NETWORK TO NETWORK CONNECTIVITY
TECHNICAL AND PRODUCT STANDARDS

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC

People ● Collaboration ● Innovation

Version 0.0

May 2008

Copyright notice

Table of Contents

Table of Figures

1 Foreword

Private public partnerships are created to enhance the effective delivery of Provincial IM/IT services. Establishing external network connections to the Province’s network is becoming more frequent. Such connections require clear specification to ensure that information that may traverse that connection remain secure.

To address the issues surrounding connectivity it must be recognized that:

1. Only interim corporate government standards exist, created in 2004

   The province wished to avoid creating new connections between the government secure network and the corporate networks of other organizations, until such time as a network segmentation project was complete. The aim of the network segmentation project was to architect a manageable, scalable, auditable, method of connecting users to systems, and systems to systems when either the users or systems are hosted on different organization’s private networks. A policy clarification was provided on July 9, 2004, respecting connections to the provincial SPAN/BC network. A copy of this policy clarification titled "Enhancing the Security and Functionality of the Provincial Network (SPAN/BC)” can be found in Annex C and further background materials in "Backgrounder to Policy Clarification on Connecting to the Provincial Network (July 12, 2004)” can be found in Annex D, which provides background information to place the clarification of policy and rules respecting connectivity to the Provincial Network within the broader security enhancement context are available in. A further “*Interim Standards for Information Systems Security and Network Connectivity”, see Annex E, was circulated August 12, 2004 to further codify the intent of the policy clarification.*

2. There are no existing published technical standard for connecting [external] networks to, and

3. The only available government product solution has never been published as a standard of government.

This submission has been developed in order to establish clear generic technical standards for secure network to network connectivity as it relates to private circuit connections (not via the Internet) and to establish official Provincial product standards (described in Annex A) and to replace wordings of the summer 2004 memo’s (Annex C, D and E).

This document has been developed by the Office of the CIO in consultation with WTS:

- Alignment between the Reference and Product standards has been confirmed; and
- This is a new document and has no preceding documentation.

2 Introduction

No published Reference or Product Standards exist and only an Interim directions exists (6.4 Interim Standards for Information Systems Security and Network Connectivity) for network to network connectivity.

As private public partnerships are regularly developed for the delivery of Provincial IM/IT services, connection of the supporting external networks to the Province's network is becoming more frequent. Such connections require the granting of exemptions from the Office of the Chief Information Officer.

Briefly summarized: Exemptions are required because of three memos issued from the Office of the CIO during the summer of 2004 (Annex C, D and E (http://www.cio.gov.bc.ca/rpts/memo/20040812intconnectstds.pdf)). The initial memo indicated that government servers, desktop and applications can not be removed from the government network to a 3rd party service provider network. The ministries that had outsourcing proposals under discussion with the private sector proponents pressed the CIO for a clarification of the government's position respecting third party connectivity to the provincial network. They required this information in order to establish the technical model and finalize the business cases.

The clarification was issued in a second memo on July 9, 2004, and August 12, 2004 and distributed to all ministry corporate ADMs and all information technology directors. The policy did not prevent the outsourcing of the ownership and management of the application or the host server, but required those servers to operate within the current SPAN/BC network until the new, segmented network was operational. Authentication systems for those operating the application or server would continue to be the existing government authorized standard methods.

In practice, this policy did not prohibit any ministry from contracting with a third party to provide application maintenance or facilities management. If connection was required to the third party's systems, that organization would be responsible for providing such access without requiring modification to the government network. This could be accomplished using WTS's 3rd Party Gateway (3PG) Service.

However, the 3rd Party Gateway is not a formal (published) OCIO Product Standard, and, outside of the 3PG Gateway Service there are no documented or approved technical standard for connecting [external] networks to the SPAN network.

International ISO standards 18028-3 (Securing communications between networks using security gateways) currently exist for the secure network to network connectivity. This document makes the recommendation to adopt those ISO standards. ISO 180028-3 is a component of ISO 27001, an adopted standard of the Province.

2.1 Classification

The proposed standard is classified into the following categories:

Standard	Type	Nature	Review	Scope
Network to Network Connectivity Standard	Technical	Strategic	Annual	Both External Network to External Network and External Network to SPAN connections
ISO/IEC 18028-3:2005 - Securing communications between networks using security gateways	Reference	Strategic	3 Years	External Network to External Network Connections
Third Party Gateway	Product	Strategic, Baseline	3 Years	External Network to SPAN connections

3 Scope

This document:

1. Establishes the 3rd Party Gateway as the Provincial Product Standard to connection to external (non-SPAN) networks;
2. Specifies specific security requirements for any external network connection that carries government data; and
3. Gives founding ISO guidelines in current and future network to network connections.

This document applies to Ministries, WTS and authorized service providers.

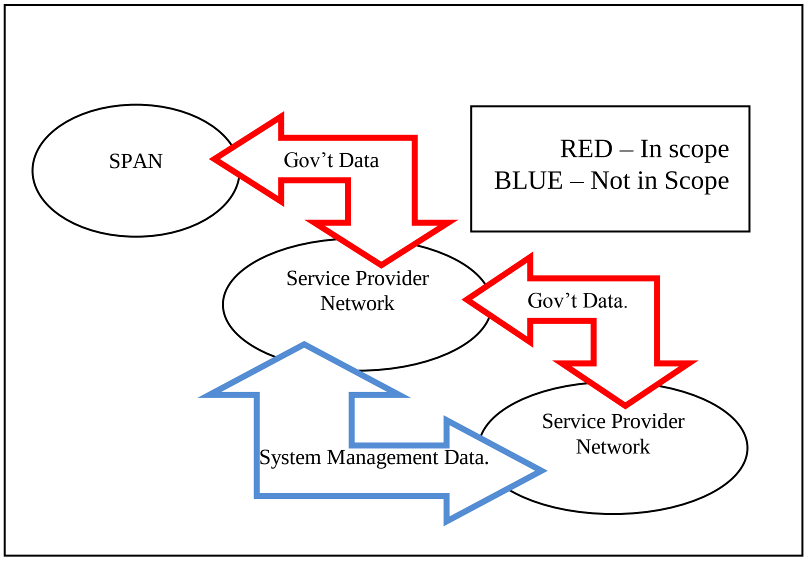


Figure 1: Scope

4 Normative references

International Standards

ISO 27001

ISO/IEC 18028-3:2005 Securing communications between networks using security gateways

Standards Manual

6.0 Information Technology Security (CPPM 12.3.6)

6.4 Interim Standards for Information Systems Security and Network Connectivity

Information Management Standards

Ministries must ensure all government information is managed in line with Government Core Policy Manual Chapter 12 Information Management and Information Technology Management 12.3.2 Information Management, http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1232. This includes Recorded Information Management, Information Utilization, Data Management and Forms Management.

A proposed solution must meet the privacy requirements of the *Freedom of Information and Protection of Privacy Act* and Proponents must address any privacy concerns or impacts that are identified in the Privacy Impact Assessment.

As part of the policy compliance, the province requires the solution provider to agree to meet the Province's security requirements as set out in 7.3 Security Clauses.

Normative references may be undated(?) unless it is considered that future editions will not be applicable.

5 Terms and Definitions

For the purposes of this document, the terms and definitions the following apply.

“Authorized” means giving the permission to the Contractor by the Province to work on or provide the Equipment or Service;

“Service” or “Services” means the services described in the Schedules to this Agreement;

“Service Location” means any community in British Columbia or geographic area where equipment and/or information is owned by the Province;

“Site” means a civic address or other geographical location within a Service Location designated by the Province from time to time as an end point or a transit point for the location of Equipment or delivery of the Service;

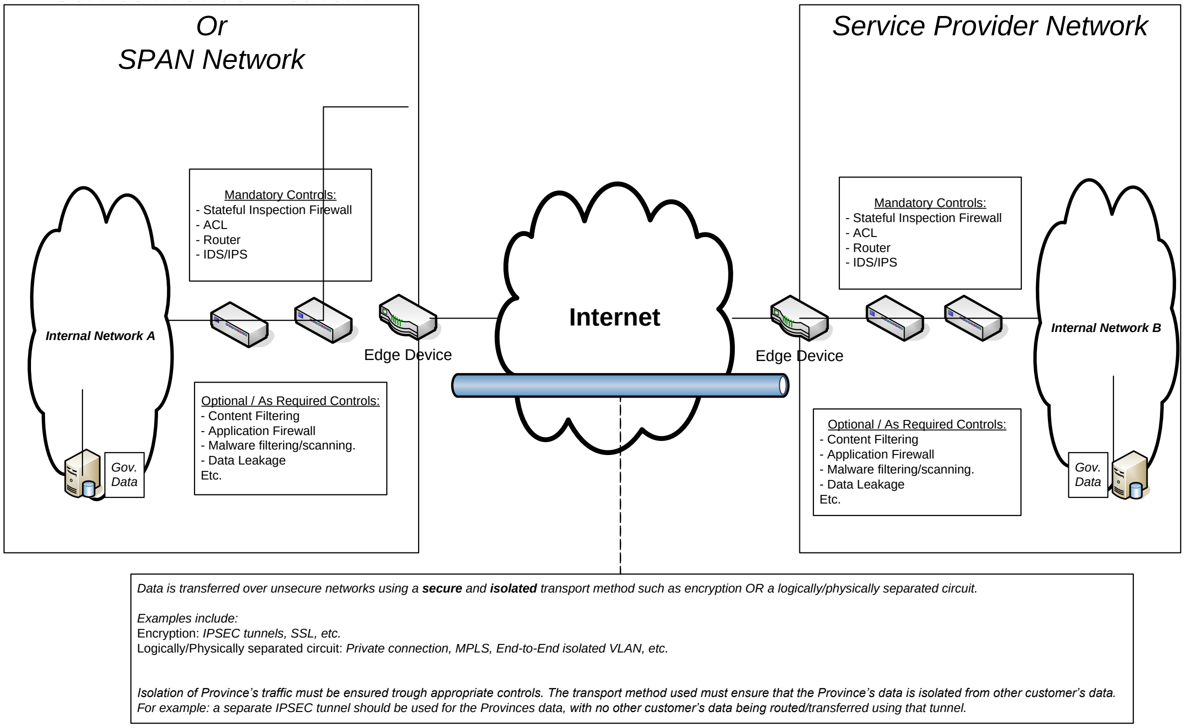
6 Requirements

Network to network connectivity standards formalization: Published (formal) Reference Standards do not exist and only an Interim Technical standard exists (6.4 Interim Standards for Information Systems Security and Network Connectivity) for network to network connectivity. There are no published Product Standards for network to network services.

Reduction in OCIO exemption requests for network to network connectivity: Only a minimal interim standard exist for network to network connectivity. Existing standards model is centered around exemption for each implementation and not a framework for successful implementation.

7 General characteristics

Figure 2: Model for Connection (ISO Screened Subnet)



*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.

7.1 Process/Contract specifications

Not applicable.

7.2 Security Characteristics

The principles of least privilege will apply.

A) All ports will be closed by default and all IP addresses will be hidden by default.

Opening of ports and IP addresses are requested by the Contract manager and must be approved by the data owner and the Ministry owning the contract.

B) Internal addresses will not be accessible by default.

Requirements to connect to internal IP addresses will be addressed through the implementation of a Split DNS Service.

C) Data transferred between networks:

1. A secure and isolated transport method should be used when transferring the Province's data. Data should be transferred between networks using encrypted tunnels, private network-to-network connections or using traffic isolation technologies such as MPLS(Multi-Protocol Label Switching), End-to-End isolated VLANs, etc.; to achieve a Virtual Private Network type connectivity.
2. 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. The encrypted tunnels or the logically/physically separated circuits used (i.e. private network-to-network connection, MPLS, End-to-End isolated VLAN, etc.) will not transfer/route other traffic besides Provincial data. ACLs, routing entries and appropriate controls will be in place to ensure this. 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.
3. If the data transfer path leaves Canada, or it cannot be guaranteed that it will not leave Canada, care needs to be taken to ensure that the FOIPPA requirements are met.
4. Minimum AES 128 encryption will be used for encryption. Encryption using keys of less than 128 bits are not acceptable. DES is not an acceptable encryption standard. If using 3DES encryption standard, the minimum key required is 168bit. Acceptable encryption standards include: 128bit AES, 168 bit 3DES.
5. If encrypted tunnels are used, processes/procedures need to be implemented to ensure that the encryption keys are changed every 90 days and/or at staff changes.
6. If wireless connections are used anywhere on the data transfer path, the minimum encryption standard to be used for the wireless connectivity is WPA, with WPA2 recommended. WEP is not an acceptable encryption.

D) Security Event Monitoring and logging will be maintained.

1. At the provinces request, the log data will need to be provided to support the Province's Security Investigations Team as well as the Province's Compliance Audits. Raw logs need to be retained for one year. The archiving of logs is acceptable as long as the Province is provided the necessary access/tools to access log data when requested.
2. Raw log data from the appropriate devices needs to be made available for inclusion in the Province's SIM(Security Information Management) or SEM(Security Event Management) System if requested by the Province.

7.3 Technology characteristics

7.3.1 Network to Network Connections (all)

Network to Network and the 3rd Party Network Gateway consists of the following components:

- **Connection Routers:**

  Each network to network connection must ensure appropriate logical, and if necessary physical, separation is achieved. Virtualized routers may also be used, but logical separation needs to be guaranteed at all times (even in the event of device failure) through the use of appropriate controls.

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

- **Managed Router Access Control List (ACL):**

  The connection routers will be configured with a 'basic' ACL to deny/permit, using the principle of least privilege, to control access from one network to another network. Separate ACL's, designed based on least privilege and using the "Deny All" as the default fall back rule, need to be configured and maintained on each interface in each direction (i.e. external vs. internal interfaces; inbound vs. outbound traffic directions) This access control list will be the first line of defense in a multi-layered protection strategy.

- **Firewall(s):**

  Stateful Inspection Firewalls will 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.

If end-to-end encryption (i.e. 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.

- **Intrusion Detection/Prevention System(s) (IDS/IPS):**

  IDS/IPS will be in place to monitor network traffic for security threats

- **Content Filtering and Malware Protection (if required):**

  Correction system(s) including content filters will be in place to screen for malicious code (viruses, etc.).

- **Data Leakage Protection** (if required):

  Appropriate controls will be in place to ensure that data is prevented from being lost/leaked.

- **Proxies: (if required)**

  Proxy server(s) (HTTP, FTP, etc.) can provide user authentication and DNS name translation for IP traffic if required.

- **VPN Gateways** (if required)

  In case 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 (stateful firewall, acl, IDS/IPS) and the optional/as required controls(content filtering, malware detection, data leakage, etc) are applied to the traffic.

If end-to-end encryption is used (i.e 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.

7.3.2 3PG

The 3rd Party Network Gateway solution provides the above. Specifically:

- The ability for a Ministry to connect their 3rd Party's private telecommunications network to the Province's telecommunications network
- The Ministries with the ability to equip their 3rd party service providers with remote access to information technology resources within the Province's private telecommunications network.
- Security controls to protect the information technology of Ministry systems not involved in the 3rd Party arrangement (e.g. Other Ministries not party to the 3rd Party solution agreement).

- Enables access to user authentication and reverse proxy services for web applications hosted on the 3rd party telecommunications network

Redundancy of components will be determined by service agreements.

7.4 Application characteristics

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

7.5 Information characteristics

In all cases access must first be approved by the information owners or the owners of the resources.

8 Detail

The guidelines listed in this section assume that readers are familiar with the policy memorandum issued July 9 and available at http://www.cio.gov.bc.ca/prgs/memo.htm .

Further to the above mentioned policy memorandum, in cases where information systems solutions cannot comply with the policy memorandum, the steps required to implement an alternative are as follows:

1. Technical design, review, and alternatives analysis of connectivity options.
   Key considerations will be:
   a) Ability to operate and manage the information systems in question
   - Ability to protect the government network at large (it's users, assets, and information) from the compromise of any non-government network or computer systems.
   - Ability to protect any non-government network or computer systems from compromise of government network or systems
   - Ability for government to manage and audit any network connections, the security, and the related systems
   - The financial and other resource costs associated with the alternative

It is generally understood that alternatives will involve technologies such as private network links, point to point network links; firewalls, access control lists on routers, network encryption and so on.

It is strongly encouraged that ministries find ways to provide the business solution without requiring modification to the existing configuration of the SPAN/BC network.

2. Any proposed alternatives must be approved by the Office of the Chief Information Officer before they are implemented

Any ministry proposing an alternative to the policy must factor the time and cost of the above process, as well as the costs required to implement and operate any alternative, into their plans and budgets.

8.1 Network Connectivity

8.1.1 3PG

The Ministry will

- Submit an order to WTS for the 3PNG and be responsible for the associated costs

- Complete the WTS provided table of source and destination IP addresses and TCP/UDP port numbers for resources to which the 3rd Party requires access.
- If the resources are not owned by the Ministry, the Ministry will obtain, and provide to WTS, authorization from resource owner.
- Coordinate access on behalf of the 3rd party service provider for the resource support staff and that of their telecommunications vendors to the Victoria and/or Vancouver sites for installation and on-going support, as required.
- Provide WTS with technical contact information for the 3rd party service provider for installation and troubleshooting.

The 3rd party service provider will

- Extend their private telecommunications network to the 3PG facilities located in the Victoria and/or Vancouver data centers.. The 3rd party is responsible for provisioning and management of the extension of their network to the demarcation point in the Victoria and/or Vancouver data centers.
- Obtain from the Ministry access authorization for their support staff and that of their telecommunications vendors to the Victoria and/or Vancouver sites for installation and on-going support, as required.
- Provide public routable IP addresses for resources on their network.
- Provide sufficient capacity and bandwidth required to carry the required traffic
- Monitor the capacity of their circuit for congestion
- Provide the necessary QOS parameters and policies EF (expedited forwarding) and AF (assured forwarding) to match WTS
- Provide the Ministry with technical contact information for installation and troubleshooting.
- Contact the WTS Customer Service Center (250-952-6000) to report any problems with the 3PNG.
- Provide an appropriate level of security, to the Ministry's satisfaction, on their network connection.
- Provide the appropriate security monitoring and logging.

8.2 Enquiry Scope

WTS and the OCIO ISB have been consulted in the development of this standard.

8.3 Analysis/Acceptance

WTS and the OCIO ISB are in agreement with the contents of this document.

8.4 Response

The inclusion of ISO as a standards basis was positively accepted.

8.5 Packaging

The standard as proposed for the Standard Manual is contained in Annex A.

9 Bibliography

CORE POLICY MANUAL 12 Information Management and Information Technology Management, http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1234 .

Annex A. Network to Network Connectivity Standard

IM/IT Standards Manual **Office of the Chief Information Officer** **Province of British Columbia**	**Effective Date**: **Scheduled Review**: **Type:** Technical, Product and Reference Standard
5.0 Information Technology Management (CPPM 12.3.5)	
5.X Network to Network Connectivity	

Description of Standard

This standard, which is composed of three sections, defines the connectivity requirements that must be addressed with respect to the connection between disparate networks. This includes connectivity to the SPAN/BC network and external service provider to external service provider networks.

1) Technical Standard:

a) Standard Components:

- **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) through the use of appropriate controls.
- **Managed Router Access Control List (ACL):** The connection routers will be configured with a ‘basic’ ACL to deny/permit using the principle of least privilege, for access from the 3rd party network to the Provinces network or from 3-rd party network to another 3-rd party network. Separate ACL’s, designed based on least privilege and using the “Deny All” as the default fall back rule, need to be configured and maintained on each interface in each direction (i.e. external vs. internal interfaces; inbound vs. outbound traffic directions) This access control list will be the first line of defense in a multi-layered protection strategy.
- **Firewall(s):** The firewall used must perform stateful packet inspection. Stateful Inspection Firewalls will 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.
- **Intrusion Detection /Prevention System(s) (IDS/IPS):** IDS/IPS will be in place to monitor network traffic for security threats.
- **Content Filtering and Malware Protection:** Correction system(s) including content filters will be in place to screen for malicious code (viruses, etc.).
- **Data Leakage Protection**:

  Appropriate controls will be in place to ensure that data is prevented from being lost/leaked.
- **Proxies: (optional)** HTTP Proxy server(s) can provide user authentication and DNS name translation for HTTP traffic if required.

b) Security: The principles of least privilege will apply.

- All ports will be closed by default and all IP addresses will be hidden by default. Opening of ports and IP addresses are requested by the Contract manager and must be approved by the data owner and the Ministry owning the contract.
- Internal addresses will not be accessible by default. Requirements to connect to internal IP addresses will be addressed through the implementation of a Split DNS Service.
- Minimum AES 128 encryption will be used for encryption. Encryption using keys of less than 128 bits are not acceptable. DES is not an acceptable encryption standard. If using 3DES encryption standard, the minimum key required is 168bit. Acceptable encryption standards include: 128bit AES, 168 bit 3DES.

2) **Product Standard:**
When one end of the connection is the SPAN network, then the Third Party Gateway (3PG) service must be used.

3) **Reference Standard:**
ISO/IEC 18028-3:2005 - Securing communications between networks using security gateways – will serve as the reference standard for network to network connectivity, specifically, the ISO Screened Subnet model.

Where Standard is Used

The standard is meant for WTS, any ministry, other public agency or external service provider that is considering interconnecting networks that carries public sector information.

Authority and Exceptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) to minimize security exposures and maximize the privacy information traveling across the connected networks. If there is a compelling business reason network to network connections should not or could not make use of this standard, the information systems director must address his or her concerns to the OCIO through a Request for Exception.

Metrics and Enforcement

WTS offers secure network to network connectivity through the 3rd Party Gateway Service. Details of this Shared Services BC service offering can be found on the WTS client website (see Reference #1 below).

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary which is currently under development by the OCIO.

References

Memo: Interim Standards for Information Systems Security and Network Connectivity
August 12, 2004
Reference: http://www.cio.gov.bc.ca/rpts/memo/20040812intconnectstds.pdf

Security Schedule G: www.gov.bc.ca (TBD)

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca .

Contact

Architecture and Standards Branch, OCIO

Annex B. ISO/IEC 18028-3:2005 Securing communications between networks using security gateways

Annex C. OCIO Memo on Enhancing the Security and Functionality of the Provincial Network (SPAN/BC)

EXCERPT

Ref: 17967

Date: July 9, 2004

To: ADMs of Corporate Services

Re: **Enhancing the Security and Functionality of the Provincial Network (SPAN/BC)**

The increasing number and severity of virus and worm attacks on the provincial information technology infrastructure have raised the concern respecting security to new heights.

The Common Information Technology Services (CITS) Branch, in conjunction with the Network BC project, is currently in the early stages of enhancing the capability of the SPAN/BC network though segmentation. A segmented network, together with revised security policy and procedures, will allow for much higher security levels than currently exist. It will also provide enhanced functionality to promote more third party service connectivity.

Moving to a segmented network configuration is a major design project for the government network administrators. It is expected that the segmented network will be redesigned and operational by the summer or fall of 2005.

Recently, there have been a number of suggestions or proposals that would see private or other third party hosted applications resident outside of the government private network connect back to government application within the network.

Given the major segmentation project noted earlier, I have been asked to clarify the policy and rules respecting connectivity to the Provincial Network.

Until the new provincial segmented network is operational:

a) Existing servers, desktops and applications will not be removed from the Provincial Network (SPAN/BC) to other networks.

b) New applications that require connectivity into the provincial government's application infrastructure must be hosted with the Provincial Network (SPAN/BC).

c) If an application is a stand-alone, such as a purely Internet-based service, it may be exempted from this policy.

d) Ministries are responsible for ensuring that remote management/administration of applications, servers and desktops is authorized through the existing standard methods including Span/Dial, SPAN/VPN; CITS/DTS; and application specific methods.

NOTE: This specific policy only applies to provincial government ministries.

If there are questions regarding this policy, please contact Peter Watkins, Director, Technology Planning and Standards, Office of the Chief Information Officer, at 387-2184 or Peter.Watkins@gems1.gov.bc.ca

"Original signed by"
R.C. McCandless
Chief Information Officer
Chief Operating Officer - Common IT Services

Annex D. Backgrounder for July 9 2004 Policy Clarification

EXCERPT

Ref: 17974
Date: July 12, 2004
To: ADMs of Corporate Services

Re: **Backgrounder to Policy Clarification on Connecting to the Provincial Network**

On July 9, 2004, I issued a clarification on the policy respecting connections to the provincial SPAN/BC network.

This backgrounder has been prepared to place the clarification within the broader security enhancement context.

“Original signed by”

R.C. McCandless

Chief Information Officer

Chief Operating Officer - Common IT Services

Attachment

Background Respecting July 9, 2004, Policy Clarification Respecting Connectivity to the Provincial Network (SPAN/BC)

1. Need for Enhanced Information Technology Security

The BC Government has a relatively advanced information technology (IT) and information management (IM) infrastructure, and is actively encouraging the move to greater use of IT, especially electronic commerce, to improve business practices and service to its citizens. Many programs are now reliant on IT to provide services, and the government has well defined corporate automated systems to support its financial (CAS) and human resources/payroll (CHIPS) operations. Businesses connect electronically to many government programs to receive information or conduct transactions.

The rapid growth in electronic applications is not unique to this province. During the 1990’s, many organizations moved quickly to automation to reduce cost and improve the availability of information and services. During this period of rapid growth and technological change, the area of security was generally given a lower priority to that of new product development.

The BC Government is also not unique in developing a concern about improving its IT and IM security capability. As organizations become more dependent on technology, they become more vulnerable to disruptions in service through natural causes, unintended human error or planned attacks on the systems and data.

The need to enhance the current security policy, practices and technology has been documented in a number of recent studies and reports. The 2003 consolidation of servers and desktops into the Common Information Technology Services (CITS) organization has a positive move in terms of improving security management. The March, 2004, realignment of the Office of the Chief

Information Officer also clarified the corporate security role of the IT Security Branch now housed within the CIO's office.

2. The BC Government Provincial Network (SPAN/BC)

One of the greatest strengths of the government's IT model is the single network (SPAN/BC) which inter-connects all ministry applications and includes many provincial agencies and Crown corporations. This single network allows connectivity within the protected network and is administered by the network operations group within CITS. Many other governments are now trying to move to a single network to improve administration, connectivity and data sharing and reduce cost.

The government's network provides a single connection point to the Internet and controls security to some extent. However, the network is relatively open and various ministries have built and maintain firewalls within the network to protect their own sensitive data. Another related strength of the government's private network is the access control established through the central user authentication and authorization system (IDIR).

Over the years, network technology has improved to enable more external connectivity with enhanced security. This new, segmented network model greatly reduces the risk of business disruptions throughout the network by compartmentalizing or segmenting the various sub-systems within the overall network. It also allows for greater third party connection to the government network to improve electronic transactions and e-commerce.

In keeping with the government's priority of greater electronic connectivity the Network BC initiative has been working to redesign the provincial network and to expand broadband services throughout the province. The government, through CITS, has purchased the necessary technology (routers, switches, etc.) to install a segmented network, and a major network segmentation design project is being planned. It is anticipated that the new segmented network will be operations by the summer of 2005.

3. Recent Outsourcing Initiatives

A number of government ministries have been seeking ways to improve their services and/or reduce their current expenditures by contracting with the private sector to build and operate new applications (e.g. revenue collections, medical billings, student information and residential tenancy disputes).

While most of the details of the technical design are still under discussion, a number of the private sector proponents believe they can develop a better business case if they operate the application on their own equipment within their own corporate network, and connect back to government applications through the SPAN/BC network.

As a result of the number of these initiatives and their impact on the current network security model, CITS reviewed their current connectivity situation respecting direct third party connections from servers outside the network. Of the 17 separate applications, where the service is directly connected, five are operated by a private company (TELUS in two cases), while the rest are with a government agency or the federal RCMP (CPIC). Most of these connections do not have detailed security policy, procedures, standards or agreements in place, but rely on a "trusted relationship".

Given the potential proliferation of new connections and the resulting potential complexity of security management that this would entail, the Chief Information Officer requested Cicso Systems to review the government's network security design and recommend ways that third party connectivity could be facilitated while protecting the government's data.

The Cisco team provided their recommendations on June 25, 2004. They complimented the government on the unified network and the well-managed authentication system. They recommended, among other things, that the government proceed with the network segmentation plan and ensure that the network redesign includes appropriate security features. Pending the launch of the new network they recommended a freeze on all new direct connections (as this would increase vulnerability and make the design project more complex), and that third parties who do not connect must use the current authentication system.

4. Policy Clarification Issued by July 9, 2004

The ministries that had outsourcing proposals under discussion with the private sector proponents had been pressing the CIO for a clarification of the government's position respecting third party connectivity to the provincial network. They required this information in order to establish the technical model and finalize the business cases.

The clarification was issued on July 9, 2004, (Appendix 1) and distributed to all ministry corporate ADMs and all information technology directors. The policy does not prevent the outsourcing of the ownership and management of the application or the host server, but requires these servers to operate within the current SPAN/BC network until the new, segmented network is operational. Authentication systems for those operating the application or server will continue to be the existing government authorized standard methods.

In practice, this policy does not prohibit any ministry from contracting with a third party to provide application maintenance or facilities management. Every individual providing that application management (where the application is to be connected to other provincial government applications) will be required to have their own authentication account. These individuals will have access to a government e-mail mailbox within the network. If connection is required to the third party's systems, that organization will be responsible for providing such access without requiring modification to the government network.

5. Moving Forward with the Security Enhancement Project

The concern about degradation of the security of the provincial network is only one aspect of the concern respecting the IT infrastructure generally. Currently, it has a high profile due to the number of outsourcing proposals. Outsourcing applications and their server support on a piece-meal basis may achieve the objectives of the individual ministries. However, the province's IT infrastructure involves more than its individual applications.

The shift to a redesigned and segmented network, with appropriate security, will allow for much greater third party connectivity, including third party-hosted applications. This will achieve the security and service objectives.

The Security Enhancement Program involves much more than the provincial network. It will encompass a review of current policies, standards and procedures, physical security, hosting, applications and data. It will be based on the principle of defense in depth, including protection, detection, defense, recovery, monitoring and education. The revised security system will be designed both for protection of the government's physical and information assets, and to enable greater access to the government's information and services in the way the government wishes to provide such access.

Electronic commerce or e-service is dependent on the public's trust. An adequate security system is a key foundation stone for the design on the province's e-government service.

Office of the Chief Information Officer

July 12, 2004.

Annex E. Interim Standards for Information Systems Security and Network Connectivity

The Network to Network Connectivity Standard replaces the Network Connectivity and Network Connectivity Guidelines sections from the August 12 Memo on Interim Standards for Information Systems Security and Network Connectivity". Specifically:

EXCERPT

Ref: 18129
Date: August 12, 2004
To: ADMs of Corporate Services

Re: **Interim Standards for Information Systems Security and Network Connectivity**

On July 9, 2004, I issued a policy clarification on the policy respecting connectivity to the provincial network (SPAN/BC). Sicne that time further work has been done to codify the intent of the policy clarification.

Attached please find a document respecting the corporate standards for systems security and network connectivity.

"Original signed by"

R.C. McCandless
Chief Information Officer
Chief Operating Officer - Common IT Services

Attachment

Network Connectivity

The province wishes to avoid creating new connections between the government secure network and the corporate networks of other organizations, until such time as a network segmentation project is complete. The aim of the network segmentation project is to architect a manageable, scalable, auditable, method of connecting users to systems, and systems to systems when either the users or systems are hosted on different organization's private networks.

A policy clarification was provided on July 9, 2004, respecting connections to the provincial SPAN/BC network. A copy of this policy clarification titled "Enhancing the Security and Functionality of the Provincial Network (SPAN/BC)" and further background materials in "Backgrounder to Policy Clarification on Connecting to the Provincial Network (July 12, 2004)" which provides background information to place the clarification of policy and rules respecting connectivity to the Provincial Network within the broader security enhancement context are available at http://www.cio.gov.bc.ca/prgs/memo.htm.

Specific guidance is provided in Attachment: 3) Network Connectivity Guidelines.zxczxczxc

Network Connectivity Guidelines

The guidelines listed in this section assume that readers are familiar with the policy memorandum issued July 9.

Further to the above mentioned policy memorandum, in cases where information systems solutions cannot comply with the policy memorandum, the steps required to implement an alternative are as follows:

1. Technical design, review, and alternatives analysis of connectivity options
   Key considerations will be:
   - Ability to operate and manage the information systems in question
   - Ability to protect the government network at large (it's users, assets, and information) from the compromise of any non-government network or computer systems
   - Ability to protect any non-government network or computer systems from compromise of government network or systems
   - Ability for government to manage and audit any network connections, the security, and the related systems
   - The financial and other resource costs associated with the alternative

   It is generally understood that alternatives will involve technologies such as private network links, point to point network links; firewalls, access control lists on routers, network encryption and so on.

   It is strongly encouraged that ministries find ways to provide the business solution without requiring modification to the existing configuration of the SPAN/BC network.
2. Any proposed alternatives must be approved by the Office of the Chief Information Officer before they are implemented

Any ministry proposing an alternative to the policy must factor the time and cost of the above process, as well as the costs required to implement and operate any alternative, into their plans and budgets.