NJ Department of Human Services

Distributed Information Technology Architecture

For 2005

"Building Technology Solutions that Support the Care, Protection and Empowerment of our Clients"

JAMES M. DAVY
Commissioner

JOSEPH OCHS
Chief of Staff

JACOB EAPEN
Assistant Commissioner

LOUIS MARINO
Chief Technology Officer

Document Version Control

Version 1 published 6/25/04.

Version 2 published 10/12/04.

1. Added Hubs/Switches/Routers, Firewalls, Specialized Appliances to Appendix 3.

Version 3 published 2/18/05.

1. Added this version control sheet.
2. Added Single-SignOn description in Application Development and Infrastructure.
3. Added Development Environment and Storage Area Network diagrams as Appendices and updated Logical and Physical Network diagrams.

Comments

All questions and comments concerning this document and its contents should be directed to the Department of Human Services Chief Technology Officer.

Table of Contents

Document Version Control 2
General Overview 4
Facilities and Environment 5
- Security and Monitoring 5
- Power 6
- Environmental Climate Control 6
- Fire Detection and Suppression Systems 6

DHS Network 7
- Tiered Internet Architecture 7
- DHS Network Architecture 7

Enterprise Servers and Operating Systems 9
- Shared Server Infrastructure 9
- Storage Area Network 9
- Backup and Recovery 9
- Distributed Information Technology (IT) Architecture 10

Data Management 12
- Database Management Systems (DBMS) 12
- Data Transfers 12

Application Development and Infrastructure 13
- Application Development Environment and Programming Languages 13
- Service Oriented Architecture 13
- Personal Computer Desktops 13
- Geographic Information System (GIS) Services 13
- Single-SignOn Service 14

Integration and Messaging 15
- Message Oriented Middleware 15
- Enterprise Application Integration (EAI) 15
- Web to Host 15

Presentation and Portal Services 16
- Portal Management 16

Identity Management 17
- Public Key Infrastructure 17
- Enterprise Directory Services 17

Network Monitoring and Performance Assessment 18
Enterprise Systems Management (ESM) Architecture 19
- Enterprise Help Desk 19

Appendix 1 - Logical Network 20
Appendix 2 - Physical Network 21
Appendix 3 - Storage Area Network 22
Appendix 4 - Development Environment 23
Appendix 5 - Products and Technologies 24

General Overview

The New Jersey Department of Human Services (DHS) Office of Information Systems (OIS) is responsible for the development, maintenance and hosting of many applications serving the agency, its employees, business partners, and clients throughout the State.

The current DHS OIS computing and data communications environment is an amalgam of centrally managed enterprise servers; division and departmental application, database, and file servers; county-administered applications; and desktop clients. Network interconnectivity is provided via Local Area Networks (LANs), Campus Area Networks (CANs), and Wide Area Networks (WANs) linking DHS facilities to the State Hub, Capital Place One, the Garden State Network (GSN), and the Internet. This environment supports hundreds of various size applications and services across all the DHS divisions. The computing environment includes security and disaster recovery resources.

DHS has implemented and is expanding the delivery of distributed services through the Internet and intranets. Additionally, DHS is currently in the process of initiating a number of large network and application modernizations in an effort to enhance client access to DHS services, while empowering employees with expanded client and program information and analysis.

Facilities and Environment

The DHS computing facilities and network are distributed across the State. There are six computer centers:

- Capital Place One (CP1)
- Quakerbridge Center (QBC)
- Luczak Data Center (LDC)
- Capital Center (CC)
- State Police Systems and Communications Center (SAC)
- Office of Information Technology (Hub)

There are nine communications hub sites:

- Woodbridge Developmental Center (Woodbridge)
- Joseph Kohn Rehabilitation Center (JKRC)
- Capital Place One (CP1)
- Quakerbridge Center (QBC)
- Capital Center (CC)
- State Police Systems and Communications Center (SAC)
- Office of Information Technology (Hub)
- Woodbine Developmental Center (Woodbine)
- Ancora Psychiatric Hospital (Ancora)

Security and Monitoring

DHS employs physical security to ensure that client assets are safe, secure, and protected against outside intrusion and unauthorized access. Uniformed and civilian personnel control the movement of all persons within the center facilities. Security measures include registration of all visitors, viewable credentials worn by employees and visitors, access key controlled door locks, camera surveillance systems and random patrolling of facilities by security personnel.

Access to secured areas is permitted via an authorized badge access system that is maintained by the DHS Facilities Group. The access badge system database is audited to ensure that only authorized personnel are permitted access to secure areas within the data center facilities. All previously authorized personnel that are no longer working with DHS or for the State of New Jersey are purged from the access badge system database.

The majority of the servers are housed within standard unlocked cabinet systems that are open and available to authorized system administrators (and vendors under system administrator supervision) to perform standard software, hardware, and diagnostic services. Locked smart cabinet systems are utilized to secure access to sensitive servers and the information they contain.

The responsibility of the Computer Center personnel is to ensure the availability, reliability and operational status of all production servers, the network, the environmental systems, and security systems within the facility. Facility Management, Capacity/Performance and Network Management systems and software are utilized by the Computer Center personnel to proactively monitor and display the status of these systems within the facility.

Alarms are strategically placed throughout each computer center facility and within the server rooms to alert personnel in the event of an unauthorized intrusion, environmental system failure, or fire. All support systems within these facilities are tested on a regularly scheduled basis to ensure that the alarm systems properly operate.

Power

Each computer center is fed commercial power to multiple onsite transformers. Each data center contains redundant power systems to achieve maximum availability and reliability of all systems. Computer Center personnel closely monitor external and internal power distribution systems to maximize system uptime.

Each computer center maintains multiple Uninterruptible Power Sources (UPS) that allow all critical systems and associated equipment to remain powered up and operational in the event of a power failure.

Environmental Climate Control

Each computer center is equipped with a complete environmental system to guarantee optimal heating, cooling, and humidity levels in order to facilitate the availability, reliability, and continued operation of all systems.

Fire Detection and Suppression Systems

Each computer center has a complete fire detection and suppression system equipped with an annunciator panel that shows the current status of the fire detection and suppression system.

DHS Network

Tiered Internet Architecture

DHS has implemented an n-tier network architecture to provide state-of-the-art security design to DHS' network resources. This architecture consists of five firewalls protecting our core network from the Internet world.

According to the DHS security policy, an Internet user can only communicate with servers on the public tier. A public tier server can only communicate with a secure tier server, and only a secure tier server can communicate with core network. A server or workstation can communicate with any device on a higher layer, and the response can come back to only that originating device. Therefore, in communicating downward in the model from the Internet, at each tier there must be a process, which takes a request and hands it down to the next layer. Typically, this model fits well with distributed application design, where tier 1 handles presentation (Web servers), tier 2 handles business logic (Application servers), and tier 3 houses the data (Data servers).

DHS Network Architecture

DHS builds and manages a multi-agency, TCP/IP network across New Jersey. This network supports agencies through dedicated and switched services in support of centralized and distributed data processing applications resident in mainframe, mini-computer, local area network (LAN), and personal computer environments. The DHS network also provides network services such as DNS (domain name system), DHCP (Dynamic Host Configuration Protocol), Active Directory, Email, and Calendar.

The DHS network is comprised of nine communication hub sites. These sites are interconnected to form a statewide backbone network. The backbone is designed with multiple paths to increase service reliability and availability in the event of a failure. Primary transport technologies in use include frame relay (FR), Asynchronous Transfer Mode (ATM), T-1, T-3, OC3, and OC12. The major contracted carrier service providers at this time are AT&T and Verizon for the Garden State Network (GSN), the State's network maintained by the Office of Information Technology.

Internet access to DHS public information is provided through the State's public access Web server (www.state.nj.us). The DHS network firewall infrastructure provides a physical n-tier architecture designed for internal, external and extranet networks. The External firewall infrastructure has a tier 1 for web serving, tier 2 for application serving (business logic) and tier 3 for database serving. The Internal firewall infrastructure has a tier 1 for web serving, tier 2 for application serving (business logic) and tier 3 for database serving. The Extranet firewall infrastructure has a perimeter defense to restrict Extranet Partners to access only State mandated systems and network services by way of TCP/IP protocol and ports. Refer to Appendix 1 – logical network diagram.

The policy prohibits advancing inbound more than one tier at a time without a process to supervise communications with the next tier. Firewall rules are created to allow specific connection defined by specific ports. The typical public access is by port 80 (http) and 443 (https). Dialup services are provided to limited users through Cisco 5350 routers. It provides 56K asynchronous capabilities for remote access. Extranet connections require point-to-point connections from the vendor to the secure layer of the firewall infrastructure. The cost of these connections varies based on the circuit ordered.

Enterprise Servers and Operating Systems

Shared Server Infrastructure

The Shared Server Infrastructure (SSI) is located at the Hub and Capital Place One data centers. It is an area in each computer room where servers are centralized to offer a common location to manage the distributed environment. Optimizing key server resources through common logical and physical environments positions DHS to properly plan, manage and control a growing server infrastructure. The SSI supports the following operating system platforms:

- IBM AIX
- Sun Solaris
- Microsoft Windows

Storage Area Network

DHS manages one Storage Area Network (SAN) at Capital Place One in Trenton. The SAN consists of a communication infrastructure that provides physical connections, and a management layer, which organizes the connections, storage elements and computer systems so that data transfer is secure and robust. The DHS SAN attaches storage devices to servers in a networked fashion, using hubs, switches, bridges, and directors to build the topology.

Backup and Recovery

Database

For daily database backup, Oracle's Recovery Manager (RMAN) utility and Tivoli's Data Protection for Oracle (TDPO) product are utilized to perform "hot" physical backups to tape. A hot backup means that the databases being backed up actually remain open and available to end-users.

"Cold" physical backups are also performed in development environments only. In this case, the database is shut down and the key Oracle database components (control, database and redo log files) are backed up at the file system level via Tivoli Storage Manager (TSM).

Logical backups are performed where data (tables, stored procedures, etc.) is extracted with the Oracle Export Utility and stored in a binary file. Logical backups are used to supplement Physical backups.

For remote backup, Oracle's Data Guard product provides complete protection against corruptions and data loss. Redo data is synchronously transmitted from the primary production database to a remote, standby database. Data Guard automates the manual process of maintaining this standby copy of the production database. The standby

database can be used if the production database is taken offline for routine maintenance or becomes unexpectedly damaged or unavailable. Data Guard can also be configured in such a way to also provide off-line reporting capabilities.

Finally, copies of backup tape sets created by Tivoli Storage Manager (see above) are stored at a remote location for disaster recovery purposes.

IBM / AIX

For IBM pSeries servers, DHS uses a combination of AIX Operating System (OS) tools and third party products to permit a complete data solution for enterprise level storage management, backup and recovery across heterogeneous IT environments comprised of hardware devices, applications, databases, and operating systems.

At the Operating System level, Tivoli Storage Manager (TSM) provides policy-based back up and restoration functionality across the entire network so that a copy of business critical data can be kept secure at all times from both natural and unnatural disasters. TSM optimizes storage utilization, minimizes downtime and streamlines storage management. AIX operating system backup images are created using the AIX **mksysb** command.

Intel / Microsoft Windows

The Intel platform running all Microsoft Windows servers are backed up using Veritas BackupExec and PowerQuest V2I. Backups occur nightly, with full backups occurring daily or weekly with daily incrementals. The servers are imaged using the PowerQuest V2I software. A server image can be restored and data restored using these two products.

Sun / Solaris

The Sun platform running all Solaris servers are backed up using Veritas NetBackup. Backups occur nightly, with full backups occurring weekly with daily incrementals.

Distributed Information Technology (IT) Architecture

The distributed IT architecture is based on IBM pSeries (formerly RS/6000 Scalable Parallel (SP)) hardware running AIX UNIX, WebSphere and Oracle software for the J2EE model, and Dell hardware and Microsoft IIS, COM and SQL Server for the Microsoft model.

Web Serving:

- IBM pSeries (AIX UNIX) running IBM HTTP Server
- Dell Servers (Windows 2000/XP) running Microsoft Internet Information Services (IIS) and Microsoft Internet Security and Acceleration (ISA)

Application Serving:

- IBM pSeries running both Oracle Internet Application Server (iAS) and

IBM WebSphere Application Server software
- Dell Servers (Windows 2000/XP) running Microsoft Component Object Model (COM)

Data Serving:
- IBM pSeries (AIX UNIX) running Oracle
- Dell Servers (Windows 2000/XP) running Microsoft SQL
- IBM WebSphere MQ (formerly MQ Series)

Directory Serving:
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory

Network Architecture:
- DHS maintains an n-tiered logical network infrastructure (separate layers for client, presentation, application, data, etc.) to provide greater flexibility and scalability
- Public (Internet based) access is limited to the webserving tier only.
- Extranet access through a secure network infrastructure

Portal Environment:
- Microsoft Content Manager
- Microsoft SharePoint

Enterprise Public Key Infrastructure:
- VeriSign Managed PKI (for PKI certificate issuance)
- VeriSign Auto-Authentication software
- VeriSign Key Management

There are a number of development servers. Some provide staging and development for the Web applications utilizing HTML scripts and graphics bound for the state public web server and the department's intranet. Others are staging and development servers for Java and Microsoft applications bound for the application Web servers.

Data Management

DHS has built a logical data model and data management framework to manage a core of common data at the enterprise level. This strategy has enabled DHS to use relational technologies to collect, disseminate and maintain the integrity of critical data elements across multiple DHS programs. By adhering to common data standards, DHS will be able to:

- Collect data once and use it often, improving data accuracy
- Warehouse data more effectively for various needs
- Store data more effectively for a timelier and more complete information picture
- Better protect the privacy of individuals while improving access to non-restricted information

The intent is to manage the overall data assets to achieve optimal integration, sharing, access, and utilization of technology resources and infrastructure. DHS utilizes various concepts and tools to accomplish these goals. These include:

- Shared Data Warehouse and Data Mart
- Business Intelligence Tools
- Extract, Transform and Load (ETL) Tools
- Meta Data Management
- Data Modeling
- Data Quality Tools
- Data Cleansing
- Data Integration
- Data Mining

Database Management Systems (DBMS)

The strategic relational database for DHS is Oracle. DHS also maintains some SQL Server Relational DBMS databases.

Data Transfers

DHS has two ways of sending and receiving files for host to host transfer. The first method is a secure file transfer (SFT) utilizing advanced data encryption technologies. This is a manual interface through the DHS Citrix server environment. Connectivity is through the use of the Citrix client and authenticating to the Citrix server environment. The user selects the file needed to send, receive or browse and selects the source or destination of that file. The transfer occurs using 128-bit encryption and the user is advised of the success of that transfer. The second method is through the DHS firewall infrastructure using the private network. No transfers occur over the Internet or the public network.

Application Development and Infrastructure

Application Development Environment and Programming Languages

The application environment for new web browser based applications is object-oriented design using Java J2EE or .Net components running on WebSphere or MS IIS application servers. Programs are developed utilizing HTML, Java Server Pages, Java Script, Microsoft .Net components, Servlets, Java Beans and Enterprise Java Beans. The goal of the enterprise is to develop reusable components and make use of DHS standard shared architectural components.

Service Oriented Architecture and Enterprise Frameworks

The DHS strategic direction is the placement of existing and future services into an enterprise design consistent with service oriented architectures. An enterprise design moves otherwise wholly unique and separate designs into an architecture that supports sharing of business processes, technical services, and common data. Each program manages its own unique business rules and information but builds from a common data model. Enterprise frameworks provide the 'glue' that simplifies the required integration among the programs. Benefits include:

- Providing common technical services such as security, scheduling, and auditing,
- Utilizing shared human services functions such as case management,
- Presenting a common interface for users and clients, and
- Reduced development and maintenance costs.

Personal Computer Desktops

Department desktops use Windows operating systems with 95% of present deployments in Windows 2000 Professional or Windows XP Professional. The remaining 5% of desktops currently using Windows 95 or Windows 98 will be transitioned to Windows XP in FY05. See Appendix 3 for the standard configuration of desktop software.

Geographic Information System (GIS) Services

DHS currently has access to the State GIS services. The State's management and access of spatial data is facilitated through a gateway, which utilizes a combination of technologies including Oracle Spatial and Environmental Research Institute (ESRI) Arc Spatial Data Engine (ArcSDE). Spatial data is provided in a format that can be accessed by a variety of desktop GIS clients or by other applications using standard SQL queries. Any proposed solution that includes a GIS component and/or incorporates spatial data is evaluated, planned, designed, and implemented in concert with the OIT Office of GIS.

Single-SignOn Service

DHS uses a Single-SignOn process which employs an application Header control. It is in the form of a light-weight Java HTTP Servlet or a .NET user control. Either of these can be called or included in another application. It is a mandatory requirement for all DHS applications developed in Java or .NET to include this universal application banner/header in all their respective applications.

Integration and Messaging

Message Oriented Middleware

DHS has implemented IBM WebSphere MQ (formerly MQ Series) in many critical application environments for enterprise messaging between systems. WebSphere MQ is currently in production on the IBM pSeries platforms for connectivity to the J2EE application environment and IIS applications.

Enterprise Application Integration (EAI)

An EAI solution enables real-time data and workflow integration from one system to another. DHS uses IBM WebSphere MQ as its EAI product.

Web to Host

The State supports two Web to Host products; GWEB for access to the Bull environment and IBM Host Integrator for access to the IBM environment.

Presentation and Portal Services

DHS has implemented a distributed n-tiered technical architecture and production environment to facilitate the delivery of web based services to clients, business partners and employees of the State of New Jersey. The distributed architecture facilitates true portal functionality through the registration and management of intranet, extranet and Internet based members into appropriate portal venues. Management of portal members is role based; i.e., users are assigned one or more roles (e.g., DHS Client, DHS Employee, Provider, etc.), which govern their access to informational and transactional services.

The Distributed architecture provides the following functional services:

- User registration, authentication & security services
- Policy Management
- Directory Services
- Public Key Infrastructure
- Data, application and web serving platforms

Portal Management

The DHS portal environment is provided via a combination of:

- Microsoft Content Management Server software
- Microsoft SharePoint
- External LDAP directory and Microsoft SQL database services
- A custom administration tool, with an HTML user interface, written in .Net and served from the distributed application server platform

Access to the LDAP directory and SQL database services is managed by a custom .Net framework served from the distributed application server platform.

Identity Management

Public Key Infrastructure

DHS has implemented and is hosting a private certificate authority using products and services from VeriSign to implement an Public Key Infrastructure. DHS technical staff has implemented the following components for PKI:

- Registration
- Certificate Issuance
- Revocation of Certificates
- Storing and Retrieving Certificates
- Certificate Revocation Lists
- Key Lifecycle Management

The infrastructure meets the majority of PKI business requirements for Internet, Intranet and Extranet users. A distributed administration model gives the Office of Information Systems control over registration and issuance of certificates. DHS maintains the Certificate Revocation function, Certificate Revocation Lists, and Key Lifecycle management. Security requirements for the DHS Portal environment will vary, ranging from simple user name and password to more stringent requirements including the use of PKI.

Enterprise Directory Services

DHS maintains a SunONE Lightweight Directory Access Protocol (LDAP) compliant enterprise directory service for all DHS employees (DHS Master Directory). It is currently in use supporting PKI deployments as well as agency-based extranet user management. DHS personnel names, locations, telephone system data, and e-mail addresses have been integrated into the directory. Approximately 20,000 entries, one for each DHS employee, extranet business partner and community service provider organizations now reside in the directory. DHS is in the process of transitioning from the SunONE Directory to Microsoft Active Directory and Active Directory Application Module (ADAM).

DHS clients and business extranet partners will also be authenticated using ADAM to allow access to certain DHS services and applications. Authorization leverages pre-defined communities of users and applies role-based policy against those communities to ensure that non-DHS employees access and use only those services for which permission has been granted and is controlled by the application program staff.

Network Monitoring and Performance Assessment

IPSwitch Whatsup Gold and MRTG (Multi-protocol Routing Traffic Grapher) are used to perform baseline analysis of the existing network environment prior to deploying new and existing applications, and connectivity to Human Service network facilities. The existing application protocols and their respective volumes traversing the local (LAN) and wide area network (WAN) are identified and their bandwidth consumption, average response times and traffic volumes measured. This analysis can be used as a benchmark comparison against future performance. In instances where a wide area network connection employs Frame Relay technologies, the circuit utilization can be obtained.

Etherpeek and TCPDump are used to collect local area network traffic packets. The packet analysis provides data for tracking host to host connectivity and type of data being sent and received over TCP/IP, ip addresses, protocols and port numbers.

Enterprise Systems Management (ESM) Architecture

Enterprise Systems Management (ESM) can be concisely defined as the end-to-end management of the evolving, heterogeneous, multi-platform, distributed computing environment. ESM tools are used to detect, correlate, escalate and prioritize events; manage responses to those events; and report on those incidents in a pro-active, real-time event management environment in order to provide a secure, highly available, robust, multi-platform enterprise infrastructure that meets or exceeds system requirements.

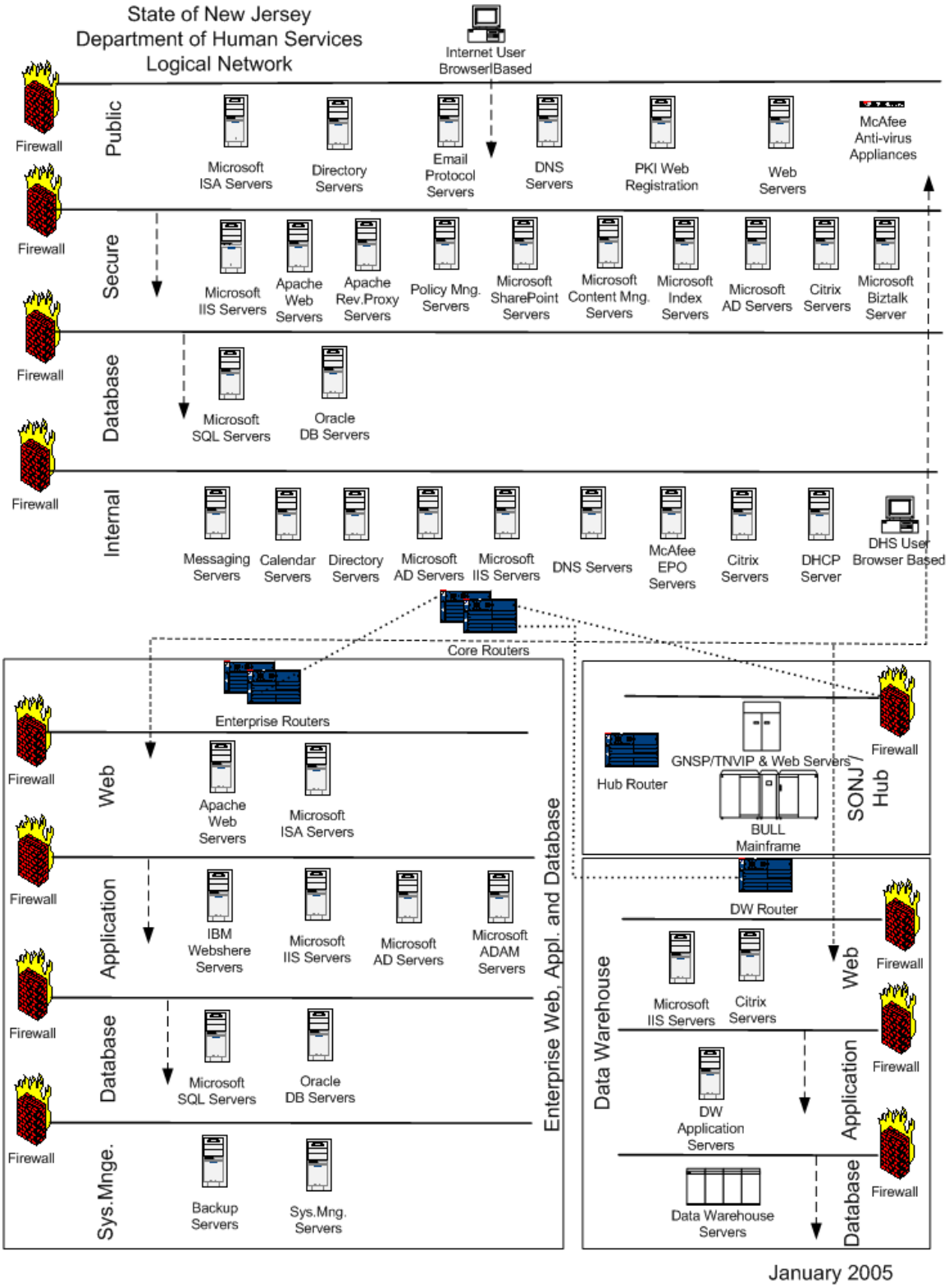
DHS has implemented various monitors, distributed storage management, and event management components that are integrated with problem management for the automatic generation of trouble tickets for critical events. Event management is via the Tivoli Enterprise Console (TEC), along with the software products that report to TEC as well as detect, record, and correlate all enterprise significant events.

DHS will also implement Tivoli's Configuration Manager for inventory, remote control and monitoring of transaction performance (to monitor the performance and availability of distributed and enterprise transactions) and Alloy Software Asset Navigator for inventory of hardware and software.

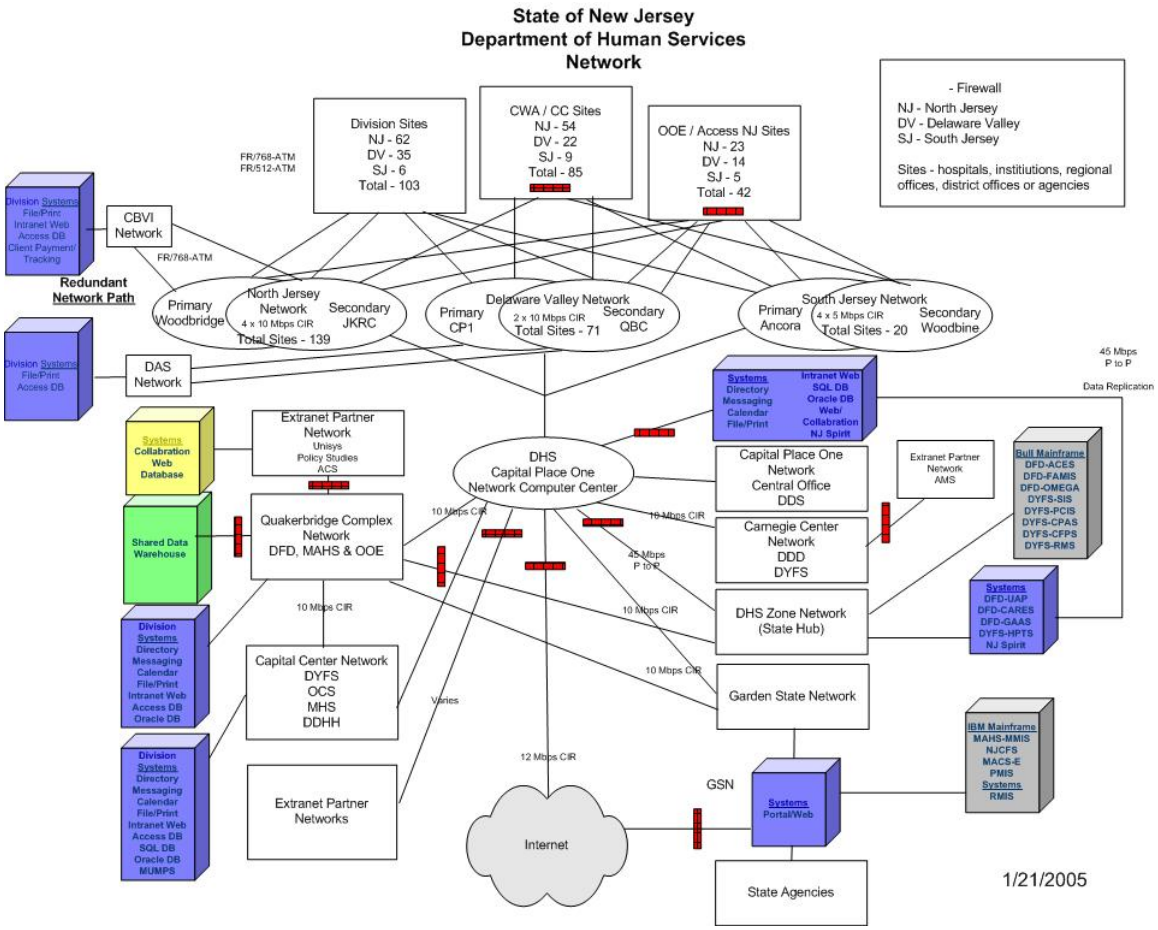
Enterprise Help Desk

Infra Corporation's *infraEnterprise* Service (Help) Desk application is used for call management, problem management and change management. This product improves client application availability through the automatic notification and escalation of problems via pager and email and the integration of problem and change management. A change control module is also included.

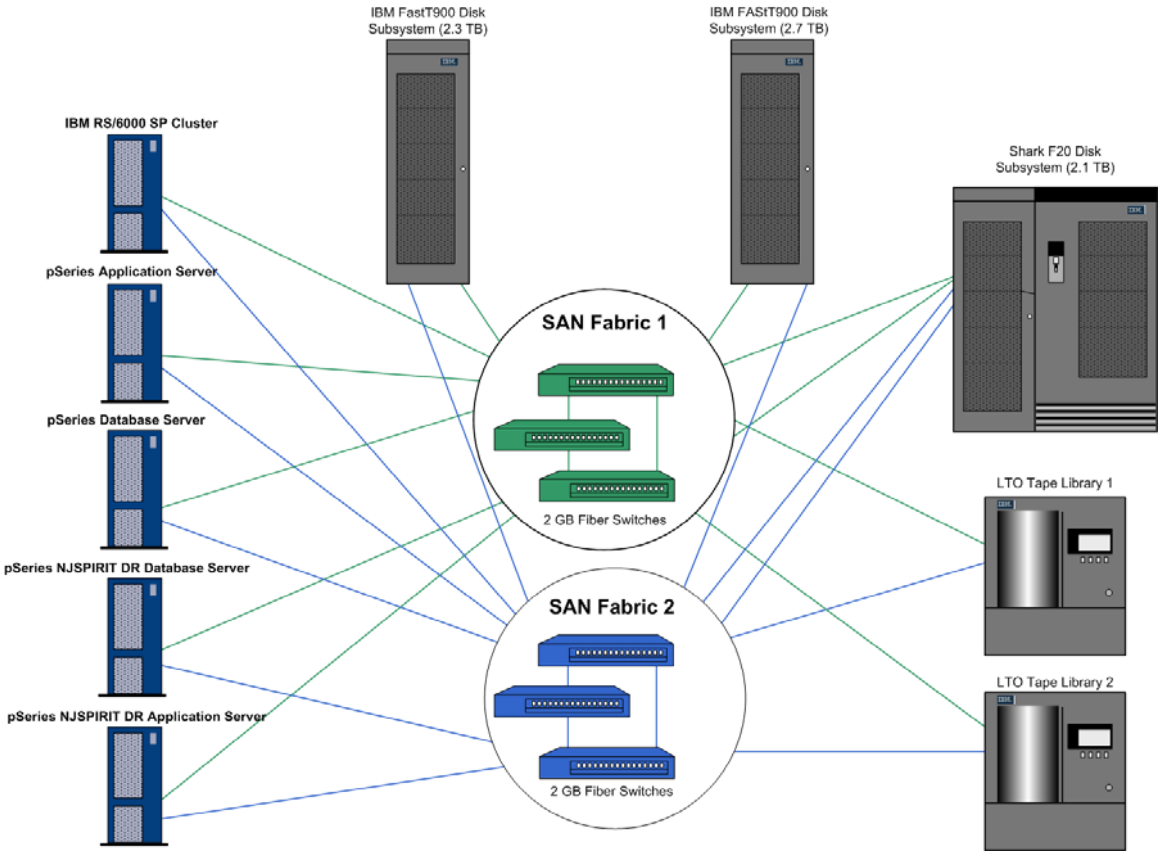
Appendix 1 - Logical Network Diagram



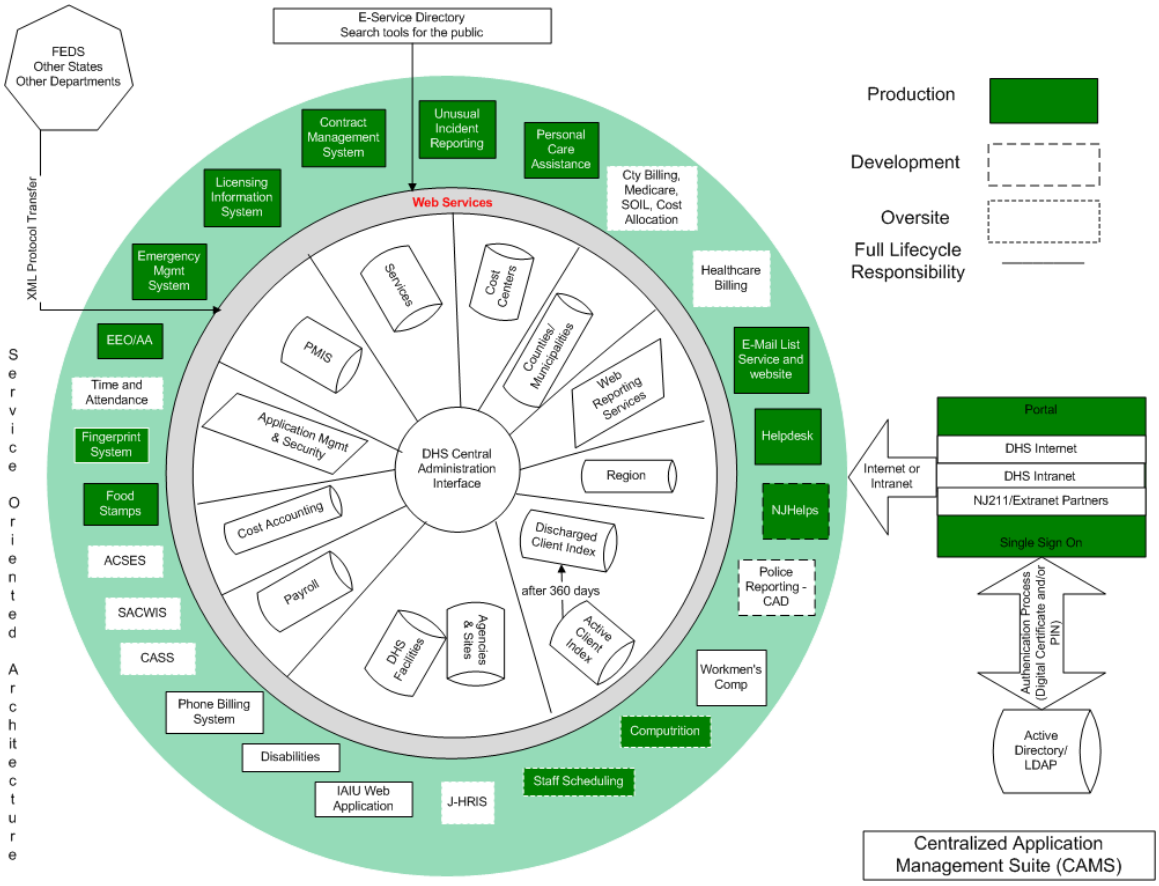
Appendix 2 - Physical Network Diagram



Appendix 3 – Storage Area Network Diagram



Appendix 4 – Development Environment



DHS IT is applying this development methodology as a means to:

- eliminate duplicate functions in each division by building and supporting then from a framework perspective
- pull common data together to eliminate duplication
- standardize access to data via web services

Appendix 5 - Products and Technologies

* Direction Key:

P = Preferred — This technology represents our strategic direction. DHS will give priority to this technology.

A = Acceptable — This technology represents our minimum requirements. DHS considers this technology adequate/satisfactory.

S = Sunset — This technology is in use, but DHS deems this technology undesirable/unacceptable.

Note: While release versions are not listed for products below, DHS expects to use the most current or next current released production version at the time of implementation.

Category	Product	Direction*
Operating Systems - Servers		
	AIX UNIX	P
	LINUX	A
	Solaris - to be replaced by Microsoft Exchange servers	S
	Windows 2000 Server	A
	Windows NT	S
	Windows 2003 Server	P
Operating Systems – PCs		
	Windows 2000	A
	Windows NT	S
	Windows XP	P
Database Platforms		
	Oracle	P
	Microsoft SQL Server	A
Languages		
	COBOL	A
	J2EE Java	P
	HTML	P
	JavaScript	P
	SQL	A
	Oracle Forms/Reports/PL SQL	S
	XML	P

Category	Product	Direction*
Portal Services		
	Microsoft SharePoint	P
	Oracle Portal Server	A
Identity Management / Policy Services		
	DHS Single Sign On Module, authentication and application controls through LDAP	P
Directory Services		
	Microsoft Active Directory	P
	Sun ONE LDAP	A
	Microsoft Active Directory Application Module (ADAM)	P
Data Transfer		
	Secure File Transfer	P
	Direct Private Connection	A
EAI (Enterprise Application Integration)		
	IBM WebSphere MQ Series	P
GIS Technology		
	ESRI: ArcSDE – Spatial Data Hosting via State services	P
Application Servers		
	Oracle Internet Application Server (iAS)	A
	IBM WebSphere Application Server	P
	Microsoft Internet Security and Acceleration (ISA)	P
Web Servers		
	IBM HTTP Server	P
	Microsoft IIS	P
	Oracle Apache	P
Messaging Technology		
	IBM WebSphere MQ Series	P
Security Tools		
	ACF2	A
	VeriSign PKI	P
	SSL	A
Imaging		
	IBM Content Manager	P

Category	Product	Direction*
Network Management		
	IPSwitch Whatsup	P
	HP OpenView	P
	Tivoli Suite	P
Mail		
	Microsoft Outlook	P
	Microsoft Outlook Express	P
	Netscape Messenger Mail	S
Calendar		
	Netscape Calendar	S
	Microsoft Outlook	P
Audio / Video		
	Real Media	A
	Microsoft	A
	Avid Xpress	A
OLAP (Online Analytical Processing)		
	Business Objects	P
	Web Focus	P
Software Administration		
	SourceSafe	P
Data Warehouse Products		
	Informatica (ETL Platform)	P
	Trillium (Data Integration - UCI)	P
	MetaCenter (Meta Data Repository)	A
	Teleran i-Sight (Performance Tool)	P
	ArcView (Geographic Analysis)	P
	Citrix Metaframe (Network Tool)	P
Data Mining & Statistical Analysis		
	BusinessObjects (Data Retrieval, Reporting & Analysis)	P
	SPSS (Statistical Analysis)	A
	SPSS Clementine (Data Miner)	A
	QueryPath (Data Retrieval and Reporting)	A

Category	Product	Direction*
Reporting Tools		
	Oracle Reports	A
	Crystal Reports	A
	Web Focus	S
	Magna8	S
Development Tools		
	Macromedia DreamWeaver (HTML)	A
	Forte	P
	Adobe	A
	Quark	A
	Macromedia Flash	A
	Macromedia Fireworks	A
	Pagemaker	A
	Microsoft FrontPage	P
	Microsoft Developer Studio	P
	Microsoft Source Safe	P
	Rationale Rapid Application Development	P
Performance Assessment Tools		
	IPSwitch Whatsup Gold	P
	Multi-protocol Routing Traffic Grapher (MRTG)	P
	WildPackets Etherpeek	P
	TCPDump	P
Desktop Software		
	Netscape Communicator	S
	Internet Explorer	P
	Office 97	S
	Office XP	P
	McAfee VirusScan	P
	McAfee ePolicy Orchestrator (ePO)	P
	Tivoli TME	P
	Microsoft SMS	P
	Glink	P
	Oracle Client	P
	Adobe Acrobat	P
	ExtendNet Connect for TCP/IP	P
	HP JetDirect Printing System	P

Category	Product	Direction*
Hubs/Switches/Routers		
	Data: Cisco	P
	VOIP: Avaya	P
	Data: 3COM	S
Firewalls		
	Cisco – Pix	P
	Nokia – Check Point FW1	P
Specialized Appliances		
	Internet Filter: XSTOP	P
	Antivirus: McAfee	P
	Cache Engine: Cisco	P
	Load Balancing: Cisco and Intel	P