that each of the objectives addresses at least one of the threats. It is followed by a discussion of how each threat is addressed by the corresponding Security Objective(s).

	O.ADMIN_GUIDANCE	O.ADMIN_ROLE	O.AUDIT_DATA	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.GOOD_TESTING	O.MANAGE	O.MANAGE_CHANGE	O.MEDIATE_INFO	O.PEER_AUTH	O.TOE_ACCESS	O.SELF_PROTECT	O.SOUND_DESIGN	O.SOUND_TOE	O.TIME_STAMPS	O.TRUSTED_PATH	O.USER_GUIDANCE	O.VULN_ANAL_TEST
T.ADMIN_ERROR	X	X					X											
T.ADMIN_ROGUE		X	X	X	X													
T.AUDIT_COMP				X	X							X						
T.CRYPTO_COMP												X						
T.FLAWED_DESIGN								X					X					X
T.FLAWED_TOE						X		X						X				X
T.MALICIOUS_USER							X					X				X		
T.MASQUERADE											X					X	X	
T.MISSED_ACTIONS			X		X										X			
T.POOR_TEST						X												X
T.SPOOFING																X		
T.UNATTENDED_SESSION											X							
T.UNAUTH_ACCESS			X	X					X								X	
T.UNAUTH_PEER										X								
T.UNKNOWN_STATE	X												X					
T.USER_ERROR																	X	

Table 6 - Mapping of Security Objectives to Threats

T.ADMIN_ERROR — *An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.*

	O.ADMIN_GUIDANCE – The TOE will provide administrators with the necessary information for secure configuration and management of the TOE. O.ADMIN_ROLE – The TOE will provide administrator roles to isolate administrative actions, and to make the administrative functions available locally. The TOE limits the functions an administrator can perform in a given role. O.MANAGE – The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. Administrators have the capability to view configuration settings. For example, if the TNG Administrator made a mistake when configuring the rule-set, providing him/her the capability to view the rules affords him/her the ability to review the rules and discover any mistakes that might have been made.
T.ADMIN_ROGUE	*An administrator's intentions may become malicious resulting in user or TOE Security Functions (TSF) data being compromised.* O.ADMIN_ROLE – The TOE will provide administrator roles to isolate administrative actions, and to make the administrative functions available locally. The TOE limits the functions an administrator can perform in a given role. This is somewhat different than the part this objective plays in countering T.ADMIN_ERROR, in that it is presumed that separate individuals will be assigned separate roles. O.AUDIT_DATA – The TOE will provide the capability to detect and create records of security-relevant events associated with users. Administrator IDs will be recorded when any security relevant change is made to the TOE (e.g., creation, deletion, or alteration of access rights and privileges, etc.). Attributes used in the audit record generation process are also required to be bound to the subject, ensuring administrators are held accountable. O.AUDIT_PROTECT – The TOE will provide the capability to protect audit information. The TOE will protect against unauthorised modification or deletion of audit logs by a rogue administrator. O.AUDIT_REVIEW – The TOE will provide the capability to selectively view audit information. Only the Security Auditor role can review audit records.
T.AUDIT_COMP	*A malicious user or process may view audit records, cause*

	audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action. O.AUDIT_PROTECT – The TOE will provide the capability to protect audit information. The TOE will protect against unauthorised modification or deletion of audit logs by a rogue administrator. O.AUDIT_REVIEW – The TOE will provide the capability to selectively view audit information. Only the Security Auditor role can review audit records. O.SELF_PROTECT – The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure. The TOE ensures that the TSF can protect itself from users. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit log. Likewise, ensuring that the functions that protect the audit log are always invoked is also critical to the mitigation of this threat.
T.CRYPTO_COMP	*A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.* O.SELF_PROTECT – The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure. The TOE ensures that the TSF can protect itself from unauthorized users. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the cryptographic data and executable code.
T.FLAWED_DESIGN	*Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.* O.MANAGE_CHANGE – The configuration of, and all changes to, the TOE and its development evidence will be analyzed, tracked and controlled throughout the TOE's development. O.SOUND_DESIGN – The TOE will be designed using sound design principles and techniques. The TOE design, design principles and design techniques will be adequately and accurately documented.

	O.VULN_ANAL_TEST – The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE and does not allow attackers to violate the TOE's security policies. The design of the TOE is tested for obvious vulnerabilities that could have arisen from design flaws.
T.FLAWED_TOE	*Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.*
	O.GOOD_TESTING – The TOE will undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements. Although the previous two objectives help minimize the introduction of errors into the implementation, this objective increases the likelihood that any errors that do exist in the implementation (with respect to the functional specification, high level, and low-level design) will be discovered through testing.
	O.MANAGE_CHANGE – The configuration of, and all changes to, the TOE and its development evidence will be analyzed, tracked and controlled throughout the TOE's development.
	O.SOUND_TOE – The implementation of the TOE will be an accurate instantiation of its design, and is adequately and accurately documented.
	O.VULN_ANAL_TEST – The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE and does not allow attackers to violate the TOE's security policies. the implementation of the TOE is tested for obvious vulnerabilities that could have arisen from a flawed implementation.
T.MALICIOUS_USER	*A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted). This threat class includes malicious software threats (e.g., viruses, Trojans, etc.).*
	O.MANAGE – The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. The TOE provides the capability to restrict access to TSF to those who are authorized to use the functions. Satisfaction of this objective (and its associated requirements) prevents

	unauthorized access to TSF functions and data through the administrative mechanisms. O.SELF_PROTECT – The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure. The TOE ensures that the TSF is able to protect itself from tampering and that the security mechanisms in the TSF cannot be bypassed. Without this objective, there is no assurance that users could not view or modify TSF data or TSF executables. O.TRUSTED_PATH – The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data. The TOE ensures that there is a trusted communication path between the TSF and various users (administrators, and trusted IT entities (for performing replication, for instance)). This ensures that the transmitted data cannot be compromised or disclosed during the duration of the trusted path. The protection offered by this objective is limited to TSF data, including authentication data and all data sent or received by trusted IT entities (a relying party's user data is not protected; only the authentication portion of the session is protected).
T.MASQUERADE	*A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.* O.TOE_ACCESS – The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate. Logical access to the TOE and its resources is controlled. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator with the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE. O.TRUSTED_PATH – The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data. The TOE ensures that there is a trusted communication path between the TSF

	and various users (administrators, and trusted IT entities (for performing replication, for instance)). This ensures that the transmitted data cannot be compromised or disclosed during the duration of the trusted path. The protection offered by this objective is limited to TSF data, including authentication data and all data sent or received by trusted IT entities (a relying party's user data is not protected; only the authentication portion of the session is protected). O.USER_GUIDANCE – The TOE will provide users with the information necessary to correctly use the security mechanisms.
T.MISSED_ACTIONS	*The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.* O.AUDIT_DATA – The TOE will provide the capability to detect and create records of security-relevant events associated with users. Administrator IDs are recorded when any security relevant change is made to the TOE (e.g., creation, deletion, or alteration of access rights and privileges, etc.). Attributes used in the audit record generation process are also required to be bound to the subject, ensuring administrators are held accountable. O.AUDIT_REVIEW – The TOE will provide the capability to selectively view audit information. Only the Security Auditor role can review audit records. O.TIME_STAMPS – The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
T.POOR_TEST	*Insufficient testing to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behaviour being undiscovered thereby causing potential security vulnerabilities.* O.GOOD_TESTING – The TOE will undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements. Although the previous two objectives help minimize the introduction of errors into the implementation, this objective increases the likelihood that any errors that do exist in the implementation (with respect to the functional specification, high level, and low-level design) will be discovered through testing. O.VULN_ANAL_TEST – The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and

	implementation of the TOE and does not allow attackers to violate the TOE's security policies. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing.
T.SPOOFING	*A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.*
	O.TRUSTED_PATH – The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data. It is possible for an entity other than the TOE (a subject on the TOE, or another IT entity on the network between the TOE and the end user) to provide an environment that may lead a user to mistakenly believe they are interacting with the TOE, thereby fooling the user into divulging identification and authentication information. This security objective mitigates this threat by ensuring users have the capability to ensure they are communicating with the TOE when providing identification and authentication data to the TOE.
T.UNATTENDED_SESSION	*A user may gain unauthorized access to an unattended TOE session.*
	O.TOE_ACCESS – The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
T.UNAUTH_ACCESS	*A user may gain access to user data for which they are not authorized according to the TOE security policy.*
	O.AUDIT_DATA – The TOE will provide the capability to detect and create records of security-relevant events associated with users. User IDs are recorded when any security relevant action is made or attempted by a user. Attributes used in the audit record generation process are bound to the subject, ensuring users are held accountable for their actions.
	O.AUDIT_PROTECT – The TOE will provide the capability to protect audit information. The TOE protects against unauthorised access, modification or deletion of audit log attempts by a user.
	O.MEDIATE_INFO – The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy. This objective works to

	mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies.
	O.USER_GUIDANCE – The TOE will provide users with the information necessary to correctly use the security mechanisms. This objective helps to mitigate this threat by providing the user the information necessary to use the security mechanisms that control access to user data in a secure manner. If this guidance was not available to the user, information could be left unprotected, or the user could mis-configure the controls and unintentionally allow unauthorized access to their data.
T.UNAUTH_PEER	*An unauthorized IT entity may attempt to establish a security association with the TOE.*
	O.PEER_AUTH – The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE. This objective mitigates the threat by ensuring that IT entities attempting to establish communications with the TOE are authenticated before permitting the communications to proceed.
T.UNKNOWN_STATE	*When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.*
	O.ADMIN_GUIDANCE – The TOE will provide administrators with the necessary information for secure configuration and management of the TOE.
	O.SOUND_DESIGN – The TOE will be designed using sound design principles and techniques. The TOE design, design principles and design techniques will be adequately and accurately documented.
T.USER_ERROR	*A user error could lead to the incorrect operation of the TOE (e.g., hardware or software fault).*
	O.USER_GUIDANCE – The TOE will provide users with the information necessary to correctly use the security mechanisms. This objective mitigates the threat by providing the user the information necessary to use the TOE functionality correctly and securely.

8.1.2 Assumptions and IT Environment Objectives

Table 7 provides a bi-directional mapping of Assumptions to Security Objectives for the IT Environment. Since the Security Objectives for the IT Environment were derived directly from the Assumptions there is a one to one mapping between them. It is also clear since the Security

Objectives for the IT Environment are simply a restatement of the applicable assumption, that each objective is suitable to meet its corresponding assumption.

	OE.AVAILABILITY	OE.CONNECT	OE.GOOD_ADMIN	OE.NO_BYPASS	OE.NO_GEN_PURPOSE	OE.NO_MAINT_PORT	OE.PHYSICAL
A.AVAILABILITY	X						
A.CONNECT		X					
A.GOOD_ADMIN			X				
A.NO_BYPASS				X			
A.NO_GEN_PURPOSE					X		
A.NO_MAINT_PORT						X	
A.PHYSICAL							X

Table 7 - Mapping of Assumptions to Security Objectives for the IT Environment

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 Security Functional Requirements Rationale

Table 8 provides a bi-directional mapping of Security Functional Requirements to TOE Security Objectives. The functional requirements satisfied by the TOE are listed first, followed by the functional requirements which are satisfied by the IT environment. Table 8 demonstrates that each of the applicable objectives for the TOE is addressed by at least one of the functions and that each of the functions addresses at least one of the objectives. The table is followed by a discussion of how each applicable Security Objective is addressed by the corresponding Security Functional Requirements. It should be noted that some of the TOE Security Objectives are satisfied by Assurance Requirements rather than Functional Requirements. These objectives are discussed in Section 8.2.3.

	O.ADMIN_ROLE	O.AUDIT_DATA	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.MANAGE	O.MEDIATE_INFO	O.PEER_AUTH	O.TOE_ACCESS	O.SELF_PROTECT	O.TIME_STAMPS	O.TRUSTED_PATH
FAU_ARP.1				X							

	O.ADMIN_ROLE	O.AUDIT_DATA	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.MANAGE	O.MEDIATE_INFO	O.PEER_AUTH	O.TOE_ACCESS	O.SELF_PROTECT	O.TIME_STAMPS	O.TRUSTED_PATH
FAU_GEN.1		X									
FAU_GEN.2		X									
FAU_SAA.1				X							
FAU_SAR.1				X							
FAU_SAR.2			X								
FAU_STG.1			X								
FAU_STG.4			X								
FCS_COP.1							X				X
FDP_ACC.1								X			
FDP_ACF.1								X			
FDP_DAU.1									X		
FDP_IFC.1						X					
FDP_IFF.1						X					
FDP_ITC.1								X			
FDP_ITT.1								X			
FIA_AFL.1(1)								X			
FIA_ATD.1(1)								X			
FIA_UAU.2(1)								X			
FIA_UID.2(1)								X			
FMT_MOF.1(1)			X		X						
FMT_MOF.1(2)			X		X						
FMT_MOF.1(3)			X		X						
FMT_MSA.1					X						
FMT_MSA.2					X						
FMT_MSA.3					X						
FMT_MTD.1(1)					X						
FMT_MTD.1(2)					X						
FMT_MTD.3					X						
FMT_SMF.1			X		X					X	

	O.ADMIN_ROLE	O.AUDIT_DATA	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.MANAGE	O.MEDIATE_INFO	O.PEER_AUTH	O.TOE_ACCESS	O.SELF_PROTECT	O.TIME_STAMPS	O.TRUSTED_PATH
FMT_SMR.1	X										
FPT_ITT.2						X					
FPT_RVM.1(1)						X					
FPT_SEP.1(1)									X		
FPT_STM.1(1)		X								X	
FTP_TRP.1											X
FAU_SAR.3				X							
FAU_SEL.1		X									
FIA_AFL.1(2)								X			
FIA_ATD.1(2)	X				X						
FIA_SOS.1	X				X			X			
FIA_UAU.2(2)								X			
FIA_UID.2(2)								X			
FIA_UAU.6								X			
FPT_RVM.1(2)						X			X		
FPT_SEP.1(2)									X		
FPT_STM.1(2)										X	

Table 8 - Mapping of Security Functional Requirements to TOE Security Objectives

O.ADMIN_ROLE — *The TOE will provide administrator roles to isolate administrative actions, and to make the administrative functions available locally.*

The TOE implements administrative roles as defined by FMT_SMR.1.

O.AUDIT_DATA — *The TOE will provide the capability to detect and create records of security-relevant events associated with users.*

The FAU_GEN.1 requirement defines the events for which the TOE will create an audit record and the data which is to be recorded in each audit record. FAU_GEN.2 ensures that each audit record is associated with the user who caused the event which resulted in the creation of the audit record.

	Finally, the FPT_STM.1(1) requirement ensures that the TOE is able to generate accurate time stamps for use in recording and identifying audit records.
O.AUDIT_PROTECT	*The TOE will provide the capability to protect audit information.* The FAU_SAR.2 requirement restricts access to the audit logs only to users who have been explicitly granted read access to the logs. FAU_STG.1 requires that the audit logs be protected from unauthorized change or deletion. FAU_STG.4 defines the actions that the TOE must take to minimize the impact of audit data loss in the event of audit storage exhaustion. Three iterations of the FMT_MOF.1 requirement ensure that the control of the audit functions and the ability to delete the audit logs are restricted to administrative accounts (TNG Manager and TNG Administrator). Finally, the FMT_SMF.1 requirement specifies the permitted management activities with respect to the audit logs.
O.AUDIT_REVIEW	*The TOE will provide the capability to selectively view audit information and alert the administrator to identified potential security violations.* The FAU_SAR.1 requirement ensures that the TOE is capable of presenting the audit data in a way that it can be interpreted. The FAU_ARP.1 and FAU_SAA.1 requirements work together to define the alarm capabilities required by the TOE. FAU_SAA.1 defines the rules which determine when an alarm condition is reached, while FAU_SAA.1 defines the action that the TOE will take when an alarm condition is detected.
O.MANAGE	*The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.* The FMT_SMF.1 functional requirement specifies the management functions which must be implemented by the TOE. The three iterations of the FMT_MOF.1 requirement specifies the restrictions which prevent unauthorized use of these TOE management functions. The FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3 requirements define how the TOE manages and protects the security attributes which control its behaviour, while the FMT_MTD.1(1), FMT_MTD.1(2) and FMT_MTD.3 requirements perform the same function for the security data (audit logs) produced

	by the TOE.
O.MEDIATE_INFO	*The TOE must mediate the flow of information between sets of TOE network interfaces or between a network interface and the TOE itself in accordance with its security policy.* This objective defines the primary function of the TOE, which is to mediate the flow of information between the networks connected to the TOE. The TOE implements this flow control via its UNAUTHENTICATED INFORMATION FLOW Security Functional Policy which is defined by the FDP_IFF.1 requirement. The enforcement of the SFP is dictated by the requirements of FDP_IFC.1. Additional requirements for the protection of the information flowing through the TOE are specified by FPT_ITT.2. The FPT_RVM.1 requirement dictates that information flowing between the networks connected to the TOE, must pass through the TOE and therefore must be subject to the SFP.
O.PEER_AUTH	*The TOE will authenticate each peer TOE that attempts to establish a security association with the TOE.* The FCS_COP.1 requirement (see Table 3) defines the cryptographic algorithm standard and key size that the TOE must use in order to authenticate each external IT entity which attempts to establish a security association with the TOE.
O.TOE_ACCESS	*The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.* The FDP_ACC.1 requirement specifies that the TOE will enforce the AUTHENTICATED USER ACCESS CONTROL Security Functional Policy on individual users who attempt to access the TOE. This SFP is defined by the FDP_ACF.1 requirement. The FDP_ITC.1 requirement specifies that the TOE will enforce either the AUTHENTICATED USER ACCESS CONTROL SFP or the UNAUTHENTICATED INFORMATION FLOW CONTROL SFP when importing user data from outside the TOE. The FDP_ITT.1 requirement specifies that the TOE will enforce the AUTHENTICATED USER ACCESS CONTROL SFP when transmitting data between physically separate components of the TOE. The IT Environment (TEMT) is required to identify and authenticate administrative users on behalf of the TOE. The

	IT Environment maintains two accounts which are permitted to access the TOE. Each of these accounts is associated with one of the TOE's two administrative roles. The IT Environment is required to identify and authenticate each user before performing any other action on behalf of that user (including permitting access to the TEMS) as described by FIA_UAU.2(2) and FIA_UID.2(2). In addition, the IT Environment is required to re-authenticate users after 15 minutes of inactivity on the TEMT (FIA_UAU.6). The TEMS software authenticates to a TNG(HQ) on behalf of an administrative user. The TNG(HQ) operating system requires identification and authentication before performing any action on behalf of a user as required by FIA_UID.2(1) and FIA_UAU.2(1) The actions to be taken by the TOE and the IT Environment in the event of authentication failure are specified by the FIA_AFL.1(1) and FIA_AFL.1(2) requirements respectively.
O.SELF_PROTECT	*The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure.* The FDP_DAU.1 requirement dictates that the TOE will provide self protection through the use of a hashing mechanism and digital signature to validate any updates to the firmware. The FPT_SEP.1 requirement ensures that the TOE maintains a domain for its own execution, thereby protecting itself and its resources from external interference, tampering and unauthorized disclosure.
O.TIME_STAMPS	*The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.* The FPT_STM.1 requirement dictates that the TOE provide reliable time stamps for its own use, which the FMT_SMF.1 requirements ensures that the TOE provides a management function which allows suitably authorized administrators to set the time used for the time stamps.
O.TRUSTED_PATH	*The TOE will provide a means to ensure that users are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.* The FTP_TRP.1 requirement specifies the details of a trusted communications path which the TOE must establish between itself and individual administrative users for local administrative connections. The cryptographic algorithm standards and key sizes which the TOE must implement are

defined by the FCS_COP.1 requirement.

8.2.2 IT Environment Security Functional Requirements

The TOE relies upon its IT environment in order to fully meet many of its security objectives. This reliance is made clear from the mappings in Table 8 and the rationale in the previous section. All of the security functional requirements levied upon the IT Environment map directly to Security Objectives of the TOE. However none of the security objectives of the TOE are satisfied solely by security functional requirements of the IT Environment. For these reasons, the ST authors have elected not to contrive additional Environmental Security Objectives the only purpose for which would be to permit a mapping of environmental security functional requirements. Rather, readers should understand that a combination of TOE security functional requirements and IT Environment security functional requirements are necessary to meet many of the Security Objectives of the TOE.

8.2.3 Assurance Requirements Rationale

For business competitive reasons, GDC has decided that the TOE will be evaluated at EAL2, augmented with flaw remediation. This combination is termed EAL2+. This provides a level of independently assured security that is consistent with the postulated threat environment. Specification of EAL2+ includes the vulnerability assessment component AVA_VLA.1, Developer vulnerability analysis, which aids in providing assurance that the product will be able to cope with some of the malicious attacks implied by attackers.

Table 9 below shows a mapping between selected TOE security objectives (those not satisfied exclusively by security functional requirements) and the security assurance requirements which satisfy the objective.

	O.ADMIN_GUIDANCE	O.GOOD_TESTING	O.MANAGE_CHANGE	O.SOUND_DESIGN	O.SOUND_TOE	O.USER_GUIDANCE	O.VULN_ANAL_TEST
ACM_CAP.2			X				
ADO_IGS.1	X	X		X	X		X
ADV_FSP.1				X	X		
ADV_HLD.1				X	X		
ADV_RCR.1				X	X		
AGD_ADM.1	X						
AGD_USR.1						X	
ALC_FLR.1			X		X	X	

	O.ADMIN_GUIDANCE	O.GOOD_TESTING	O.MANAGE_CHANGE	O.SOUND_DESIGN	O.SOUND_TOE	O.USER_GUIDANCE	O.VULN_ANAL_TEST
ATE_COV.1		X			X		
ATE_FUN.1		X			X		X
ATE_IND.2		X			X		X
AVA_VLA.1		X					X

Table 9 - Mapping of Security Assurance Requirements to TOE Security Objectives

8.2.4 Functional Requirement Dependencies Rationale

8.2.4.1 Dependency Analysis

Table 10 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components which are hierarchical to the specified dependency. Justification for any dependencies which are not satisfied is listed at the end of Table 10.

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FAU_ARP.1	FAU_SAA.1	Yes	
FAU_GEN.1	FPT_STM.1	Yes	The TOE and the IT Environment share the responsibility for meeting the requirements of FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes Yes	 FIA_UID.2 is hierarchical to FIA_UID.1 The TOE and the IT Environment share the responsibility for meeting the requirements of FIA_UID.2.
FAU_SAA.1	FAU_GEN,1	Yes	
FAU_SAR.1	FAU_GEN.1	Yes	
FAU_SAR.2	FAU_SAR.1	Yes	
FAU_STG.1	FAU_GEN.1	Yes	
FAU_STG.4	FAU_STG.1	Yes	

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	No No Yes	See Section 8.2.4.2 See Section 8.2.4.2
FDP_ACC.1	FDP_ACF.1	Yes	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes	
FDP_DAU.1	None	N/A	
FDP_IFC.1	FDP_IFF.1	Yes	
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes Yes	
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.3	Yes Yes	Both FDP_ACC.1 and FDP_IFC.1 are claimed.
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Both FDP_ACC.1 and FDP_IFC.1 are claimed.
FIA_AFL.1(1)	FIA_UAU.1	Yes	FIA_UAU.2 is hierarchical to FIA_UAU.1 and the FIA_UAU.2(1) iteration is included in the ST. Note that the FIA_UAU.2(1) iteration applies to the TOE (TNG(HQ)) while the FIA_UAU.2(2) iteration applies to the IT Environment (TEMT).
FIA_ATD.1(1)	None	N/A	
FIA_UAU.2(1)	FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1 and the FIA_UID.2(1) iteration is included in the ST. Note that the FIA_UID.2(1) iteration applies to the TOE (TNG(HQ)) while the FIA_UID.2(2) iteration applies to the IT Environment (TEMT).
FIA_UID.2(1)	None	N/A	
FMT_MOF.1(1)	FMT_SMR.1 FMT_SMF.1	Yes Yes	
FMT_MOF.1(2)	FMT_SMR.1 FMT_SMF.1	Yes Yes	
FMT_MOF.1(3)	FMT_SMR.1 FMT_SMF.1	Yes Yes	

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Yes	Both FDP_ACC.1 and FDP_IFC.1 are claimed.
	FMT_SMR.1	Yes	
	FMT_SMF.1	Yes	
FMT_MSA.2	ADV_SPM.1	No	See Section 8.2.4.2
	FDP_ACC.1 or FDP_IFC.1	Yes	Both FDP_ACC.1 and FDP_IFC.1 are claimed.
	FMT_MSA.1	Yes	
	FMT_SMR.1	Yes	
FMT_MSA.3	FMT_MSA.1	Yes	
	FMT_SMR.1	Yes	
FMT_MTD.1(1)	FMT_SMR.1	Yes	
	FMT_SMF.1	Yes	
FMT_MTD.1(2)	FMT_SMR.1	Yes	
	FMT_SMF.1	Yes	
FMT_MTD.3	ADV_SPM.1	No	See Section 8.2.4.2
	FMT_MTD.1	Yes	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1. The TOE and the IT Environment share the responsibility for meeting the requirements of FIA_UID.2.
FPT_ITT.2	None	N/A	
FPT_RVM.1(1)	None	N/A	
FPT_SEP.1(1)	None	N/A	
FPT_STM.1(1)	None	N/A	
FTP_TRP.1	None	N/A	
FAU_SAR.3	FAU_SAR.1	No	See Section 8.2.4.2
FAU_SEL.1	FAU_GEN.1	No	See Section 8.2.4.2
	FMT_MTD.1	No	See Section 8.2.4.2
FIA_AFL.1(2)	FIA_UAU.1	Yes	FIA_UAU.2 is hierarchical to FIA_UAU.1 and the FIA_UAU.2(2) iteration is included in the ST. Note that the FIA_UAU.2(2) iteration applies to the IT Environment (TEMT) while the FIA_UAU.2(1) iteration applies to the TOE (TNG(HQ)).

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FIA_ATD.1(2)	None	N/A	
FIA_SOS.1	None	N/A	
FIA_UAU.2(2)	FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1 and the FIA_UID.2(2) iteration is included in the ST. Note that the FIA_UID.2(2) iteration applies to the IT Environment (TEMT) while the FIA_UID.2(1) iteration applies to the TOE (TNG(HQ)).
FIA_UID.2(2)	None	N/A	
FIA_UAU.6	None	N/A	
FPT_RVM.1(2)	None	N/A	
FPT_SEP.1(2)	None	N/A	
FPT_STM.1(2)	None	N/A	

Table 10 - Security Functional Requirement Dependencies

8.2.4.2 Justification for Unsatisfied Dependencies

8.2.4.2.1 FMT_MSA.2 / FMT_MTD.3 (dependency on ADV_SPM.1)

The ADV_SPM.1 assurance requirement is a dependency of both the FMT_MSA.2 (Secure security attributes) and the FMT_MTD.3 (Secure TSF data) functional requirements. However in both cases, the Administrator Guidance provided by the developer will define the secure values for the “security attributes” and the “secure TSF data” and show why these values may be considered secure. As a result, there is no requirement to produce a TSP model in order to accomplish the same result.

8.2.4.2.2 FCS_COP.1 (dependency on FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)

The dependencies of FCS_COP.1 on either FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 are intended to define how the key(s) for the algorithm(s) defined by FCS_COP.1 are generated. However, the key used by the TOE for the AES algorithm is installed in the hardware during production and remains unchanged throughout the life of the TOE. For this reason the TOE does not require key generation support for its implementation of the AES algorithm.

8.2.4.2.3 FCS_COP.1 (dependency on FCS_CKM.4)

As noted in the previous paragraph, the key used by the TOE for the AES algorithm is installed in the hardware during production and remains unchanged throughout the life of the TOE. Before the TOE reaches the customer, this key is protected by the secure delivery measures employed by the TOE developer. After the TOE is placed into service, the key is protected both by the physical measures employed to protect the TOE in its operating environment and the access control measures implemented by the TOE. Since the key does not change, key destruction is not required.

8.2.4.2.4 FAU_SAR.1 (IT Environment) / FAU_GEN.1 (IT Environment) / FMT_MTD.1 (IT Environment)

The TOE depends on its IT environment for assistance with certain audit and identification and authentication functions. For this reason there are several functional requirements levied on the IT Environment which in turn have dependencies. While these dependent functional requirements are listed in this ST as requirements of the TOE, in the purest sense, dependencies of requirements levied on the IT Environment should be met by environmental requirements. However expanding the list of environmental requirements in this manner is not considered necessary or useful. The operating environment of the TOE consists of the Windows 2000 operating system which has been evaluated at the EAL 4 level and included all of the requirements listed at the top of this paragraph as unsatisfied dependencies. For this reason, these requirements have been excluded from the ST and only the primary requirements of the IT Environment have been listed.

8.2.5 Assurance Requirement Dependencies Rationale

Table 11 identifies the Security Assurance Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency

Security Assurance Requirement	Dependencies	Dependency Satisfied
ACM_CAP.2	None	N/A
ADO_DEL.1	None	N/A
ADO_IGS.1	AGD_ADM.1	Yes
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.1	ADV_FSP.1	Yes
	ADV_RCR.1	Yes
ADV_RCR.1	None	N/A
AGD_ADM.1	ADV_FSP.1	Yes
AGD_USR.1	ADV_FSP.1	Yes
ALC_FLR.1	None	N/A
ATE_COV.1	ADV_FSP.1	Yes
	ATE_FUN.1	Yes
ATE_FUN.1	None	N/A
ATE_IND.2	ADV_FSP.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes
	ATE_FUN.1	Yes
AVA_SOF.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes

Security Assurance Requirement	Dependencies	Dependency Satisfied
AVA_VLA.1	ADV_FSP.1	Yes
	ADV_HLD.1	Yes
	AGD_ADM.1	Yes
	AGD_USR.1	Yes

Table 11 - Security Assurance Requirement Dependencies

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 TOE Security Functions Rationale

Table 12 provides a bi-directional mapping of Security Functions to Security Functional Requirements. It shows that each of the SFRs is addressed by at least one of the Security Functions and that each of the Security Functions addresses at least one of the SFRs. The table is followed by a discussion of how each Security Functional Requirement is addressed by the corresponding Security Function.

	F.HMI	F.REF_MEDIATE	F.AUDIT	F.CRYPTO	F.INFO_FLOW_CTRL	F.ACCESS_CTRL	F.DOMAIN	F.TIME	F.TRUSTED_COMMS
FAU_ARP.1			X						
FAU_GEN.1			X						
FAU_GEN.2			X						
FAU_SAA.1			X						
FAU_SAR.1			X						
FAU_SAR.2			X						
FAU_STG.1			X						
FAU_STG.4			X						
FCS_COP.1				X					
FDP_ACC.1						X			
FDP_ACF.1						X			

	F.HMI	F.REF_MEDIATE	F.AUDIT	F.CRYPTO	F.INFO_FLOW_CTRL	F.ACCESS_CTRL	F.DOMAIN	F.TIME	F.TRUSTED_COMMS
FDP_DAU.1	X								
FDP_IFC.1					X				
FDP_IFF.1					X				
FDP_ITC.1						X			
FDP_ITT.1									X
FIA_AFL.1(1)						X			
FIA_ATD.1(1)						X			
FIA_UAU.2(1)						X			
FIA_UID.2(1)						X			
FMT_MOF.1(1)	X								
FMT_MOF.1(2)	X								
FMT_MOF.1(3)	X								
FMT_MSA.1	X								
FMT_MSA.2	X								
FMT_MSA.3	X								
FMT_MTD.1(1)	X								
FMT_MTD.1(2)	X								
FMT_MTD.3	X								
FMT_SMF.1	X								
FMT_SMR.1	X								
FPT_ITT.2									X
FPT_RVM.1(1)		X							
FPT_SEP.1(1)							X		
FPT_STM.1(1)								X	
FTP_TRP.1									X

Table 12 - Mapping of Security Functions to Security Functional Requirements

FAU_ARP.1 Security alarms

F.AUDIT satisfies the requirement for security alarms. The TEMT configures and sends update requests to the oNAUs, and the oNAUs download event/log files to the TEMT on an as-requested or as-configured basis. The TNG oNAUs use SNMP to create traps, the details of which are either recorded in local logs or sent back to an associated TEMT (via SSH sessions). Some of these events are considered alarms/alerts and are displayed as notices onscreen on the TEMT as well as being included in logs.

FAU_GEN.1 Audit data generation

F.AUDIT satisfies the requirement for audit data generation. The TEMT configures and sends update requests to the oNAUs, and the oNAUs download event/log files to the TEMT on an as-requested or as-configured basis.

The TNG oNAUs are capable of generating audit records for all of the events defined in FAU_GEN1.1. The TNG oNAUs are also capable of generating for each audit record the audit information defined in FAU_GEN1.2.

The TNG oNAUs use SNMP to create traps, the details of which are either recorded in local logs or sent back to an associated TEMT (via SSH sessions). Some of these events are considered alarms/alerts and are displayed as notices onscreen on the TEMT as well as being included in logs. Logs sent back from the oNAUs to the TEMT are exported/imported in Rich Text Format (RTF) in order to be readable and parsable by the Windows XML Notepad. For audit purposes, a flag or delimiter within the ASCII text file denoting the event as “security” is used.

The standard Windows Event viewer can search the standard Windows logs (security, application, system), parse those events and allow viewing.

FAU_GEN.2 User identity association

The F.AUDIT security function dictates that each audit record include all the information necessary to scope the event including the event type and the management terminal commanding the event. For audit events recorded by the TEMS, the audit information will identify which administrative account is associated with the auditable event. For audit records recorded by the TNG(HQ), the audit information will include the appropriate NetBSD account identification.

FAU_SAA.1 Potential violation analysis

The F.AUDIT security function requires the TOE to apply a set of rules in monitoring events and based upon those rule to indicate a potential violation of the TSP both via alarms and through the creation of audit records. The F.AUDIT function entirely satisfies the requirements of the FAU_SAA.1 requirement.

FAU_SAR.1 Audit review

F.AUDIT satisfies the requirement for audit review. TNG(HQ) logs sent back from the oNAUs to the TEMT are exported/imported in ASCII text format in order to be readable and parsable by the Windows XML Notepad. For audit purposes, a flag or delimiter within the ASCII text file denoting the event as “security” is used.

The log files are exported to and stored on the TEMT in an access-controlled directory. As required by the TNG Administrator or TNG Manager it will be possible to parse through these files and pick out security events for viewing using Windows XML Notepad.

Note that the TEMT's Windows Application and System logs are reviewable by both the TNG Manager and the TNG Administrator roles via the Windows Event Viewer. The TEMT's Windows Security log is viewable (and deletable) only by the TNG Administrator as a defined Windows security auditor.

FAU_SAR.2 Restricted audit review

F.AUDIT satisfies the requirement for restricted audit review. The TNG restricts access to security Audit functions, i.e. the Windows Security log, to authorised Security Auditors.

FAU_STG.1 Protected audit trail storage

F.AUDIT satisfies the requirement for audit trail storage. TNG(HQ) log files are retained except on command from the TEMS. Prior to allowing deletion of a log file the TEMS makes a check to ensure that the log file has been exported to its associated TEMT. When deletion of stored but unarchived or unexported log file is requested, a warning screen is displayed on the TEMT. Deletion of that unarchived / unexported file only takes place once explicit action has been taken by the user. The only access to the TNG(HQ) is via the TEMS software. As this application does not provide any functions which permit audit log modifications, it is not possible to modify the TNG(HQ) audit logs. Audit logs stored on the TEMT are protected by the Windows OS, which restricts access to the log files to administrative accounts. As noted in Section 3 (Assumptions) TOE administrators are assumed to be competent and to follow all administrative guidance.

FAU_STG.4 Prevention of audit data loss

F.AUDIT satisfies the requirement for prevention of audit data loss. If the space allocated to audit logs files has been exceeded then the TNG module automatically overwrites the earlier records in the same order as they were originally recorded.

FCS_COP.1 Cryptographic operation

F.CRYPTO satisfies the requirement for cryptographic operation. The TNG performs specified cryptographic operations in accordance with the specified cryptographic algorithms and cryptographic key sizes that meet specified FIPS/PKCS algorithm standards. The TNG implements the cryptographic algorithms associated with SSH (Advanced Encryption Standard (AES) -256 and Secure Hashing Algorithm (SHA) -1).

FDP_ACC.1 Subset access control

F.ACCESS_CTRL satisfies the requirement for subset access control:

a. TNG Manager: This TNG application specific power user is used for TNG(HQ) and TNG(Fw) day-to-day management functions, excluding (for TNG(HQ) firmware upgrade; and

b. TNG Administrator: The Administrator has control over all TEMT aspects including all functions contained in the TNG management applications, i.e., those functions assigned to the TNG Manager as well as firmware upgrade capability. The TNG Administrator is considered to be the TNG Security Auditor and is therefore the only TNG user to be allowed access to the TEMT Windows security log.

FDP_ACF.1 Security attribute based access control

F.ACCESS_CTRL satisfies the requirement for subset access control. The TNG incorporates a role-based access control capability that defines tasks that authorized (management) users are allowed to perform. The TNG oNAUs do not perform authentication as an authenticated user of the TEMT has the right to request a SSH session of a particular TNG agent. For example: using the TEMS (on the TEMT) the TNG Administrator is allowed to perform FW upgrades, but the TNG Manager does not have access to the FW upgrade function. The TNG application will therefore not allow the TNG Manager access to the FW upgrade function. The GUI will be greyed out for the TNG Manager. Thus, a request to the oNAU to perform FW upgrade (or more correctly, to establish a SSH session to the FW Upgrade agent on the oNAU) will only come from the approved user - the TNG Administrator, who can access that GUI on the TEMT. The authentication as TNG Administrator or TNG Manager is done via standard Windows login. The TEMS proper will only be accessible by these two accounts. Further, access to some functionality GUIs are restricted to specific users within the application itself.

All management commands are authenticated. There is access control/authentication on the TEMT and then the assumption by the TNG oNAUs regarding if a SSH session can be opened, then the user is authorized and logged into the appropriate NetBSD account. Each management agent on the oNAU is associated with a specific NetBSD user account. When TEMS (external access) asks to connect with that agent and use its functionality, the TEMS (and hence the TNG Manager) are logged in as that user account. These user accounts (TNG Manager and TNG Administrator) are only available through authenticated SSH sessions. Management data is transferred between the TEMS and the TNG(HQ) via SSH sessions. Management/configuration data is protected during transfer between the TEMT and the TNG(HQ) and between peer TEMTs through the use of SSH sessions. In TEMTs, the TNG Manager account controls/initiates SSH sessions via the TEMS. Operating system user account types are not capable of being created, modified, or deleted except by firmware upgrade. The firmware (FW) upgrade use of digital signatures provides for the authentication and integrity of new FW loads. All management operations are preceded by SSH session initiation requests and operation are validated (after session establishment).

FDP_DAU.1

The F.HMI function includes the capability to upload updates of the TOE firmware including support for a hashing mechanism and digital signature. The upload mechanism will only be successful if the digital signature is verified. This capability allows the administrators of the TOE to confirm the validity of the update and meets the requirements of the Basic Data Authentication FDP_DAU.1 security functional requirement.

FDP_IFC.1 Subset information flow control

F.INFO_FLOW_CTRL satisfies the requirement for information flow control. For TNG(HQ) oNAU configurations, ports are configured with the security mode (Secure/Non-Secure) and data is routed through VLANs. If the security mode is set to Secure, all Non-Secure traffic is dropped. If the security mode is set to Non-Secure, all Secure traffic is dropped.

FDP_IFF.1 Simple security attributes

F.INFO_FLOW_CTRL satisfies the requirement for simple security attributes. In Secure mode all Non-Secure traffic is discarded; in Non-Secure mode all Secure traffic is discarded. Separate VLANs are used for Secure and Non-Secure traffic passing between TNG interfaces, and for

separating user data and management traffic, as well as preventing them from being mixed with voice traffic. Packets without the appropriate VLAN identification (either absent or misrouted) are discarded.

FDP_ITC.1 Import of user data without security attributes

F.ACCESS_CTRL satisfies the requirement for subset access control. In TEMTs, the TNG Manager or TNG Administrator account controls/initiates SSH sessions via the TEMS. TNG(HQ) operating system user account types are not capable of being created, modified, or deleted except by firmware upgrade. The firmware (FW) upgrade use of digital signatures provides for the authentication and integrity of new FW loads. Lack of a digital signature or failure to verify the digital signature aborts the upgrade function before a new image overwrites the alternate image. All management operations are preceded by SSH session initiation requests and operation are validated (after session establishment).

FDP_ITT.1 Basic internal transfer protection

F.TRUSTED_COMMS satisfies the requirement for basic internal transfer protection. Trusted paths provide communications between the TOE and local TNG Administrators.

FIA_AFL.1(1) Authentication failure handling

F.ACCESS_CTRL satisfies the requirement for authentication failure handling. The TNG(HQ) detects any unsuccessful authentication attempts and generates an audit record in response.

FIA_ATD.1(1) User attribute definition

F.ACCESS_CTRL satisfies the requirement for user attribute definition. The IT Environment (TEMT) maintains two accounts which are permitted to access the TOE. Each of these accounts is associated with a TOE role which determines which administrative functions are accessible to the user.

FIA_UAU.2(1) User identification before any action (TOE)

F.ACCESS_CTRL satisfies the requirement for user authentication before any action. The TOE (TNG(HQ)) requires identification and authentication before taking any action on behalf of a user. During normal operations, the TEMS application supplies the required identification and authentication parameters to the TNG(HQ) on behalf of the user.

FIA_UID.2(1) User identification before any action (TOE)

F.ACCESS_CTRL satisfies the requirement for user identification before any action. The TOE (TNG(HQ)) requires identification and authentication before taking any action on behalf of a user. During normal operations, the TEMS application supplies the required identification and authentication parameters to the TNG(HQ) on behalf of the user.

FMT_MOF.1(1), FMT_MOF.1(2) and FMT_MOF.1(3) Management of security functions behaviour

F.HMI satisfies the requirement for management of security functions behaviour. Tasks are restricted to the TNG Administrator and/or TNG Manager. Administrative access to the TOE shall be restricted to authorised administrators. Access control shall be provided through a set of defined profiles (roles) that permit specific administrative activities to be performed. The roles are defined in FMT_SMR.1.1, as are conditions on the roles.

FMT_MSA.1 Management of security attributes

F.HMI satisfies the requirement for management of security attributes. Tasks that are restricted to the TNG Administrator and/or TNG Manager are listed in the F.HMI portion of Section 6.

FMT_MSA.2 Secure security attributes

F.HMI satisfies the requirement for secure security attributes. Administrative access to the TOE is restricted to authorised administrators. Access control is provided through a set of defined profiles (roles) that permit specific administrative activities to be performed. The roles are defined in FMT_SMR.1.1, as are conditions on the roles. F.HMI ensures that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialization

F.HMI satisfies the requirement for static attribute initialization. The TNG enforces the restrictive default values for security attributes that are used to enforce the SFPs. The TNG Manager and TNG Administrator accounts are allowed to specify alternative initial values to override the default values.

FMT_MTD.1(1) and FMT_MTD.1(2) Management of TSF data

F.HMI satisfies the requirement for static attribute initialization. Only TNG Administrator and TNG Manager accounts can delete/clear TNG(HQ) archived audit logs. Both the TNG Administrator and TNG Manager accounts can query the Windows Application, Windows System and the archived TNG(HQ) audit logs. Only the TNG Administrator account (i.e., the TNG Security Auditor role)] can query or otherwise manipulate the Windows Security audit log.

FMT_MTD.3 Secure TSF data

F.HMI satisfies the requirement for secure TSF data ensuring that only secure values are accepted. The TEMT management application always checks the digital signature on keys (with the exception of the TNG Master public which is loaded prior) when updating or prior to their use by any TEMT function (e.g. SSH), uploaded FW upgrades (prior to transfer to an oNAU) and software applications.

FMT_SMF.1 Specification of Management Functions

F.HMI satisfies the requirement for specification of management functions. The TNG provides for the following functionality:

a. log file management;

b. key management;

c. FW upgrade;

d. National Identifier Area Code (NIAC) configuration;

e. Predetermined Multi-Address (PMA) lists for connected Ethernet network;

f. Frequently called number lists;

g. Status reports; and

h. BIT.

FMT_SMR.1 Security roles

F.HMI satisfies the requirement for security roles. TNG (Windows) accounts and their functionality are:

a. TNG Manager: TNG application specific Power User, used for TNG(HQ) and TNG(Fw) day-to-day management functions, excluding (for TNG(HQ) firmware upgrade; and

b. TNG Administrator: Administrator user, has control over all TEMT aspects including all functions contained in the TNG management applications, i.e., those functions assigned to the TNG Manager as well as firmware upgrade capability. The TNG Administrator is considered to be the TNG Security Auditor and therefore is the only TNG user to be allowed access to the TEMT Windows Security log.

TNG(HQ) user accounts are part of the overall approach to NetBSD secure configuration. They are used to control external access into the OS as well as for controlling the rights and privileges of the daemons that perform the various tasks. Each management agent on the oNAU is associated with a specific NetBSD user account. When TEMS (external access) asks to connect with that agent and use its functionality, the TEMS (and hence the TNG Manager) are logged in as that user account. Security considerations in this respect include control of rights and privileges as well as accountability.

FPT_ITT.2 TSF data transfer separation

F.TRUSTED_COMMS satisfies the requirement for TSF data transfer separation.

Management/configuration data is protected during transfer between the TEMT and the TNG(HQ) or the TNG(Fw) through the use of SSH sessions.

FPT_RVM.1(1) Non-bypassability of the TSP

F.REF_MEDIATE satisfies the requirement for non-bypassability of the TSP.

The TNG (HQ) modules (oNAUs) authenticate all management commands. The privileges and access are statically defined for each process and can only be changed by loading a new FW image.

The TNG (HQ) oNAUs' operating system provides separation between management traffic and operational traffic. The TNG(HQ) uses NetBSD version 3 as its OS. The privileges and access are statically defined for each process and this can only be changed by loading a new FW image.

FPT_SEP.1(1)

The TOE, via the F.DOMAIN security function, maintains a security domain for its own execution which protects it from interference or tampering by untrusted subjects. Further, this function ensures that the TOE assigns each subject to separate physical and logical interfaces, thereby enforcing separation between the security domains of the subjects. These features of F.DOMAIN satisfy the requirements of the FPT_SEP.1 security functional requirement.

FPT_STM.1(1) Reliable time stamps

F.TIME satisfies the requirement for reliable time stamps. The TOE provides reliable time stamps for its own use which includes audit record creation.

FTP_TRP.1 Trusted path

F.TRUSTED_COMMS satisfies the requirement for Trusted path. Management/configuration data is protected during transfer between the TEMT and the TNG(HQ), between peer TEMTs, or the TNG(Fw) through the use of SSH sessions.

8.3.2 TOE Assurance Measures Rationale

Table 13 provides a bi-directional mapping of Assurance Measures to Assurance Requirements. It shows that each of the Assurance Requirements is addressed by at least one of the Assurance Measures and that each of the Assurance Measures addresses at least one of the Assurance Requirements. Each assurance measure is discussed in Section 6.2.

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_FLR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
M.ID	X													
M.CMSYS	X													
M.GETTOE		X												
M.SETUP			X											
M.SPEC				X	X									
M.TRACE						X								
M.DOCS							X	X						
M.FLAWREM									X					
M.TESTCOV										X				
M.TEST											X	X		
M.VULNER													X	X

Table 13 - Mapping of Assurance Measures to Assurance Requirements

8.4 STRENGTH OF FUNCTION RATIONALE

The TNG provides a level of protection that is appropriate against obvious vulnerabilities in IT environments that require that information flows be controlled and restricted among network nodes where the TNG oNAUs and the TEMT can be appropriately protected from physical attack. The TEMT must be controlled to restrict access to only authorized administrators. It is expected that the TNG oNAUs will be protected to the extent necessary to ensure that they remain connected to the networks that they provide services to. The claimed minimum strength of function, SOF-Basic, is consistent with these requirements.

9 ACRONYMS, ABBREVIATIONS, AND INITIALIZATIONS

BGP	Border Gateway Protocol
BIT	Built In Test
BRI	Basic Rate Interface
CA	Certificate Authority
CC	Common Criteria
CM	Configuration Management
DTMF	Dual Tone Multi-Frequency
E1	
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
Fw	Firewall
FW	Firmware
GDC	General Dynamics Canada Ltd.
HQ	Headquarters
I&A	Identification and Authentication
ID	Identification
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
LRU	Line Replaceable Unit
MoD	Ministry of Defence
NIAC	National Identification Area Code
ONAU	Objective Network Access Unit
OSPF	Open Shortest Path First
PIB	Perth in a Box
PMA	Pre-determined Multi-Address
PP	Protection Profile
PRI	Primary Rate Interface
Pt	Ptarmigan
QSig	
SFP	Security Functional Policy

SFR	Security Functional Requirement
SOF	Strength of Function
SSH	Secure Socket Handler
ST	Security Target
STANAG	Standard NATO Agreement
TacISDN	Tactical Integrated Service Digital Network
TBD	To Be Determined
TEMS	TNG Equipment Management System
TEMT	TNG Equipment Management Terminal
TNG	Tactical Network-layer Gateway
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UK	United Kingdom
VEDS	Vehicle External Distribution System
VLAN	Virtual Local Area Network