Document Version: 2.0
Effective Date: May 2008
Last Reviewed: October 2022

1. PURPOSE

The purpose of this standard is to establish clear technical standards for secure network-to-network connectivity. The IMIT 5.08 Network-to-Network Connectivity Security Standard (NNCSS) supplements the IMIT 6.19 Information Security Standard (ISS) published on the IM/IT Standards web site.

2. DESCRIPTION

The IMIT 5.08 NNCSS defines the connectivity requirements with respect to the connection between disparate networks. This includes connectivity to the SPAN/BC network and external service providers to external service provider networks. In addition to this standard, the ***5.08 Network-to-Network Connectivity Security Standard Specifications*** document provides detailed requirements. The specifications outlined in the *Specifications* document MUST be followed in conjunction with this standard.

3. AUTHORITY

Core Policy and Procedures Manual (CPPM) – Chapter 12: Information Management and Information Technology Management
Core Policy and Procedures Manual (CPPM) – Chapter 15: Security
Information Security Policy

4. APPLICATION / SCOPE

The IMIT 5.08 Network-to-Network Connectivity Security Standard, also known as the Third-Party Gateway (3PG) Standard, is meant for core government, other public agencies or external service providers that are considering interconnecting networks that carry public sector information. Contracted service providers conducting business on behalf of government MUST comply with the NNCSS (or demonstrate compliance with ISO 27002:2022) and the other IM/IT Standards. See **Section 6** below for a list of references and hyperlinks.

Exemptions from an IM/IT or Architecture Standard may be granted subject to the approval of the Government Chief Information Officer (GCIO). An exemption request and supporting documentation for the business need MUST be submitted to the GCIO for consideration of the exemption request.

5. REQUIREMENTS

Technical Standard

1. **Connection Routers:** Each network-to-network connection MUST ensure appropriate logical, and if necessary physical, separation is achieved. A virtualized

router may also be used, but logical separation needs to be guaranteed at all times (even in the event of device failure) using appropriate controls.

2. **Security Transit Point**
    a. **Firewall(s):** The firewall used MUST perform stateful packet inspection. Stateful Inspection Firewalls MUST be installed with the managed security rules permitting and denying access based on the principle of least access/privilege. **NOTE:** Devices that combine the Stateful Inspection Firewall and Routing functionality on one device are acceptable as long as the above requirements are met fully.
    b. **Intrusion Prevention/Detection System(s) (IPS/IDS):** IPS/IDS MUST be in place to monitor network traffic for security threats.
    c. **Content Filtering and Malware Protection:** Protection system(s), including content filters, SHOULD be used to screen for malicious code (viruses, etc.).
    d. **Data Leakage Protection:** Appropriate controls SHOULD be in place to ensure that data is prevented from being lost/leaked.
3. **Security:** the principles of least privilege apply:
    a. All ports MUST be closed by default and all IP addresses may be hidden by default (address NAT'ing). Request to open ports and IP addresses MUST be approved by the data owner and the Ministry owning the contract.
    b. Encryption MUST be used in accordance with the IMIT 6.10 Cryptographic Standards for Information Protection.

When one end of the connection is the SPAN network, then the ***Third-Party Gateway (3PG)*** service MUST be used.

6. SUPPORTING DOCUMENTS

IMIT 5.08 Network to Network Connectivity Security Standard Specifications
IMIT 6.19 Information Security Standard

7. DEFINITIONS/GLOSSARY

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

8. REVISION HISTORY

Version	Revision Date	Author	Description of Revision
1.0	2008-05		
2.0	2022-09-15	Kristina Petrosyan	New template, updated content

9. CONTACTS

For questions or comments regarding this standard, please contact:

Information Security Branch
Ministry of Citizens' Services
Email: Information Security Advisory Services CITZ: EX
InfoSecAdvisoryServices@gov.bc.ca