INFORMATION SERVICES BOARD

Contributors:

Scott Came
Department of Information Services

Jim Albert
Department of Information Services
Enterprise Architecture Committee Steward

Network Standards

ISB Standards

Version 4.0

September 14, 2006

Information Services Board
Enterprise Architecture Committee

Sue Fleener, *Washington State Patrol*
Cathy Munson, *Legislative Service Center*
Co-Chairs

Scott Came, *Department of Information Services*
Chief Enterprise Architect

1110 Jefferson Street SE
P.O. Box 42445
Olympia, WA 98504-2445
Phone 360/902.3519
Fax 360/902.2982
ScottCa@dis.wa.gov

Table of Contents

1. Document History

Date	Version	Editor	Change
May 26, 2006	1.0	Scott Came	Initial Draft
June 9, 2006	1.1	Scott Came	Updates per EA Committee comments (see Appendix B)
June 22, 2006	2.0	Trina Regan	Endorsed by the EAC
September 14, 2006	4.0	Trina Regan	Adopted by ISB

2. Document Context

This document currently has ISB Standards status. This status signifies that the document has been adopted as Standards by a vote of the Information Services Board. For more information about the ISB Enterprise Architecture Committee and its initiative, please visit the EA Committee website at: http://isb.wa.gov/committees/enterprise/index.aspx.

3. Introduction and Purpose

This document designates the State Government Network (SGN) and InterGovernmental Network (IGN) as common networking infrastructure for state government.

In accordance with the over-arching enterprise architecture Commonality Principle, this document establishes a clear business case for the designation of the SGN and IGN as common networking infrastructure.

The SGN and IGN are defined in the **[SGN]**[†] and **[IGN]** solution set documents, respectively.

3.1. Summary of Standards

The State Government Network (SGN) is the common, standard Internet Protocol-based network to be used by state agencies to connect separate locations within and among those agencies.

The InterGovernmental Network (IGN) is the common, standard Internet Protocol-based data network to be used by state agencies to connect state agencies, counties, and cities with known end points, managed gateways, and applications.

4. Compliance Component Information

This section documents key information required of all compliance components in the architecture.

4.1. Basic Component Metadata

Component Identifier:	**Error! Unknown document property name.**
Adoption Date:	**Error! Unknown document property name.**
Effective Date:	**Error! Unknown document property name.**

4.2. Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the Information Services Board (ISB), including the authority to develop statewide or interagency information services and technical policies, standards, and procedures.

4.3. Scope

These standards apply to all institutions under the purview of the Information Services Board. These standards do not apply to educational institutions, which use the K-20 network.

In this document, the terms “state agency” and “agency” mean any agency or institution within the scope of the previous paragraph, and the term “state enterprise” means all agencies and institutions (collectively) within the scope of the previous paragraph.

4.4. Relationship to Other Components, Policies, Standards, or Guidelines

In **[Investment Standards]**, the Information Services Board (ISB) exempts new wide area networks from agencies’ delegated authority.

[†] Text formatted in this **[Style]** indicates a citation to a reference. References appear in section 6.

5. Network Standards and Rationale

This section documents the network standards and the rationale behind them.

5.1. Standards

5.1.1. State Government Network (SGN)

The State Government Network (SGN) is the common, standard Internet Protocol-based network to be used by state government agencies to connect separate locations within and among those agencies. The SGN is defined in **[SGN]**.

This standard designates the SGN as a common solution, within the context of the over-arching enterprise architecture principle of commonality (defined in **[Principles]**.) A state agency must make a clear business case to design or implement network circuits outside of the SGN to connect separate locations within that agency and/or among agencies.

The scope of this standard at this time excludes satellite, radio or microwave communications (of voice or data) among state agency locations.

5.1.2. InterGovernmental Network (IGN)

The InterGovernmental Network (IGN) is the common, standard Internet Protocol-based data network to be used by state agencies to connect state agencies, counties, and cities with known end points, managed gateways, and applications. The IGN is defined in **[IGN]**.

This standard designates the IGN as a common solution, within the context of the over-arching enterprise architecture principle of commonality (defined in **[Principles]**.) A state agency must make a clear business case to provision networks or connectivity separately to local government locations.

The scope of this standard at this time excludes use of the network for voice or video among IGN participants. This standard should be reviewed at least every twelve months to maintain its alignment with the capabilities of the IGN. The scope of this standard does not include satellite, radio or microwave communications (of voice or data) among state agency and local government locations.

For purposes of this standard, the term IGN Participant means a state agency, county government, or municipal government that enters into a contractual arrangement for use of the IGN. The term “local government” means any county or municipal government IGN Participant, or another organization that connects to the IGN via a contractual arrangement with an IGN Participant.

5.2. Rationale

The Commonality Principle states that technologies, such as networks, should be common where there is a clear business case. In the case of networks, guidelines exist for what constitutes a “clear business case” (see **[NBCG]**.) This section demonstrates how the SGN and IGN meet the “clear business case” criteria specified in these guidelines.

5.2.1. Business Case for State Government Network (SGN) Standard

5.2.1.1. Efficiency and cost-effectiveness

The SGN promotes efficiency and cost-effectiveness of the state’s networking investments in the following ways.

- The SGN leverages the state's ability to aggregate network traffic onto a single, high-bandwidth backbone, reducing the overall number of circuits needed to carry data among state government agency locations. Since the cost of carrying a given amount of data over two circuits is generally higher than the cost of carrying that same amount of traffic over one larger circuit, the traffic aggregation provided by the SGN is more efficient and cost-effective than alternatives provisioned separately by individual agencies.
- The SGN leverages the state's buying power in negotiating with telcos to obtain circuit provisioning arrangements more favorable to agencies. Telco contracts for circuits on the SGN generally reduce or eliminate the costs of terminating or relocating circuit connections. Contracts establish stable rates for longer periods than agencies would be able to achieve on their own, allowing the enterprise overall to predict biennial networking infrastructure costs more accurately. Some telco contracts reduce the cost of a redundant connection from a customer site to a second core SGN node, to support business continuity in the event of a service disruption at the primary node.
- The SGN allows agencies to share skilled, specialized network engineering staff resources at the Department of Information Services (DIS) who monitor and maintain the core and local access network segments, and continuously plan for growth in the enterprise's demand for bandwidth and network services. Consolidating many network monitoring, maintenance, and capacity planning tasks frees state agencies to devote more resources to their core business missions and to direct technology support for their customers.
- The SGN allows DIS to manage the enterprise's interactions with telcos on behalf of agencies. These interactions include routine maintenance, problem resolution, invoice management, correction of billing errors, and contract management. Consolidating vendor management tasks frees state agencies to devote more resources to their core business missions and to direct technology support for their customers.

5.2.1.2. Support for enterprise applications and other common solutions

The SGN supports enterprise applications and other common solutions in the following ways.

- The SGN is currently a de-facto standard that connects most state agency locations.
- The SGN offers connectivity, at required levels of bandwidth, to core technology services such as (see section 5.1.3 of **[SGN]**):
    - Domain Name Services (DNS)
    - Network attached storage
    - Middleware to support system integration
    - DIS Mainframe applications
    - Web Server Farms
    - Washington State Enterprise Active Directory
- These core technology services support existing core enterprise applications (such as the Human Resource Management System (HRMS), Agency Financial Reporting System (AFRS), and Travel Voucher System (TVS)) and will support future core enterprise applications (such as the Financial/Administrative Roadmap envisioned systems). The SGN supports these applications by providing network connectivity among state agency locations and the environments in which the enterprise hosts the applications.

5.2.1.3. Ensuring levels of network security, availability, and reliability commensurate with stakeholder (citizen, business, employee) expectations and business requirements

The SGN ensures levels of security, availability, and reliability commensurate with stakeholder expectations and requirements, in the following ways (see sections 5.2.1-5.2.5 of **[SGN]**).

- The SGN leverages the state network backbone's redundant core design, in which each node site is connected to at least two other node sites. Node sites have 72 hours of backup power supply, with further backup power provided by diesel generators. DIS maintains 24/7 on-site/on-call support for node site equipment, with spare equipment available on-site and next-day equipment replacement arrangements with vendors. Because of the SGN's ability to aggregate traffic and share node site facilities across the enterprise, it provides these mechanisms to support high levels of availability and reliability in a cost-effective manner.
- All SGN core and local access circuits are physically diverse, improving availability and reliability.
- The SGN is protected by perimeter firewalls and security gateways. All state agencies using the SGN must comply with Information Services Board (ISB) security policies and standards, and must conduct a third-party security audit every three years. The perimeter firewalls, gateways, and security policies implement a baseline level of network security that satisfies enterprise-wide security requirements.
- Investments in Quality of Service mechanisms (detailed in section 5.2.7 of **[SGN]**) allow DIS to support differentiated services and guaranteed levels of bandwidth according to individual agency requirements.
- The statewide backbone network supports the SGN. It is based on vendor-provided Synchronous Optical Network (SONET) circuits. The physical ring topology and protection capabilities of SONET improve the reliability and availability of the SGN. More recently, vast improvements to this optical technology have become available in the marketplace. SONET framed DWDM wave services are the next step for SONET based networks. The next generation of the statewide backbone network will use SONET framed DWDM wave services and multi-service provisioning platforms (MSPP). MSPPs provide the usual capabilities of SONET add-drop multiplexers (ADM) with support for multiple rings and additional protocols. The new network design provides increased bandwidth, provisioning flexibility, and management and operational enhancements. It will support a variety of protocols and services while providing SONET reliability and availability. According to Gartner, "the majority of optical networks currently used in support of high-speed Ethernet services are SONET-based" ([Gartner Ethernet Report], p.5). For local access and customer site connectivity to the SGN, DIS uses the most current technology available from service providers to meet customer requirements. These factors align the SGN with current technology and industry direction.

5.2.1.4. Support for interoperable exchange of information and linkage of business processes among agencies

The SGN supports exchange of information and linkage of business processes among agencies in the following ways.

- The SGN provides underlying network transport for existing system integration infrastructure, such as Websphere MQ and Secure File Transfer services.
- The SGN provides connectivity between state agency locations and core enterprise applications (see section 5.2.1.2 above) with which agency systems may need to integrate. The SGN also provides connectivity to core technology services, such as Enterprise Active Directory, that support system integration.

- The SGN satisfies underlying network transport requirements for the infrastructure elements of the future integration architecture for the state government enterprise (see **[CITRA]**.) SGN connectivity will enable composite, cross-agency applications, such as the Enterprise Business Portal and Enterprise Geographic Information Technology Portal, in a more cost-effective and efficient manner than alternative networking approaches.
- The SGN streamlines and simplifies inter-agency integration over alternative networks by:
    - Allowing agencies to use common integration infrastructure, rather than selecting integration infrastructure for each partnership with another agency
    - Providing direct access to supporting services like Enterprise Active Directory
    - Encouraging the delivery of applications and exchange of information over the same network, simplifying the agency's technology environment

5.2.1.5. Flexibility and Business Agility

The SGN supports flexibility and business agility in the following ways.

- DIS constantly monitors and manages the SGN core and local access segments to ensure adequate bandwidth exists to support changes in agency business requirements. The SGN core and local access segments are designed to scale without disruption to individual agency network environments.
- The SGN provides agencies with the control in the Customer Site segment of the network necessary to support their business requirements. For example, agencies remain responsible for supporting the configuring of routers and switches, providing workstation support, and managing applications on their local area networks (that is, within the Customer Site segment).
- DIS negotiates specific customer requirements regarding Quality of Service and support on a customer-by-customer basis.
- The SGN leverages the state's buying power to obtain favorable terms from telcos regarding termination and relocation of circuits, providing agencies with greater flexibility and agility than they could achieve alone.

5.2.1.6. Implications

The designation of the SGN as common, shared infrastructure has the following implications, in addition to the benefits described in the previous sections.

- Future networking investments may be necessary to move agencies not currently on the SGN from agency-provisioned circuits and equipment to the SGN. This may include building a migration plan and risk mitigation strategies, as well as funding migration projects for each agency.
- Future networking investments may be necessary (in SGN circuits, equipment, and network administration resources) to align SGN capacity with the increased usage that will result from adoption of this standard.

5.2.2. Business Case for InterGovernmental Network (IGN) Standard

5.2.2.1. Efficiency and cost-effectiveness

The IGN promotes efficiency and cost-effectiveness of the state's networking investments in the following ways.

- The IGN leverages the state's ability to aggregate network traffic onto a single, high-bandwidth backbone, reducing the overall number of circuits needed to carry data among state government agency locations. Since the cost of carrying a given amount of data over two circuits is generally higher than the cost of carrying that same amount of traffic over one larger circuit, the traffic aggregation provided by the IGN is more efficient and cost-effective than alternatives provisioned separately by individual agencies.
- The IGN aggregates traffic among IGN Participants onto common circuits, using the fewest number of circuits necessary. Since the cost of carrying a given amount of data over two circuits is generally higher than the cost of carrying that same amount of traffic over one larger circuit, the traffic aggregation provided by the IGN is more efficient and cost-effective than alternatives provisioned separately by individual agencies. In addition, aggregation onto a single circuit significantly simplifies the network interface from state government to a city or county, reducing the costs and risks to local government involved in maintaining multiple connections.
- The IGN leverages the state's buying power in negotiating with telcos to obtain circuit provisioning arrangements more favorable to agencies. Telco contracts for circuits on the IGN generally reduce or eliminate the costs of terminating or relocating circuit connections. Contracts also generally establish stable rates for longer periods than agencies would be able to achieve on their own, allowing the enterprise overall to predict biennial networking infrastructure costs more accurately.
- The IGN allows agencies to share skilled, specialized network engineering staff resources at the Department of Information Services (DIS) who monitor and maintain the core and local access network segments, and continuously plan for growth in the enterprise's demand for bandwidth and network services. Consolidating many network monitoring, maintenance, and capacity planning tasks frees state agencies to devote more resources to their core business missions and to direct technology support for their customers.
- The IGN allows DIS to manage the enterprise's interactions with telcos on behalf of IGN Participants. These interactions include routine maintenance, problem resolution, invoice management and correction of billing errors, and contract management. Consolidating vendor management tasks frees IGN Participants to devote more resources to their core business missions and to direct technology support for their customers.

5.2.2.2. Support for enterprise applications and other common solutions

The IGN supports enterprise applications and common solutions in the following ways.

- The IGN provides local government entities with connectivity to applications provided by state agencies. A partial listing of these applications appears in Appendix D of **[IGN]**.
- The IGN provides local government entities the option of a common gateway to the public Internet. This is available to local governments as a separately-priced service.

5.2.2.3. Ensuring levels of network security, availability, and reliability commensurate with stakeholder (citizen, business, employee) expectations and business requirements

The IGN ensures levels of security, availability, and reliability commensurate with stakeholder expectations and requirements, in the following ways (see sections 5.2.1-5.2.5 of **[IGN]**).

- The IGN leverages the state network backbone's redundant core design, in which each node site is connected to at least two other node sites. Node sites have 72 hours of backup power supply, with further backup power provided by diesel generators. DIS maintains 24/7 on-site/on-call support for node site equipment, with spare equipment available on-site and next-day equipment replacement arrangements with vendors. Because of the IGN's ability to aggregate traffic and share node site facilities across the

enterprise, it provides these mechanisms to support high levels of availability and reliability in a cost-effective manner.

- Investments in Quality of Service mechanisms (detailed in section 5.2.7 of **[IGN]**) allow DIS to support Managed Bandwidth according to IGN Participant requirements.
- The IGN is a private network with known end points and managed gateways. A single managed entry point for each IGN participant protects the networks of local government and simplifies threat prevention. The IGN is more protected than public network alternatives, such as the Internet.
- Managed security gateways provide connectivity and managed access control between the IGN and other networks. See section 4 of **[IGN]** for more information on these gateways.
- All participants in the IGN (state agencies and local government entities) sign a service-level agreement (SLA) in order to obtain access to the network. The IGN SLA requires participants to adhere to security practices and principles outlined in section 5.2.1 of **[IGN]**.
- IGN Participants may implement additional layers of security (for instance, Virtual Private Networks (VPNs)) when deploying applications to IGN users if the application or data involved require stronger security measures.
- The statewide backbone network supports the IGN. It is based on vendor-provided Synchronous Optical Network (SONET) circuits. The physical ring topology and protection capabilities of SONET improve the reliability and availability of the IGN. More recently, vast improvements to this optical technology have become available in the marketplace. SONET framed DWDM wave services are the next step for SONET based networks. The next generation of the statewide backbone network will use SONET framed DWDM wave services and multi-service provisioning platforms (MSPP). MSPPs provide the usual capabilities of SONET add-drop multiplexers (ADM) with support for multiple rings and additional protocols. The new network design provides increased bandwidth, provisioning flexibility, and management and operational enhancements. It will support a variety of protocols and services while providing SONET reliability and availability. According to Gartner, "the majority of optical networks currently used in support of high-speed Ethernet services are SONET-based" ([Gartner Ethernet Report], p.5). For local access and customer site connectivity to the IGN, DIS uses the most current technology available from service providers to meet customer requirements. These factors align the IGN with current technology and industry direction.

5.2.2.4. Support for interoperable exchange of information and linkage of business processes among agencies

The IGN supports exchange of information and linkage of business processes among IGN Participants in the following ways.

- The IGN provides underlying network transport for existing service infrastructure, such as the DIS Secure File Transfer service.
- The IGN satisfies underlying network transport requirements for the infrastructure elements of the future integration architecture for the state government enterprise (see **[CITRA]**), that will include integration of state and local government systems. The IGN will enable composite applications among state and local government, such as the Enterprise Business Portal and Enterprise Geographic Information Technology Portal, in a more cost-effective and efficient manner than alternative networking approaches.
- The IGN streamlines and simplifies integration among state and local government by:

- Allowing agencies to use common integration infrastructure, rather than selecting integration infrastructure for each project, state agency, or business area
- Encouraging the delivery of applications and exchange of information over the same network, simplifying the technology environment for state agencies and local government

5.2.2.5. Flexibility and Business Agility

The IGN supports flexibility and business agility in the following ways.

- DIS constantly monitors and manages the IGN circuits to ensure adequate bandwidth exists to support changes in business requirements. The IGN is designed to scale without disruption to the network environments of state agencies or local government entities.
- DIS negotiates specific customer requirements regarding Quality of Service and support on a customer-by-customer basis
- The IGN leverages the state's buying power to obtain favorable terms from telcos regarding termination and relocation of circuits, providing IGN Participants with generally greater flexibility and agility that they could achieve alone

5.2.2.6. Implications

The designation of the IGN as common, shared infrastructure has the following implications, in addition to the benefits described in the previous sections.

- Future networking investments may be necessary to migrate these connections to the IGN. This may include building a migration plan and risk mitigation strategies, as well as funding migration projects for each agency.
- Investments in expansion of IGN capacity (circuits, equipment, and administrative resources) may be necessary to improve the capability and features of the IGN.

6. References

CITRA — Washington State Information Services Board, Enterprise Architecture Committee (2006). *Conceptual Integration Technical Reference Architecture*, Enterprise Architecture Committee Document.

Gartner Ethernet Report — Gartner Inc. (2006). *An Introduction to High-Speed Ethernet Services in the U.S.* Gartner ID DPRO-111738.

IGN — Washington State Information Services Board, Enterprise Architecture Committee (2006). *InterGovernmental Network Solution Set*, Enterprise Architecture Committee Document

Investment Standards — Washington State Information Services Board (2003). *Information Technology Investment Standards*.

IP Telephony Domain — Washington Department of Information Services, Enterprise Architecture Program (2006). *IP Telephony Domain*, Documenter Team Draft.

NBCG — Washington State Department of Information Services, Enterprise Architecture Program (2006). *Network Business Case Guidelines*, Documenter Team Draft

Principles	Washington State Information Services Board (2004). *Over-Arching Enterprise Architecture Principles*.
SGN	Washington State Information Services Board, Enterprise Architecture Committee (2006). *State Government Network Solution Set*, Enterprise Architecture Committee Document

Appendix A: Documenter Team

This document was developed through the Networking Standards enterprise architecture initiative, chartered December 7, 2005. The following individuals were members of the Documenter Team for this initiative, and participated in review of this document.

- Scott Came, Department of Information Services
- David Curtiss, Department of Licensing
- Dennis DeFries, Department of Transportation
- Paul Warren Douglas, Department of Information Services
- Mark Fortier, Office of Financial Management
- Mike Frost, Department of Social and Health Services
- Ron Kappes, Department of Information Services
- Geoff Lakeman, University of Washington
- Lorraine Louderback, Department of Corrections
- Stu Lundmark, Washington State Patrol
- Fred McDowell, Legislative Service Center
- Laura Parma, Department of Information Services
- Dan Parsons, Washington State Patrol
- Michael Partlow, Department of Information Services
- Joe Russo, Washington State Patrol
- Peter Tamayo, Department of Retirement Systems

Appendix B: Review Log

The following feedback on this document was received by the Enterprise Architecture Program; the response to each contribution is noted below.

Review by whom and when	Contribution	Response
EA Committee May 31, 2006	• Improve characterization of SONET and network technical currency • Change implications from "will" to "may" • Recommend that DIS be responsible for identifying non-IGN state-local network connections • Change review period of standard to 12 months from 6	Incorporated into document
EA Committee June 14, 2006	• Remove suggestion that DIS should conduct an inventory of non-IGN network circuits	Incorporated into document
ISB September 14, 2006	• Adopted by ISB	Adopted and posted