

---

11/18/09

**The InterGovernmental Network (IGN)** provides connectivity among state agencies, counties, and local government entities. It is managed by the Department of Information Services (DIS).

State agencies that contract with DIS for IGN resources - called ANCHOR TENANTS - support IGN applications and ensure bandwidth for applications deployed to client groups within counties and cities. Additionally, many local governments use the IGN as their Internet Service Provider (ISP).

Some state agencies deploy applications to counties and cities via the IGN, but do not contract for IGN resources.

The IGN has a physical network aggregation presence in all 39 Washington counties and a number of cities, which allows application access and information sharing across all levels of government.

On a contextual level, the IGN contains several components.

- IGN Core is the segment owned and managed by DIS that contains the Data Center and the DIS Regional Node Sites. The IGN Core includes data processing equipment, carrier-class switching equipment, primary transport circuits, and support infrastructure. Some IGN applications are deployed directly on the IGN.
- IGN POINT OF PRESENCE (POP) is a DIS managed router that marks the demarcation point (DEMARC) where DIS' managed network control ends and the county's begins.
- IGN POP ACCESS CIRCUIT connects the IGN Core to an IGN POP. IGN POP Access Circuits can be one or more DS-1 private lines, DS-1 Frame Relay, or 10/100 Mbps Ethernet circuits.
- MANAGED SECURITY GATEWAYS provide connectivity and managed access control between networks. DIS manages the following gateways for the IGN:
  - SGN Gateway – provides managed interconnection between the SGN and the IGN.
  - Internet Gateway – provides outbound access to the Internet and limited inbound access for email.
  - Business Partner Gateway – provides connections to private organization's network applications, such as Premera Blue Cross, for agencies and local governments.
  - Service Provider Gateway – provides connections to wireless network services with companies, such as Cingular, for local governments.

11/18/09

## Connected Locations

There are 39 POPs that connect the counties to the IGN. The POPs are routers which are owned and managed by DIS, and are typically located in a county's main administrative office. The POPs provide a connection to a local government's corporate network.

The Managed Security Gateways provide IGN connection to the SGN, the Internet, Business Partner networks, and Service Providers.

In addition to the county connections, there are other local government entities connected to the IGN (e.g. cities, tribes, health districts, etc).

## TRAFFIC:

The IGN is exclusively INTERNET PROTOCOL (IP)-based and is capable of carrying data to any point across the network.

## SERVICES

Examples of services that are available for the IGN include:

- Anchor Tenant applications.
- Internet connectivity.
- Managed Security Gateways.
- Application access and information exchange between local governments.
- Connectivity to specialized external service providers (e.g. wireless access for local law enforcement agencies).

## BANDWIDTH:

Anchor Tenants and local governments subscribe to bandwidths from 128 Kbps to 10/100 Mbps Ethernet

---

## SECURITY

The IGN is a PRIVATE NETWORK with known end points and tenants and is separated from the public Internet and the SGN via the Managed Security Gateways. A single managed entry point, the POP, protects the security of local government networks and simplifies threat prevention. The structure of a dedicated network minimizes the risk of disruption during times of Internet instability as a result of viruses, worms, and denial of service attacks. Such separation enables applications and information sharing among state, county, and city government entities to continue operating, even during periods of Internet instability.

DIS provides Managed Security Gateways to facilitate authorized access for:

11/18/09

- The Internet to the IGN.
- BUSINESS PARTNER NETWORKS to the IGN.
- SERVICE PROVIDER NETWORKS to the IGN.
- IGN access to the SGN.

Participants agree to follow security principles in conjunction with terms and conditions set forth in Service Level Agreements (SLAs) such as:

- The security of applications, data, and business processes are the responsibility of their respective owners. Each government entity operating a network is responsible for IGN access, authorization, and authentication. This is a requirement and a design principle of the network.
- The participants shall not make new connections to other networks (including ISPs) while receiving IGN services without prior review and approval by DIS.
- The participants will provide DIS with a list of all network addresses.
- The participants will not implement new network addresses without prior review by DIS.
- The participants will not install dial-up access systems, connect to other networks, or implement other network changes that could compromise security by potentially enabling unauthorized access to the IGN without prior review and approval by DIS.

#### FACILITY SECURITY:

The POPs are located within the county locations where facility security is managed by the counties.

IGN participants agree that the hosts, systems, gateways, etc. connected to the county network will be restricted to authorized use by physical security (i.e. the hosts will be in locations preventing unauthorized use) and/or user authentication managed by the IGN participant (e.g., user ID and passwords or other authentication). Extending use to non-customer locations will not be permitted unless such use is under the control and management of the county.

DIS manages the physical security for the Managed Security Gateways and the IGN Core.

---

#### FAULT TOLERANCE

Within the IGN Core, the IGN has the same fault tolerant design as the SGN including:

- Carrier class equipment at all node sites.
- Node to Node circuits are designed with ROUTE DIVERSITY.
- SONET, ATM, IP overlay network.
- Ethernet Ring with physical diversity.
- On-site spares for IGN Core equipment.
- 24/7 on-site maintenance for IGN Core equipment.

---

11/18/09

A POP is connected to a single DIS node site within the IGN Core. Failure of the node site would cause the POP to be disabled.

---

### **BUSINESS CONTINUITY**

The IGN Core is designed to support the recovery of key agency business services and functions. It is designed to continue operations in the event of the loss of a single node. Mission critical network connections based on business requirements are redundant.

Within the IGN Core, Node sites are connected to at least two other nodes. Node sites have UPS with fuel on-site for 72 hours. Node site equipment is designed to carrier class standards where possible. Advanced vendor on-site and technical support is maintained on all node equipment. Spare equipment is located on-site. Node sites are staffed during business hours and staff is available 24/7.

Business Continuity of the IGN applications is the responsibility of each agency or local government application owner.

### **PROBLEM MANAGEMENT**

DIS monitors the IGN network, including the Core and POPS, and the operations center is staffed 24/7. Problems are logged into a trouble ticketing system for timely resolution. Problems are reported as follows:

**IGN Core:** All core network technology has fault management systems that report problems in real-time. Problems are logged and tracked until resolution. Affected customers are notified and provided status throughout the troubleshooting process.

**IGN POP:** DIS managed network equipment is monitored 24/7. DIS operations staff initiates troubleshooting procedures in the event of a problem. Customers can report problems 24/7 using a DIS provided toll-free number. All calls are logged and customers receive a response in accordance to service level agreements.

---

### **QUALITY OF SERVICE**

The IGN provides BEST EFFORT Quality of Service (QoS) support for IP traffic. Bandwidth utilization is measured and managed to meet contracted service levels with IGN participants.

The IGN Core is built on a **MULTIPROTOCOL LABEL SWITCHING (MPLS)** infrastructure. The MPLS infrastructure supports **DIFFSERV** (differentiated services) QoS capabilities. IGN traffic on the MPLS infrastructure is remarked to the best effort service class.

DIS is currently implementing **IGN MANAGED BANDWIDTH**. Anchor Tenants purchase a

---

11/18/09

minimum commitment of transport bandwidth to each IGN POP for support of their applications . DIS configures packet classification and policing on the IGN POP Access Circuits to ensure Anchor Tenant applications receive at least the minimum commitment of bandwidth to each IGN POP.

---

### **SCALABILITY**

The network scales to meet customer needs. The network can scale to add customer sites, bandwidth capacity, services, and support additional data traffic.

IGN Core: The core segment is designed to support network growth over three to five year periods. Circuits among nodes are contracted for three to five year periods and networking devices are designed to accommodate projected growth.

---

### **VENDOR INVOICE MANAGEMENT AND CUSTOMER BILLING**

DIS has staff and automated systems to assure vendor invoice management and customer billing accuracy. Service features applicable to the IGN Core include:

- Invoice Reconciliation – Circuit and equipment invoices are consistent with contracts and network configuration.
- Electronic Invoicing – Vendor agreements to allow billing data transfer in electronic form.
- Billing Reports Media – Provides delivery options for billing reports.
- Consolidated Customer Billing – Multiple vendor bills are consolidated into a single DIS invoice. Circuit and equipment costs are organized around customer location, programs, projects, or based on other agency accounting needs.

### **CONTRACT NEGOTIATION AND MANAGEMENT**

The IGN is built upon infrastructure resources of the SGN. DIS leverages IGN and SGN aggregated customer demand to obtain contract terms and conditions with the service providers.

The following benefits of contract management are applicable to the IGN Core, POPs, and Managed Security Gateways:

- Termination Liability – Mitigates the financial penalty of circuit location changes, additions, or deletions.
- Performance Guarantee – DIS negotiates performance guarantees.
- Credits for Non Performance – DIS negotiates guaranteed credits where possible.
- Service Migration – Manages the financial risk of upgrading to new services as they become available.

11/18/09

- Network Equipment and Maintenance – DIS negotiates equipment discounts and maintenance agreements through high-volume purchases.
- 

## **FLEXIBILITY**

IGN Core: The core is designed to handle growth in bandwidth and hardware in 3-5 year planning cycles. Bandwidth capacity between DIS node sites changes as needed to meet participant networking requirements.

---

## **SUPPORTABILITY**

IGN Core: DIS monitors and implements all networking equipment and network software upgrades, including patch management. DIS performs core network maintenance, as much as possible, in ways to minimize interruptions to services and customers. Maintenance events are scheduled in advance with customers according to the Data Center Conventions Manual. Impact on customers is the primary consideration for determining the maintenance window of specific maintenance events. DIS negotiates a published schedule with its customers and notifies them in advance of any changes.

Private sector: **TELCO** vendors are required to schedule maintenance activities outside of core business hours between 6 a.m. to 6 p.m.

---