5.08 NETWORK-TO-NETWORK CONNECTIVITY SECURITY STANDARD SPECIFICATIONS

Abstract

Supporting document for the IMIT 5.08 Network-to-Network Connectivity Security Standard. It provides clarification and additional requirements of the standard.

Information Security Branch

infosecadvisoryservices@gov.bc.ca

Contents

1. INTRODUCTION

This Specifications document was developed to provide detailed security requirements to support the IMIT 5.08 Network-to-Network Connectivity Security Standard (NNCSS). The specifications outlined in this document MUST be followed in conjunction with the IMIT 5.08 Network-to-Network Connectivity Security Standard.

2. DEFENSIBLE SECURITY LINKAGE

The IMIT 5.08 NNCSS establishes the baseline security measures required for third-party network connections (a.k.a. Business-to-Business). This is in accordance with the government's Defensible Security Framework for the protection of government information assets and government information systems.

The Defensible Security elements that relate to all IMIT security standards (highlighted in blue in the table below) are: Executive Support, Roles & Responsibilities, Incident Management, Policy (Information Security), Awareness Program/Courses, and Security Governance.

Additional elements specific to the NNCSS (highlighted in yellow) are: Risk Appetite & Register, Risk Assessment, Security Assessment, Asset Management, Change Management, Vendor Requirements, Backup & Retention, Logging & Monitoring, Logical Access, Defense-in-Depth (endpoints & networks), Vulnerability Management (VM) & Patching, Application Security (AppSec), Information Security (InfoSec) Classification.

Pre-requisites	Directives	Respiration	DNA (culture)
Executive Support	**Asset** Management	**Backup** & Retention	**Program** (Information Security)
Roles & Responsibilities	**Change** Management	**Logging** & Monitoring	**InfoSec** classification
Crown Jewels	Incident Management	**Physical** & Visible ID	**Awareness** Program/ Courses
Risk Appetite & Register	**BCP**	**Logical** Access	**Security** Governance
Risk Assessment	**DRP**	**Personnel** Security	
Security Assessment	**Incident** Response	**Defence**-in-Depth (endpoints & networks)	
	Policy (Information Security)	**VM** & Patching	

Pre-requisites	Directives	Respiration	DNA (culture)
	Vendor Requirements	**AppSec**	

3. RESPONSIBILITY ASSIGNMENT MATRIX CHART (RACI)

RACI: **R** = Responsible; **A** = Accountable; **C** = Consult; **I** = Inform

Network-to-Network Connectivity Security Standard Deliverables	**Roles**									
	Information Owner	**Information Custodian**	**Government Chief Information Officer (GCIO)**	**Ministry Chief Information Officer (MCIO)**	**Chief Information Security Officer (CISO)**	**Ministry Information Security Officer (MISO)**	**Executive / Director / Manager / Supervisor**	**Employee**	**Contractor**	**Vendor**
Firewall rules	**A**	**R**			**C**	**C**	**R**	**I**	**R**	**R**
Third-party gateway (3PG) connection requirements	**A**	**R**		**I**	**C**	**C**	**R**	**I**	**R**	**R**
Log files	**I**	**A**			**I**	**C**	**I**	**R**	**R**	**R**

4. ROLES & RESPONSIBILITIES

Information Owners are responsible for:

- Determining the requirements for the 3PG request; and
- Approving firewall rule requests and ensuring the requests comply with NNCSS.

Information Custodians are responsible for:

- Maintaining log files in accordance with Province's policies and standards; and
- Ensuring configuration details and architecture for the connectivity to external networks meet the requirements as identified by Information Owners.

Contractor is responsible for:

- Ensuring adherence to the information security terms as defined by contract.

Ministry Information Security Officers (MISOs) are responsible for:

- Assisting service delivery units within their portfolio to follow the NNCSS; and

- Ensuring the details and architecture for the connectivity to external networks meets the IMIT policies and standards.

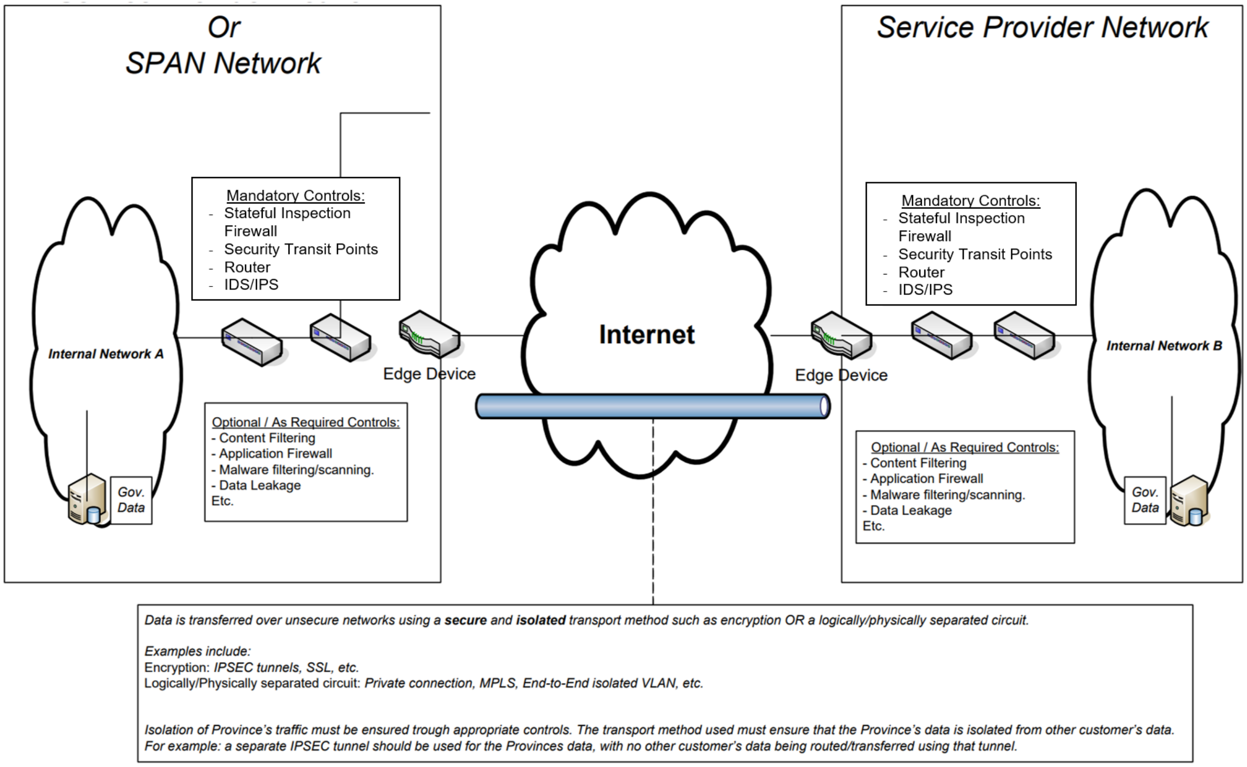
The OCIO's *Information Security Branch* is responsible for:

- The ongoing development, maintenance, continuous review, improvement, and support of the NNCSS;
- Monitoring the compliance of government organizations to the NNCSS;
- Providing related tools, templates, specifications, guidelines, process, documentation, and training to MISOs; and
- Configuration and Operation of the 3PG Security Transit Points.

5. SPECIFICATIONS

This document:

1. Establishes the 3PG service as the Provincial standard to connect to external (non-SPAN) networks;
2. Specifies specific security requirements for any external network connection that carries government data; and
3. Provides guidelines for network-to-network connections. This document applies to core government and authorized service providers.



Data is transferred over unsecure networks using a ***secure*** *and* ***isolated*** *transport method such as encryption OR a logically/physically separated circuit.*

Examples include:
Encryption: *IPSEC tunnels, SSL, etc.*
Logically/Physically separated circuit: *Private connection, MPLS, End-to-End isolated VLAN, etc.*

Isolation of Province's traffic must be ensured trough appropriate controls. The transport method used must ensure that the Province's data is isolated from other customer's data. For example: a separate IPSEC tunnel should be used for the Provinces data, with no other customer's data being routed/transferred using that tunnel.

Figure 1: Model for connection (ISO screened subnet)

5.1. Security Characteristics

The principles of least privilege apply.

5.1.1. All ports MUST be closed by default and all IP addresses should be hidden by default. Requests to open ports and IP addresses MUST be approved by the Information Owner and the Ministry owning the contract.

5.1.2. Internal addresses MUST be inaccessible by default.

5.1.3. Data transferred between networks:

a. A secure and isolated transport method MUST be used when transferring the Province's data. Data MUST be transferred between networks using encrypted tunnels, private network-to-network connections, or using traffic isolation technologies (e.g., Multi-Protocol Label Switching (MPLS), end-to-end isolated VLANs, etc.) to achieve a Virtual Private Network (VPN) type connectivity;

b. When encrypted VPN tunnels are used, VPN gateway devices might be required at each end of the circuit. This will allow for the connections to be decrypted before the mandatory controls (security transit point) and the optional/as-required controls (content filtering, malware detection, data leakage, etc.) are applied to the traffic.

c. Isolation of Province's traffic MUST be ensured through appropriate controls. The transport method used MUST ensure that the Province's data is isolated from other customers' data. The encrypted tunnels or the logically/physically separated circuits used (e.g., private network-to-network connection, MPLS, End-to-End isolated VLAN, etc.) MUST NOT transfer or route other traffic besides Province's data. Routing entries and appropriate controls MUST be in place to ensure this (e.g., a separate IPSEC tunnel should be used for the Province's data, with no other customers' data being routed or transferred using that tunnel);

d. For in scope Payment Card Industry (PCI) systems that are involved in the transfer and processing of payment card data, a separate physical router MUST be used for each circuit. In this case, separate router interfaces or virtualized routers are not acceptable;

e. Encryption MUST be used in accordance with the IMIT 6.10 Cryptographic Standards for Information Protection;

f. Automated Key Exchange/Update MUST be employed over encrypted links. If end-to-end encryption (e.g., from server to server) is not used, the encrypted tunnels, private network-to-network connections or MPLS tunnels MUST be terminated at an appropriate location so that intrusion prevention/detection, as well as content filtering and malware protection controls can be applied;

g. If end-to-end encryption is used (e.g., from source server storing the data to destination server storing the data, with encryption applied before the data leaves the server), the requirement for the mandatory and optional controls above is lessened to account for the presence of end-to-end encryption. The requirement, however, of a secure and isolated data transport for the Province’s data remains as the governing principle; and

h. If wireless connections are used anywhere on the data transfer path, the minimum encryption standard to be used for the wireless connectivity MUST be WPA 2 or higher.

5.1.4. Security event monitoring and logging MUST be maintained:

a. At the Province’s request, the log data MUST be provided to support the Province’s Security Investigations and Incident Response team, as well as the Province’s Compliance Audits. Raw logs MUST be retained for thirteen months. The archiving of logs is acceptable as long as the Province is provided the necessary access to log data when requested; and

b. At the Province’s request, raw log data from the appropriate devices MUST be provided for inclusion in the Province’s SIEM (Security Information and Event Management) system.

5.2. Application characteristics

Any services and devices within the gateway architecture MUST be protected against malware attacks, regularly maintained, updated and patched as required by service agreements. All services MUST have an annual review to ensure controls are providing adequate security to prevent a breach.

5.3. Information Characteristics

In all cases, access MUST first be approved by the Information Owners or the owners of the resources.

5.4. Network Connectivity – 3PG

The Ministry and the third-party MUST follow the OCIO-ES established process for the 3PG service.

6. DEFINITIONS/GLOSSARY

Information Security Glossary - Province of British Columbia (gov.bc.ca)

7. SUPPORTING DOCUMENTS

IMIT 5.08 Network to Network Connectivity Security Standard
IMIT 6.18 Information Security Classification Standard
IMIT 6.19 Information Security Standard

8. REVISION HISTORY

Version	Revision Date	Author	Description of Revisions
1.0	2022-09-15	Kristina Petrosyan	Document creation

9. CONTACTS

For questions or comments regarding this standard, please contact:

Information Security Branch, OCIO
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca