O. Proposed Technical Plan

NeuStar's proposed technical solution for usTLD operations meets all of the U.S. Department of Commerce's (DOC's) requirements for the existing and expanded usTLD, in addition to providing numerous improvements and enhancements:

Full Existing and Expanded usTLD Space Support—NeuStar will provide support for the existing usTLD space, which will include support for existing delegees, as well as providing registrar service for new and existing registrants. In addition, NeuStar will provide full registry support to all eligible registrars for the expanded usTLD space.

Database Centralization—NeuStar proposes to implement a Centralized usTLD Database including a Delegated Manager Database and a centralized Whois. This approach will offer improved consistency and accuracy of data.

Improved Reliability—In support of registry, registrar, database, and information services for the usTLD, NeuStar will implement co-active data centers and a number of nameserver data centers to create a resilient infrastructure protected against outages through redundancy, fault tolerance, and geographic dispersion. The benefits to the U.S Internet community are improved availability and better access to DNS services.

HIGHLIGHTS

- **Co-active, redundant Enhanced Shared Registration System Data Centers in VA and IL with two-way replication**
- **Three geographically dispersed nameserver Data Centers (CA, VA, & IL). Each Data Center containing multiple load balanced nameservers**
- **High availability cluster architecture with flexibility, scalability, and reliability**
- **Redundant Database Servers with seamless failover for applications**
- **Enhanced SRS is sized initially to handle the projected workload but can grow incrementally**
- **Enhanced SRS application software architecture is standards based, open systems to facilitate cost-effective upgrade**
- **Rapid Application Development Methodology for new application development**

Providing Real-Time Responsiveness—NeuStar will implement near-real-time updates to the zone files and the Whois database. The benefit to the U.S Internet community is the elimination of delay-caused confusion over domain name registrations.

Eliminating Bottlenecks—NeuStar's high-availability cluster architecture provides scalable processing throughput, dynamic load balancing between the two data centers, and multiple high-speed Internet connections. The benefit to the Internet user and registrar communities is the elimination of registry bottlenecks.

Encouraging Competition—NeuStar will develop and deploy a new, streamlined registry-registrar protocol for the expanded usTLD space: the eXtensible registry protocol (XRP). The XRP provides more features and functionality than the existing registry/registrar interface and far greater security. The benefits to the Internet community are greatly improved Internet stability and increased public confidence. NeuStar will work with the Internet Engineering Task Force (IETF) to bring the protocol to standard status.

NeuStar's proposed usTLD technical solution is based on our experience with the Number Portability Administration Center (NPAC) and with the .biz registry operations. As requested, Section O.1 provides an overview of our proposed facilities and systems; subsequent sections expand this overview into a comprehensive technical plan for registry operations detailing the equipment software, hardware, and related technology NeuStar will use to meet the usTLD program objectives and needs.

O.1 Proposed Technical Facilities and Systems

NeuStar proposes world-class redundant Enhanced Shared Registration System (SRS) Data Centers in Virginia and Illinois and initially three Nameserver Data Centers, co-located with the Enhanced SRS Data Centers and a standalone in California, that will provide the facilities and infrastructure to host the usTLD Registry. Our facility locations were selected to give wide geographic separation and provide resilience against natural and man-made disasters. The benefit to the DOC and the Internet community is reliable, non-stop usTLD registry, registrar, database, and information services operation.

NeuStar has developed a redundant facility implementation, high availability cluster server architectures, redundant database technology, and redundant alternate routed network connectivity that successfully supports mission-critical services today. The Internet community needs to be able to depend on the Internet as a stable, highly available infrastructure for worldwide collaboration and commerce.

In the subsection that follows, we describe where the NeuStar facilities are located and provide a functional description and physical description of the Enhanced Shared Registration System (SRS) data center and the nameserver sites. In subsequent subsections, we provide a more detailed system description of each of the systems residing within these facilities.

O.1.1 Registry Facilities Site Description

This section describes NeuStar's proposed usTLD Registry architecture consisting of redundant Enhanced SRS data centers and multiple nameserver sites to provide a seamless, responsive, and reliable registry service to registrars and Internet users. As shown in Exhibit O-1, our TLD registry redundant Enhanced SRS and nameserver data center sites are geographically dispersed and interconnected with a Virtual Private Network (VPN) to provide nationwide coverage and protect against natural and man-made disasters and other contingencies.

O.1.1.1 Enhanced Shared Registration System (SRS) Data Center Functional Description

High availability registry services can be provided only from facilities that have been designed and built specifically for such a critical operation. The NeuStar Enhanced SRS data centers incorporate redundant uninterruptible power supplies; high-capacity ventilation and climate control; fire suppression; physical security; firewalls with intrusion detection; redundant, high availability cluster technology; and redundant network and telecommunications architectures. When selecting the sites, we considered their inherent resistance to natural and man-made disasters. The functional block diagram of our Enhanced SRS data center is depicted in Exhibit O-2. As can be seen from this exhibit, the Enhanced SRS data center is highly redundant and designed for no single point of failure.

Each Enhanced SRS data center facility provides the functions listed in the system function directory table below. Descriptions of the Enhanced SRS systems providing these functions are provided in the next subsection.

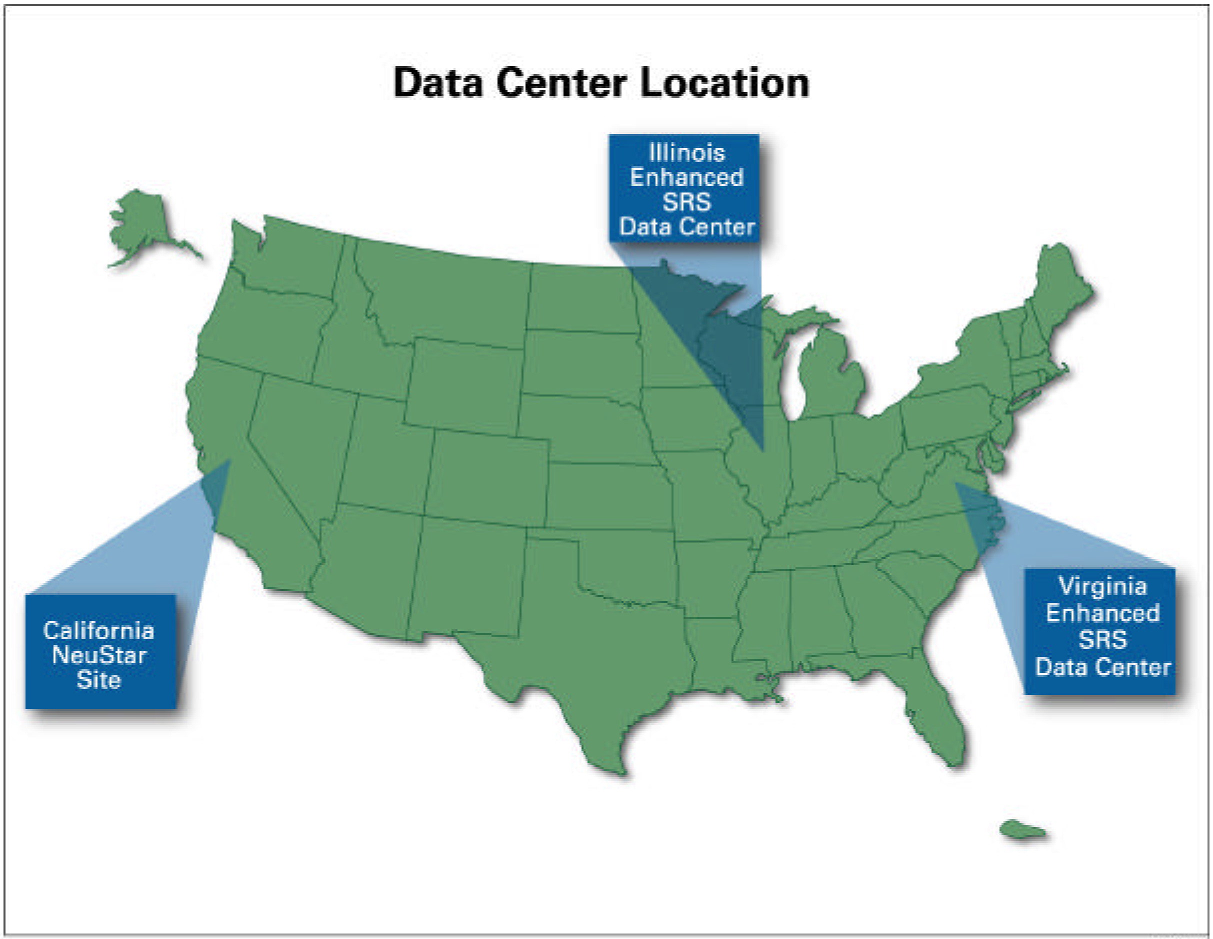

Data Center Location
Illinois Enhanced SRS Data Center
California NeuStar Site
Virginia Enhanced SRS Data Center

Exhibit O-1. *To enhance service availability and reduce the possibility of catastrophic failure, NeuStar will initially deploy three nameservers at sites in CA, VA, and IL. Two of the nameserver sites will be co-located with the co-active pair of Enhanced SRS Data Centers.*

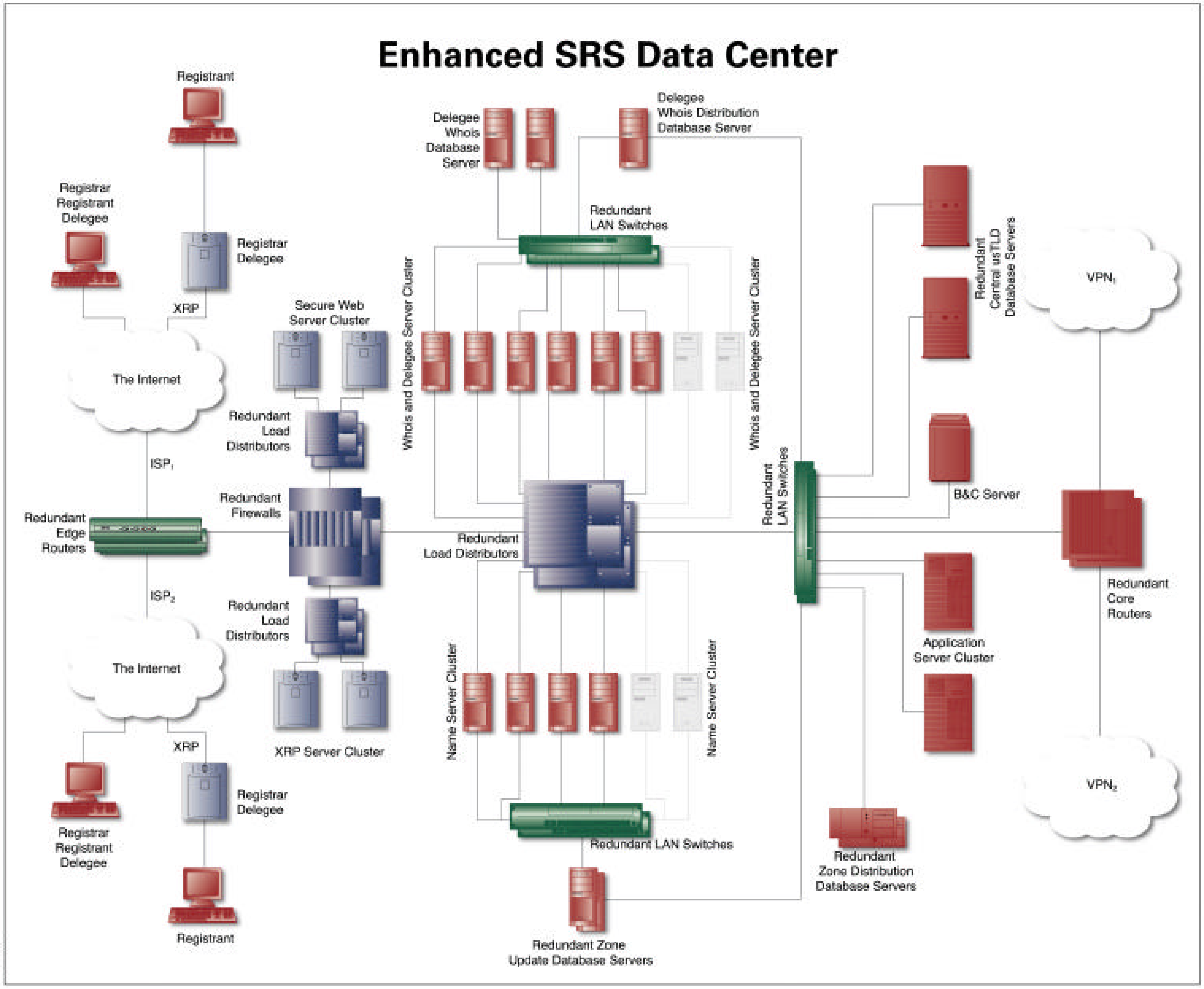

Enhanced SRS Data Center
Registrant
Registrar Registrant Delegee
Registrar Delegee
XRP
The Internet
ISP$_1$
Redundant Edge Routers
ISP$_2$
The Internet
XRP
Registrar Registrant Delegee
Registrar Delegee
Registrant
Secure Web Server Cluster
Redundant Load Distributors
Redundant Firewalls
Redundant Load Distributors
XRP Server Cluster
Delegee Whois Database Server
Delegee Whois Distribution Database Server
Redundant LAN Switches
Whois and Delegee Server Cluster
Whois and Delegee Server Cluster
Redundant Load Distributors
Name Server Cluster
Name Server Cluster
Redundant LAN Switches
Redundant Zone Update Database Servers
Redundant LAN Switches
Redundant Central usTLD Database Servers
B&C Server
Application Server Cluster
Redundant Zone Distribution Database Servers
VPN$_1$
Redundant Core Routers
VPN$_2$
006a.usTLD

Exhibit O-2. *NeuStar's Enhanced SRS data centers feature redundant network connectivity, high availability clusters, and replication to a second data center engineered to provide 99.95% availability and scalability.*

Enhanced Shared Registration System (SRS) Function Directory

System Function	Functional Description
Web Server	High capacity Web Servers provide secure Web services and information dissemination. It contains a registry home page to enable registrars to sign in and inquire about account status, get downloads and whitepapers, access frequently asked questions, obtain self help support, or submit a trouble ticket to the TLD Registry Help Desk.
Secure Web Provisioning Interface	High capacity web servers provide a secure interface for the delegated managers and registrants in the locality space to provision registration data. Delegated managers will be provided with authenticity information that they will need to input to access their account information. Registrants that utilize NeuStar as a registrar will be provided with similar authenticity information for their registrations. This is to ensure that only that registrant can modify the registration.
Protocol (XRP) Servers	XRP transactions received from registrars undergo front-end processing by the XRP server that manages the XRP session level dialog, performs session level security processing, and strips out transaction records. These XRP transaction records are sent to the Enhanced SRS data center application server cluster for security authentication and business logic processing.
Application Servers	Processing of the XRP applications business logic, user authentication, posting of inserts, deletes, updates to the master database, and interfaces to authentication, billing and collections, backup, and system/network administration.
Centralized usTLD Database Servers	The Centralized usTLD database maintains registry data in a multi-threaded, multi-session database for building data-driven publish and subscribe event notifications and replication to downstream data marts such as the Whois, Delegee, Zone, and Billing and Collection services.
Whois Distribution Database	The Whois Distribution Database is dynamically updated from the Centralized usTLD database and propagates the information to the Whois Database clusters.
Whois Database Clusters	The Whois Database is dynamically updated from the Whois Distribution Database and sits behind the Whois Server clusters. The Whois Database clusters are used to look up records that are not cached by the Whois Servers.
Whois Servers	The Load Balanced Whois Server Clusters receive a high volume of queries from Registrants and Internet users. The Whois service returns information about Registrars, domain names, nameservers, IP addresses, and the associated contacts.
Delegee Whois Distribution Database	The Delegee Distribution Database is dynamically updated from the Centralized usTLD database and propagates the information to the Delegee Database clusters.
Delegee Whois Database Clusters	The Delegee Database is dynamically updated from the Delegee Distribution Database and sits behind the Delegee Server clusters. The Delegee Database clusters are used to look up records that are not cached by the Delegee Servers.
Delegee Whois Servers	The Load Balanced Delegee Server Clusters receive a high volume of queries from Registrants and Internet users. The Delegee service returns information about Registrars, domain names, nameservers, IP addresses, and the associated contacts.
Zone Distribution Database	The Zone Distribution Database is dynamically updated from the registry Centralized usTLD database and propagated to the nameserver sites located worldwide. It contains domain names, their associated nameserver names, and the IP addresses for those nameservers.
Billing and Collection	A commercial off-the-shelf system is customized for registry specific eCommerce billing and collection functions that are integrated with XRP transaction processing, the master database and a secure Web server. The system maintains each registrar's account information by domain name and provides status reports on demand.
Authentication Services	Authentication Service uses commercial X.509 certificates and is used to authenticate the identity of entities interacting with the Enhanced SRS.
Backup Server	Provides backup and restore of each of the various cluster servers and database servers files and provides a shared robotic tape library facility for central backup and recovery.

Enhanced Shared Registration System (SRS) Function Directory

System Function	Functional Description
Systems/Network Management Console	Provides system administration and simple network management protocol (SNMP) monitoring of the network, LAN-based servers, cluster servers, network components, and key enterprise applications including the XRP, Web, Whois, Zone, Billing and Collections, Backup/Restore, and database application. Provides threshold and fault event notification and collects performance statistics.
Applications Administration Workstations	Provides client/server GUI for configuration of Enhanced SRS applications including XRP, Web, Billing and Collection, Database, Authentication, Whois, Zone, etc.
Building LAN	Provides dual redundant switched Gigabit Ethernet LAN-based connectivity for all network devices in the data center
Firewall	Protects the building LAN from the insecure Internet via a Firewall that provides policy-based IP filtering and network-based intrusion detection services to protect the system from Internet hacking and denial of service attacks.
Load Balancers	Dynamic Feedback Protocol (DFP) – based load balancing of TCP/IP traffic in a server cluster including common protocols such as least connections, weighted least connections, round robin, and weighted round robin.
Telecommunications Access	Dual-homed access links to Internet Service Providers (ISPs) and Virtual Private Network (VPN) services are used for connectivity to the Internet and the NeuStar Registry Management Network.
Central Help Desk	A single point of contact telephone and Internet-Web help desk provides multi-tier technical support to registrars on technical issues surrounding the Enhanced SRS.

O.1.1.2 Nameserver Sites Functional Description

As discussed above, two nameserver sites are co-located at our Enhanced SRS Data Centers and a third nameserver System site is geographically separated with dual-homed Internet and VPN local access telecommunications links to provide resilience and disaster recovery. The additional nameserver site will be installed in a Data Center in California. Additional nameserver sites will be introduced as demand warrants. Additional nameserver sites will be introduced as demand warrants. The functional block diagram of our nameserver sites is depicted in Exhibit O-3. As can be seen from the exhibit, the nameserver sites are configured to be remotely managed and operated “lights out.” The hardware configuration is highly redundant and designed for no single point of failure.

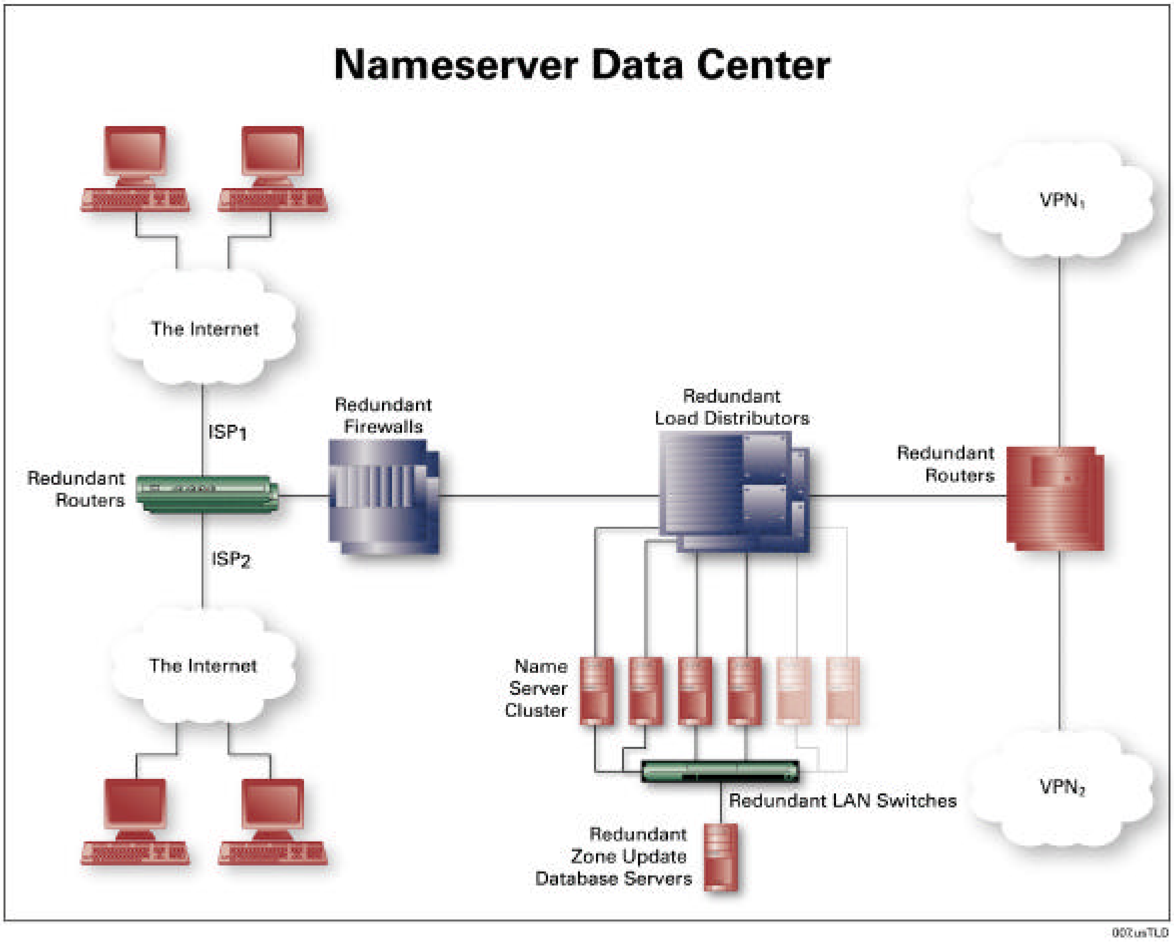


Exhibit O-3. *Redundant network components and high availability nameserver cluster provide scalable high availability.*

The following function directory table lists the nameserver functions. Descriptions of the systems providing these functions are provided in the next subsection.

Nameserver Function Directory

System Function	Functional Description
Zone Update Database	The Enhanced SRS Zone Distribution Database is propagated to the Zone Update Database Servers at the nameserver sites. Information propagated includes domain names, their associated nameserver names, and the IP addresses for those nameservers.
Nameserver	The nameserver handles resolution of usTLD domain names to their associated nameserver names and to the IP addresses of those nameservers. The nameservers are dynamically updated from the Zone Update Database. Updates are sent over the VPN Registry Management Network.
Building LAN	Provides dual redundant switched Gigabit Ethernet LAN-based connectivity for all network devices in the data center
Firewall	Protects the building LAN from the insecure Internet via a Firewall that provides policy-based IP filtering and network-based intrusion detection services to protect the system from Internet hacking and denial of service attacks.
Load Balancers	Dynamic Feedback Protocol (DFP) – based load balancing of TCP/IP traffic in a server

Nameserver Function Directory

System Function	Functional Description
	cluster including common protocols such as least connections, weighted least connections, round robin, and weighted round robin.
Telecommunications Access	Dual-homed access links to Internet Service Providers (ISPs) and Virtual Private Network (VPN) services are used for connectivity to the Internet and the NeuStar Registry Management Network.

O.1.1.3 Enhanced SRS Data Center and Nameserver Buildings

Each NeuStar data center facility is located in a modern, fire-resistant building that offers inherent structural protection from such natural and man-made disasters as hurricanes, earthquakes, and civil disorder. Sites are not located within a 100-year flood plain. Facilities are protected by a public fire department and have their internal fire-detection systems connected directly to the fire department.

Data centers are protected from fire by the sprinkler systems of the buildings that house them. Furthermore, each equipment room is protected by a pre-action fire-suppression system that uses Inergen gas as an extinguishing agent.

The environmental factors at the Enhanced SRS Data Center and nameserver sites are listed in the following table.

Environmental Factors at Enhanced SRS Data Center and Nameserver Sites

Ventilation and Climate Control	Dual redundant HVAC units control temperature and humidity. Either unit will maintain the required environment.
Lighting	2x2-foot ceiling-mounted fluorescent fixtures
Control of static electricity	All equipment-mounting racks are grounded to the building's system, and are equipped with grounding straps that employees wear whenever they work on the equipment.
Primary electrical power	208-volt, 700-amp service distributed through four power panels
Backup power supply	30 minutes of 130-KVA UPS power 1000-KVA generator (Enhanced SRS data center) 250-KVA generator (nameserver data center)
Grounding	All machines are powered by grounded electrical service A 12-gauge cable under the equipment-room floor connects all equipment racks to the building's electrical-grounding network

Building Security

In addition to providing physical security by protecting buildings with security guards, closed circuit TV surveillance video cameras, and intrusion detection systems, NeuStar vigilantly controls physical access to our facilities. Employees must present badges to gain entrance and must wear their badges at all times while in the facility. Visitors must sign in to gain entrance. If the purpose of their visit is found to be valid, they are issued a temporary badge; otherwise, they are denied entrance. At all times while they are in the facility, visitors must display their badges and must be escorted by a NeuStar employee. Sign-in books are maintained for a period of one year.

Security Personnel

On-site security personnel are on duty 24 hours a day, 7 days a week to monitor the images from closed-circuit television cameras placed strategically throughout the facilities. Security personnel are stationed at each building-access point throughout normal working hours; at all other times (6:30 p.m. to 6:30 a.m. and all day on weekends and major holidays), individuals must use the proper key cards to gain access to the buildings. Further, any room housing sensitive data or equipment is equipped with a self-closing door that can be opened only by individuals who activate a palm-print reader. Senior facility managers establish the rights of employees to access individual rooms and ensure that each reader is programmed to pass only authorized individuals. The palm readers compile and maintain a record of individuals who enter controlled rooms.

O.1.2 Enhanced Shared Registration System Descriptions

This section provides system descriptions of the NeuStar Enhanced SRS Data Center sites and the Nameserver Data Center. We provide brief system descriptions and block diagrams of each functional system within the two sites and their network connectivity. The NeuStar usTLD system architecture's central features are as follows:

- Co-active redundant data centers geographically dispersed (with two-way database replication between the centers) to provide mission critical service availability.
- Nameserver sites designed with full redundancy, automatic load distribution, and remote management for "lights out" operation.
- A Virtual Private Network provides a reliable, secure management network and dual-homed connectivity between the data centers and the nameserver sites.
- Each Enhanced SRS data center and nameserver site uses high availability cluster technology for flexibility, scalability, and high reliability.
- Registry systems sized initially to handle more than the expected initial workload can grow incrementally to accommodate workload beyond the initial implementation.
- The usTLD databases use redundant server architecture and are designed for continuous operation with synchronous replication between the primary and secondary databases.

NeuStar is proposing standard, mid-level, and high-end cluster server platforms for installation at each site. The servers are selected for applications depending on the requirements, storage capacity, throughput, interoperability, availability, and level of security. The generic server platform characteristics are summarized in the following table.

Server Platform Description

Platform	Features	Application
Standard Intel Server Clusters	Rack-mounted Intel 700 Mhz, 32-bit, 2- to 6-way SMP CPUs with 8 GB of ECC memory, CD ROM, four hot-swap disk drives (9-36 MB each), redundant hot swappable power supplies, dual attach 100 BaseT Ethernet Adapter, clustering and event management software for remote management. Red Hat Linux 6.1	• Nameserver Cluster • Whois Server Cluster • Backup Server • Network Management Server • Update Servers (Zone/Whois) • XRP Server • Web Server
Mid-level RISC Server Clusters	RISC 550 Mhz 2- to 8-way SMP, 64-bit CPUs, 32 GB ECC RAM, 72 GB internal disk capacity, 71 TB external RAID, redundant hot swappable power supplies, dual attach Gigabit Ethernet Adapter, clustering and event management software for remote management. Unix 64-bit operating system	• Application Server Cluster • Billing & Collection Server • Authentication Server • Whois Database Server
High-end RISC Server Cluster	RISC 550 MHz CPU, 64-bit 2- to 32-way cross-bar SMP with 8x8 non-blocking multi-ported crossbar, 32 GB ECC RAM, 240 MB/sec channel bandwidth, 288 GB Internal mass storage, up to 50 TB external RAID storage, redundant hot swappable power supplies, dual attach Gigabit Ethernet Adapter, clustering and event management software for remote management. Unix 64-bit operating system	Redundant Server for database system

O.1.2.1 Enhanced SRS Data Center System Descriptions

As previously shown in Exhibit O-2**,** the Enhanced SRS data centers provide co-active fully redundant system configurations with two-way replication over the high-speed VPN Registry Management Network, a co-located complete nameserver cluster, and dual-homed connectivity to the Internet Service Providers (ISPs). Descriptions of each of the systems in the Enhanced SRS Data Center site are as follows.

XRP Server Cluster

XRP transactions received from registrars over the Internet undergo front-end processing by the XRP Server which manages the XRP session level dialog, performs session level security processing, and strips out the transaction records. These XRP transaction records are sent to the Enhanced SRS data center application server cluster for security authentication and business logic processing. The XRP server is a rack-mounted Intel machine with local disk storage. It off-loads the front end processing of the XRP protocol and off-loads the extensive communication protocol processing, session management, and SSL security encryption/decryption from the applications servers. The XRP server strips the fields out of the XML document transaction and builds XRP binary transaction packets that are sent to the application server for initial security authentication and log-on with user ID and password. Once the user is authenticated, the session is active and the XRP application server performs all business logic processing, billing, collection, and database operations.

Nameserver

A complete nameserver cluster for DNS queries is co-located in each Enhanced SRS data center site. As previously shown in Exhibit O-3, the nameserver cluster consists of redundant ISP and Virtual Private Network (VPN) local access links to provide alternate routed connectivity to Internet users and NeuStar's Registry Management Network. Redundant Internet firewalls provide policy-based IP filtering to protect our internal building LAN from intruders and hackers.

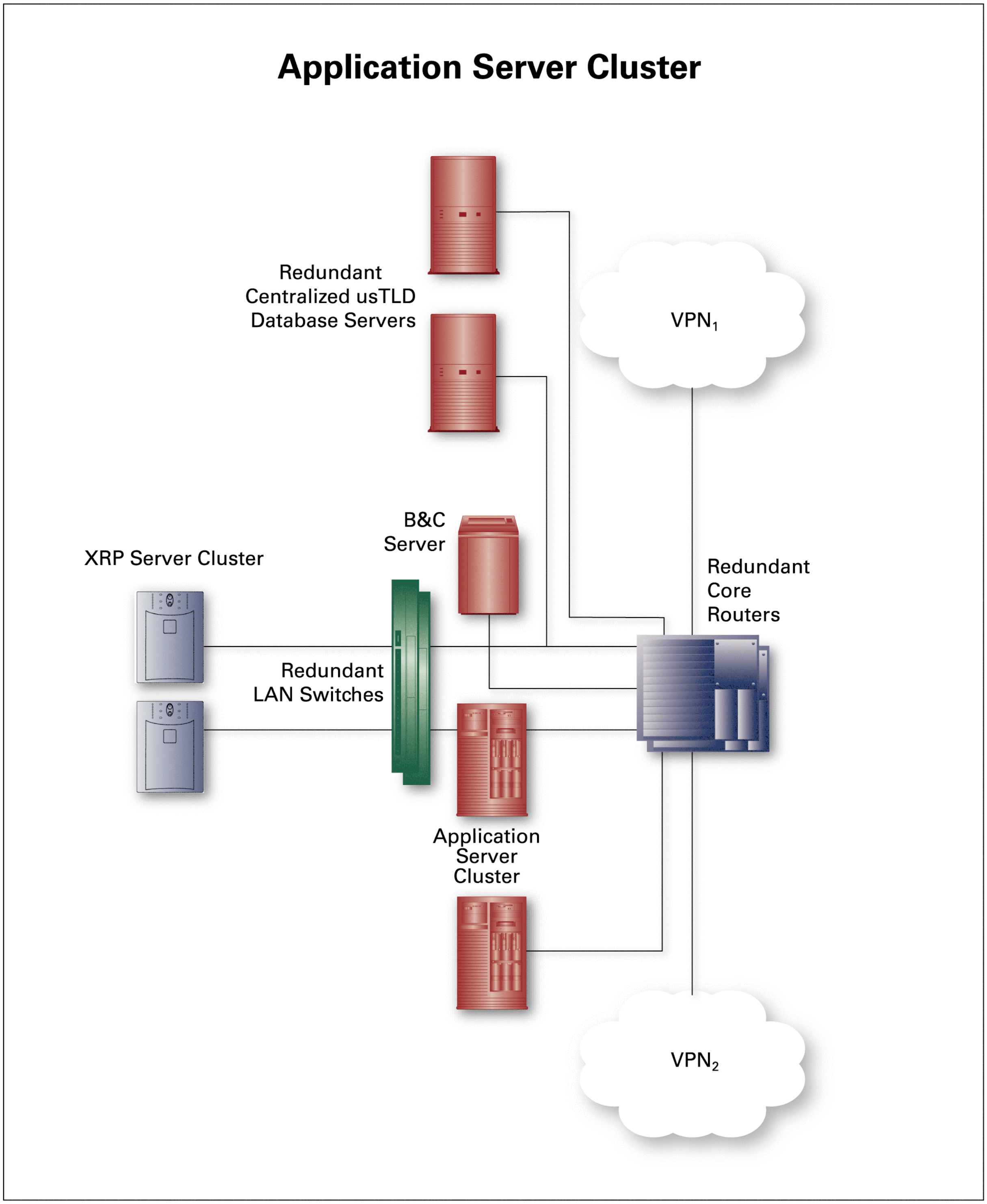
Application Server Cluster

The application server cluster is a high availability multiple computer cluster. Each computer within the cluster is a mid-level processor with its own CPU, RAID disk drives, and dual LAN connections. Processor nodes used in the clusters are RISC symmetric multiprocessor (SMP) architectures scalable in configurations from 2- to 8-way with the processing and storage capacity for very large applications. As depicted in Exhibit O-4, the application server cluster is designed to handle the registrar transaction workload and provides the business logic processing applications and interfaces to the authentication server, Centralized usTLD database, and billing and collection system. The application server cluster is front-ended with a TCP/IP load balancer to equitably distribute the processing load across the cluster processors. The cluster manager software monitors hardware and software components, detects failures, and responds by reallocating resources to support applications processing. The process of detecting a failure and restoring the application service is completely automatic—no operator intervention is needed.

Database Server

The database server consists of two identical redundant RISC systems that are designed for high-volume, online transaction-processing (OLTP) database applications. Each server contains high-end RISC processors scalable in configurations from 2- to 32-way SMP. A crossbar-based SMP memory subsystem is capable of supporting up to 32 GB of memory needed to maintain high OLTP transaction workloads. The storage subsystem supports up to 288 GB of internal RAID storage and up to 50 TB of external RAID storage. The database management software is based on a parallel database architecture with a redundant server option capable of maintaining 24 x 7 availability. The server supports high availability operations by implementing synchronous replication. The database enables transparent database failover without any changes to application code or the operating system. Clients connecting to a replicated database are automatically and transparently connected to the replicated pair of databases. The database replication feature makes it possible to maintain geographically separated data services for multiple sites over a WAN to provide disaster recovery.

A multi-session, multi-threaded server and dual cache architecture (client/server) provides exceptionally high throughput and fast access to stored objects. A powerful database-driven publish and subscribe event notification system enables applications such as Whois or Zone Distribution to subscribe to a specific Centralized usTLD database activity (e.g., a domain name insert). When the domain name insert occurs, an event is generated by the database to be handled as a dynamic update to the Whois and Zone distribution servers.


Application Server Cluster
Redundant Centralized usTLD Database Servers
VPN$_1$
B&C Server
XRP Server Cluster
Redundant Core Routers
Redundant LAN Switches
Application Server Cluster
VPN$_2$

008.usTLD

Exhibit O-4. *High Availability cluster provides scalable throughput to handle projected registrar, delegated manager, and registrant transaction workload.*

Whois Distribution Database

Certain Centralized usTLD Database events such as a domain name insert, domain name delete, or domain name change, generate a notification to subscriber databases such as the Whois Distribution Database. Modifications to the Whois Distribution Database are replicated to the Whois Database Clusters.

Whois Database

The Whois architecture gives the flexibility to deploy a Whois database to any number of NeuStar Data Centers. In the initial phase, the Whois infrastructure will be deployed to the two Enhanced SRS Data Centers. However, in the future, and based on load placed on the initial two Data Centers, additional infrastructure can be deployed to any of the nameserver Data Centers managed by NeuStar.

Each Whois Database receives replicated updates from the Whois Distribution Database. The initial Whois Database will consist of two mid-level RISC database servers configured in a high availability cluster with RAID storage and from 2- to 8-way SMP processors. Since data is cached in the Whois Servers, the Whois Database is hit only when a Whois Server has not cached a request in memory.

Whois Server Cluster

The Whois service is available to anyone and is engineered to handle large volumes of transactions per day. The cluster is a rack-mount Intel Pentium-based high availability multiple computer cluster that maintains a separate database for domain name registrations and caches commonly requested records. Processor nodes used in the Whois cluster are standard Intel Pentium SMP machines scalable in configurations from 2- to 6-way SMP with local disk storage.

The Whois database contains information about registrants, associated registrars/delegated manager, domain names, nameservers, IP addresses, and the contacts associated with them. This is an improvement over the current registry that provides no end-user contact information. The Whois server cluster is front-ended with a load balancer designed to distribute the load equitably to the servers in the cluster and handle extremely high volumes of queries. The load balancer tracks processor availability and maintains high query processing throughput.

Delegee Whois Distribution Database

Certain Centralized usTLD database events such as a delegation/sub-delegation insert, delegation/sub-delegation delete, or delegation/sub-delegation change, generate a notification to subscriber databases such as the Delegee Whois Distribution Database. Modifications to the Delegee Whois Distribution Database are replicated to the Delegee Whois Database Clusters.

Delegee Whois Database

The Delegee architecture gives the flexibility to deploy a Delegee Whois database to any number of NeuStar Data Centers. Initially, the Delegee infrastructure will be deployed to the two Enhanced SRS Data Centers. However, in the future, and based on load placed on the initial two Data Centers, additional infrastructure can be deployed to any of the nameserver Data Centers managed by NeuStar.

Each Delegee Whois Database receives replicated updates from the Delegee Whois Distribution Database. The initial Delegee Whois Database will consist of two mid-level RISC database servers configured in a high availability cluster with RAID storage and from 2- to 8-way SMP processors. Since data are cached in the Delegee Whois Servers, the Delegee Whois Database is hit only when a Delegee Whois Server has not cached a request in memory.

Delegee Whois Server Cluster

The Delegee Whois service is available to anyone. The cluster consists of rack-mount Intel Pentium-based high availability multiple computer cluster that maintains a separate database for domain name delegations and caches commonly requested records. Processor nodes used in the Delegee cluster are standard Intel Pentium SMP machines scalable in configurations from 2- to 6-way SMP with local disk storage.

The Delegee Whois database contains information about delegated managers, domain names, nameservers, IP addresses, and the contacts associated with them. The Delegee Whois server cluster is front-ended with a load balancer designed to distribute the load equitably to the servers in the cluster and handle extremely high volumes of queries. The load balancer tracks processor availability and maintains high query processing throughput.

Zone Distribution Database

The Zone Distribution Database is dynamically updated from the Centralized usTLD database using the same technique used for the Whois Distribution Database. The Zone Distribution Database is propagated to Zone Update Database at the nameserver sites using replication. This approach is far better than the current approach of TLD Zone File updates for .com, .net, and .org that occur two times per day.

Billing and Collection Server

The Billing and Collection server is a LAN-based mid-level RISC machine in configurations scalable from 2-to 8-way SMP with the processing and storage capacity for very large enterprise applications. This server runs a commercial off-the-shelf customer relationship management and billing and collection system that interfaces with the Centralized usTLD database.

Secure Web Server Cluster

A high-capacity secure Web Server cluster is provided to enable secure Web services and information dissemination. It contains a registry home page to enable registrars to sign in and inquire about account status, get downloads and white papers, access frequently asked questions, obtain self-help support, or submit a trouble ticket to the TLD Registry Help Desk. The Web Server is a rack-mounted Intel machine with local disk storage.

Authentication Server

The authentication server is a LAN-based mid-level RISC machine scalable in configurations from 2- to 8-way SMP with local RAID storage. This server runs commercial X.509 certificate-based authentication services and is used to authenticate the identity of registrars, delegated managers, and registrants, as well as NeuStar personnel. In addition, the authentication server supports our secure Web server portal for customer service functions.

Backup Server

The backup server is an Intel Pentium-based SMP server that runs the backup and restore software to backup or restore each of the various cluster servers and database servers and provide a shared robotic tape library facility. It interfaces to the Intel server clusters and RISC server clusters over a high-speed fiber channel bridge. It interfaces with the high-end redundant database servers via a disk array and the fiber channel bridge that interconnects to the robotic tape library. It is capable of performing remote system backup/restore of the nameservers over the VPN-based Registry Management Network.

System/Network Management Console

The system/network management console provides simple network management protocol (SNMP) monitoring of the network, LAN-based servers, cluster servers, and key enterprise applications including the XRP, Web, Whois, Zone, Billing and Collections, and database applications. The server is a LAN-based standard Intel Pentium-based SMP machine with local RAID disk storage and dual attached LAN interconnections.

Building LAN Backbone

The redundant switched Gigabit Ethernet building LAN backbone gives unprecedented network availability via redundant Gigabit Ethernet switches. Devices are dual attached to each of the gigabit switches to provide a redundant LAN architecture. The building LAN is protected from the insecure Internet via a firewall that provides IP filtering and network-based intrusion detection services to protect the system from Internet hacking and denial of service attacks.

Dual-Homed Telecommunications Access

We are using dual-homed high-speed Internet local access telecommunications links to two separate ISP providers. These links will be alternately routed to provide resilience against cable faults and loss of local access telecommunications links. Similarly, the telecommunications access links to our VPN provider for the Registry management network will be dual-homed and alternate routed.

O.1.2.2 Nameserver Description

Two nameserver sites are co-located at our Enhanced SRS Data Centers and the third nameserver cluster site is geographically separated, with dual-homed Internet and VPN local access telecommunications links to provide resilience and disaster recovery. The additional zone server clusters will be installed in California, Additional nameserver sites will be installed as demand warrants. The functional block diagram of our nameserver cluster is previously depicted in Exhibit O-3. As can be seen from the exhibit, the nameserver sites are configured to operate “lights out.” The hardware configuration is highly redundant and designed for no single point of failure and exceptionally high throughput. The following are the nameserver subsystem functions:

Zone Update Database

The Zone Distribution Database at the Enhanced SRS Data Center is propagated to the Zone Update Database using replication. Replication takes place over the VPN Registry Management Network. The Zone Update Database is not hit when resolving DNS queries; instead, the nameservers update their in-memory database from the Zone Update Database, within defined service levels.

Nameserver Cluster

The nameserver cluster handles resolution of usTLD domain names to their associated nameserver names and to the IP addresses of those nameservers. The resolution service can handle in excess of 500 million queries per day, and our load-balanced architecture allows additional servers to be added to any nameserver cluster to allow on-demand scalability.

The nameserver Cluster is a high availability rack-mounted multiple computer cluster consisting of standard Intel Pentium-based SMP machines configurable from 2- to 6-way SMP with local disk storage and dual attachment to the LAN. A TCP/IP server load balancer switch is used to distribute the load from Internet users. The server load balancer uses dynamic feedback protocol to enable servers to provide intelligent feedback to the load balancer to ensure that traffic is not routed to overutilized servers. The load balancer supports algorithms including least connections, weighted least connections, round-robin, and weighted round-robin.

Building LAN Backbone

A redundant switched Ethernet building LAN backbone maintains high network availability via redundant Ethernet switches. Devices are dual attached to each of the Ethernet switches to provide a redundant LAN architecture. The building LAN is protected from the insecure Internet via a firewall that provides IP filtering and network-based intrusion detection services to protect the system from Internet hacking and denial of service attacks.

A summary of the features and benefits of our usTLD system architecture is provided in the following table.

usTLD Registry

Feature	Benefit
Three classes of scalable processor configuration—standard, mid-level, and high-end	Provides flexible processing power and scalability to the applications
Direct Access Storage up to 50 Terabytes for database applications	Unmatched storage scalability of the database
Switched Gigabit Ethernet Redundant building LAN architecture	High capacity LAN infrastructure with no bottlenecks
Full Redundancy of all critical components with no single point of failure	Zero downtime and zero impact to users
Dual-homed, alternate routed local access links to two separate Internet Service Providers	Maintains connectivity if one of the ISP's services should experience and outage
Dual-homed, VPN connections to the VPN service provider	Protects against digging accidents that could damage local access cables
Redundant parallel database architecture configured for high OLTP transaction throughput	Non-stop database services and throughput scaled to handle all registry operations out of one data center.
Load balancing session distribution algorithm (SDA) to intelligently and transparently distribute traffic across servers	Maximize the number of Transmission Control Protocol/Internet Protocol (TCP/IP) connections managed by a server farm.
Separate Whois Server cluster and datamart to process Whois transactions	Facilitates rapid response to Whois queries.

O.1.3 Registry Network System Description

NeuStar is using the Internet to provide connectivity to the Registrars, Delegated Managers, and Registrants (where applicable) and a VPN to provide a secure Registry Management Network for communications between the Enhanced SRS data centers and the nameserver sites.

O.1.3.1 Internet Connectivity

NeuStar will deploy two 45-MB T-3 local access telecommunications links at each of our data centers, enabling each to provide TLD services independently of the other. We will provision 5 MBs of capacity on each of the T-3 links. Therefore, we will provision 10 MB into each nameserver site and have up to 90 MB (2 x 45 MB) of capacity for growth. This should be sufficient growth for at least two years.

Connectivity to each data center will be via redundant routers. For security purposes, the router will be configured to allow only DNS UDP/TCP and BGP4 packets. Each router is connected to a load balancer that distributes the query load among the nameservers in that site's cluster. These links will be alternately routed to provide resilience against cable faults and loss of local access telecommunications links. Similarly the telecommunications access links to our VPN provider for the Registry Management Network will be dual-homed and alternate routed. Redundant routers are used for both Internet and VPN access.

O.1.3.2 VPN Registry Management Network

Each Enhanced SRS Data Center is connected to each of the nameserver sites over a VPN. In addition there are two ATM links that connect the two Enhanced SRS Data Centers. Like the Internet access, the ATM links will be delivered over a T-3 local access link. Each link will be configured with some fraction of the full 45 MB of bandwidth. At the nameservers, the two VPN connections will be delivered over a 1.5 MB T-1 local access link. The bandwidth on each of the VPN circuits will be some fraction of the full 1.5 MB. The VPN Registry Management Network is a secure network used for NeuStar internal registry information exchange. It handles:

- Nameserver database replication from the Zone Distribution Database to the Zone Update Database at the nameserver sites,
- Remote system/network management/backup of the nameservers, and
- Remote administration of nameservers.

O.1.4 Registry System Application Software

Supporting existing delegees and registrants, as well as planning for the growth associated with domain registration and administration in the expanded usTLD space, requires vision and a flexible design. NeuStar's vision is to successfully conduct leading-edge software engineering and product development that will address the needs of each of the usTLD registry's sets of customers. NeuStar's proven record of successful development and implementation of large projects benefits the COTR by reducing technical and schedule risk.

NeuStar software components are developed using open system and software standards to facilitate cost-effective application expansion and upgrade. The functional design consists of a number of components representing a blend of:

- Proven software design and development methodology;

- Change management and deployment process; and
- Proven, mission-critical-grade, third-party software products to complement the NeuStar-built software components.

O.1.4.1 Application Components

The following components, illustrated in Exhibit O-5, deliver the Registry application functionality:

- Protocol adapters
- Application server component
  - Process manager
  - Processing engines
- Whois component
- Delegee Whois component
- Datastore
- Web server (presentation) component
- Billing and Collections component
- Nameserver component

Further information regarding these components is presented in the following paragraphs.

Protocol Adapter Component

The protocol adapter component is the software module running on the XRP protocol servers. This component provides the standards based interface between the Registry and the Registrar or Delegee systems. The XRP protocol will be based on open industry standards such as:

- **XML—**NeuStar proposes the introduction of a new standard protocol, the eXtensible Registry Protocol (XRP), based on XML. This protocol supports system level communication between the Registrar/Delegee and the Registry.
- **SSL—**X.509 Certificates will be used over an encrypted SSL session to authenticate Registrars/Delegees (in addition to IP-based and user ID/password security).

The protocol adapters will receive secure, encrypted data from Registrar/Delegee systems. They will convert the verbose external XML message into a compact binary internal message format, which is delivered to the application server's process manager for processing. When processing is complete, the process manager will send the binary internal message back to the protocol adapters for conversion to the protocol appropriate for communicating with the external system (i.e., XRP).

The protocol adaptor architecture allows NeuStar to support a simple but powerful XML-based protocol supporting a comprehensive security policy, while eliminating additional load that would otherwise be placed on the core Enhanced SRS system.

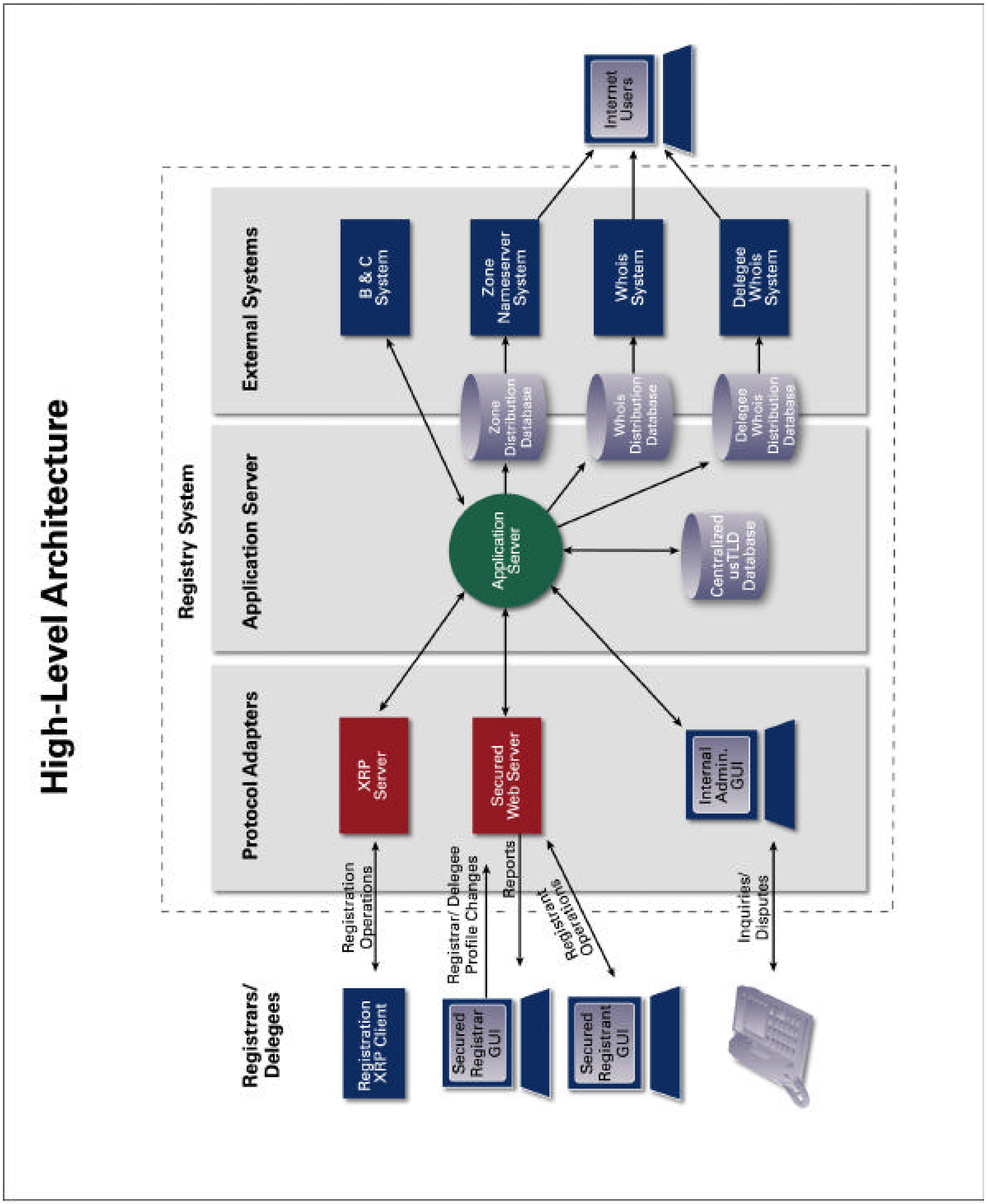


Exhibit O-5. *High-level architecture illustrates a high-level view of the Enhanced SRS and the interactions with external systems.*

Application Server Component

The design of the application server component is modular and flexible to support the requirements and scalable to meet demands placed on the system. The application server utilizes a stateless architecture that allows scalability simply by adding additional machines to the tier. The core business logic is built into the application server component. This component manages all back-end resources and performs services such as connection pooling and monitoring.

The process engines defined in this section are some of the major functional components of the system. Process engines will be added and configured to meet the functional requirements.

Process Manager—is used to manage the different processes supported by the application, including starting processes in a specific order at initialization time, monitoring the health of executing processes, restarting failed processes, and starting new processes to address application load requirements. The process manager mediates processing and information requests from external systems by forwarding requests to the respective process engines.

Process Engines—will perform the underlying processing steps or primitives that are involved in performing the operation. The process engines receive data and parameters from other application components, including the process manager. The process engines access data from databases and update the databases while processing a transaction. The primary process engines are:

- Domain Name Administration,
- Registrar/Registrant Administration,
- Whois Administration,
- Delegee Whois Administration,
- Zone Administration,
- Security,
- Billing and Grace-period Administration, and
- Logging, Auditing & Reporting.

The functionality of the primary process engines is explained in detail in Sections O.3 and O.6.

Whois Component

Whois-related modifications to the Centralized usTLD database cause equivalent changes to the subscribing Whois Distribution Database. Updates to the Distribution Database are replicated to the Whois Database Cluster at each Enhanced SRS Data Center. Machines in the Whois Server Cluster cache common requests in-memory, taking load off the Whois Database Cluster. Cached items expire after a defined time interval to ensure that Whois data can be guaranteed correct within defined service levels (see Section O.8 for a detailed description of the Whois capabilities). Exhibit O-6 provides a more detailed application architecture overview.

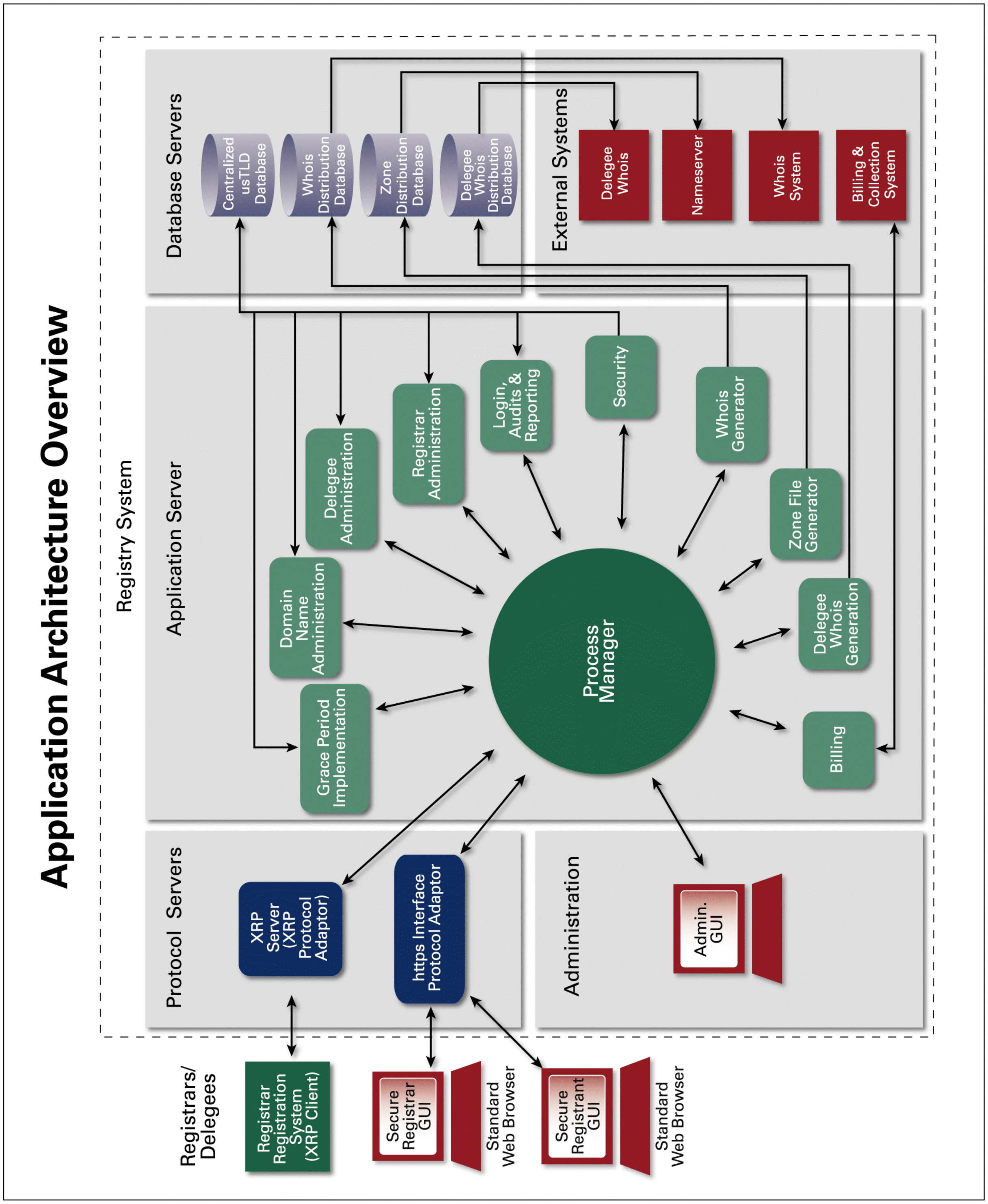


***Exhibit O-6.** The application architecture overview provides a high-level view of the registry processes necessary to support registry functionality and interactions with external systems and the Centralized usTLD database.*

Delegee Component

Delegee-related modifications to the Centralized usTLD database cause equivalent changes to the subscribing Delegee Whois Distribution Database. Updates to the Distribution Database are replicated to the Delegee Database Cluster at each Enhanced SRS Data Center. Machines in the Delegee Whois Server Cluster cache common requests in-memory, taking load off the Delegee Whois Database Cluster. Cached items expire after a defined time interval to ensure that Delegee data can be guaranteed correct within defined service levels (see Section O.9 for a detailed description of the Delegee capabilities). Exhibit O-6 provides a more detailed application architecture overview.

Datastore

The Enhanced SRS architecture includes a co-active databases supporting high availability operations by implementing synchronous replication. This enables transparent database failover without any changes to application code or the operating system. Clients connecting to a co-active database are automatically and transparently connected to the co-active pair of databases.

The architecture utilizes a powerful database-driven publish and subscribe event notification system that enables components such as Whois or Zone Distribution to subscribe to specific Enhanced SRS events. Subscribed events cause dynamic updates to the Whois and Zone distribution servers (see Section O.3 for a detailed description of the Database capabilities).

Web Server Component

NeuStar will provide usTLD Registry functionality via a Web-based, Internet-accessible interface. Expanded usTLD space registrars, as well as existing usTLD space delegees and registrants will all have the ability to access various registry/registrar functionality via a Web interface.

The guiding principles for the design of the proposed Web Server component are flexibility and security. The Web interface will be accessible over the Internet, using a client Web browser and will be served up by the Registry Web server clusters at the Enhanced SRS Data Centers. The secure Web servers provide front-end HTTPS (secure Web) protocol handling with client browsers accessible over the Internet.

Some of the key features of the Registry Web interface architecture include:

- Extensible design;
- Open, non-proprietary, standards-based technology (HTTP + SSL);
- Intuitive user interface;
- Secure access;
- Online help;
- Ease of navigation; and
- Data entry type checking (before forwarding requests to the application server tier).

Billing and Collection System

NeuStar will combine our customized B&C methodology that has proved successful in the past with an accounts receivable product to provide comprehensive, secured, high-quality, scalable, and Web-accessible B&C service. The major components of the system will include:

- Database,
- Transaction processor,
- Monitor and notifier, and
- Report generator.

See Section O.6 for a detailed description of the Billing and Collection system along with the interfaces, security, and access privileges.

Nameserver Component

Zone-related modifications to the Centralized usTLD database cause equivalent changes to the subscribing Zone Distribution Database. Updates to the Zone Distribution Database are replicated out to the Zone Update Databases at each nameserver Data Center. Machines in the nameserver cluster reconcile their in-memory database with the Zone Update Database at regular intervals defined in the service level agreement. The entirety of zone data is held memory resident.

Section O.5 explains nameserver architecture in detail, along with the process, software, and advantages.

O.1.4.2 Registry Software Development Methodology

The quick-time-to-market and software technologies required to design and implement the registry software applications dictate software development methodologies that minimize software development and reduce development time without sacrificing software quality. NeuStar's technical personnel are experts in software applications development of registry and clearinghouse protocols and software applications used in Internet domain names and phone number registry systems. NeuStar's experience will benefit the COTR by providing software products that meet the functional requirements and operate reliably.

On the basis of our experience, NeuStar is using Rapid Application Development (RAD) methodology and Computer-Aided Software Engineering (CASE) tools for registry software applications development. RAD methodology enables large applications systems to be developed and tested incrementally in planned releases consisting of alpha, beta, and full production versions. We have found that incremental development of software applications is a key success factor in fielding feature-rich software applications that meet business needs. This is because each incremental build provides a testable software product that can be demonstrated to users and stakeholders. Changes can be easily incorporated in the next build cycle, and each successive build provides increased functionality until the full production release is completed, tested, and accepted. NeuStar feels that this approach is ideally suited for allowing new software projects to quickly and fully benefit from our previously developed software applications.

RAD Methodology

In the RAD methodology there are five phases:

1. **Business Analysis—**Focus group and joint application design sessions are used to document the system requirements, business process flows, business logic, and system data requirements.
2. **System Design—**Software specifications are developed using object-oriented analysis and object-oriented design CASE tools, and logical data models are developed using entity relationship diagram data modeling. Meta data are developed for each data entity.
3. **Architecture Design—**The system hardware and software architecture is designed and documented. Then hardware and software systems specifications and configurations are developed and finalized for acquisition.
4. **Implementation—**The applications software is developed for the target hardware platforms and operating system environment using object-oriented programming languages, database development tools, and fourth-generation languages. Development test beds are built for software testing. The applications software is built and tested in increments, and the functionality grows with each build, from alpha to beta to full production. The system hardware and software are installed in the planned data centers for rollout and acceptance of the applications software production release. The Carnegie Mellon University Software Engineering Institute's Software Capability Maturity Model (SW-CMM) best practices are used for project management, requirements management, software configuration control, and software quality assurance.
5. **Growth and Maintenance—**During this phase, the applications software is successively upgraded in planned build and release cycles. Software incident reports are addressed in each build and release. Maintenance releases are developed for serious software problems that cannot wait until a planned upgrade release.

Development Tools and Languages

NeuStar is using object-oriented analysis and object-oriented design CASE tools for requirements analysis and detailed software design. We use object-oriented programming, database development tools, and fourth-generation programming languages for software development. The following table gives examples of tools NeuStar has used in the past and will use on the usTLD project.

usTLD Software Development Tools

Development Tool/Language	Purpose
CASE Tools	NeuStar will utilize CASE tools such as Oracle CASE and Rational Rose. These tools provide full feature object-oriented analysis and design.
Java, C++, Delphi, SQL	NeuStar has extensive experience with, and will utilize, these development languages where appropriate to implement all business logic.
CORBA, RMI	NeuStar has extensive experience with, and will utilize, these Remote object protocols.
Java Servlets, Java Server Pages, Cold Fusion, CGI-script, XML, and XSL	NeuStar has extensive experience with, and will utilize, these Web development technologies for building Web sites and thin client applications for distribution to a wide range of users.

O.2 Registry-Registrar Model and XRP Protocol

In the past, registry/registrar model and their associated protocol is a "thin" (limited amount of data) registry serving a "thick" (more data) registrar. NeuStar will deploy a "thick registry" model, with contact and authentication details stored centrally at the Registry. Under this model, the business relationships would be unchanged: registrants would still deal with the registrar, and the registrars would deal with the registry.

As part of its thick-registry proposal, NeuStar will deploy, the eXtensible Registry Protocol (XRP). The XRP protocol will accommodate both thin and thick registry models. We do not anticipate introducing the XRP protocol until after the initial "land rush" period has ended.

The XRP Protocol provides the following benefits:

- Extensible protocol based on XML,
- Utilizes BEEP as a transport protocol,
- Support for both thick and thin registry models,
- Support for centralized contact information/centralized Whois,
- Standardized Whois service (same fields regardless of registrar's Web site),
- Machine readable Whois format (when specified),
- Extensible data-field support (registrars can add custom fields to Whois following standardized fields),
- Functionally complete (exposing all registry data via one interface),
- Secure,
- Non-repudiation (no deniability),
- Redundant (duplicate requests have no adverse effect),
- Real-time XRP functions (e.g., check and register),
- Near Real-time DNS and Whois updates,
- Support for IPv6 addresses,
- Standard, centralized registrant authentication method,
- Extensible registrant authentication methods (e.g., support for digital certificates),
- Simple account transfer (between registrars, using centralized authentication),
- Event broadcasting (ability for registrars to place 'listeners' on registry events), and
- Rollback support (i.e., rollback registrar transfer; not necessarily transactional).

O.3 NeuStar's Database Capabilities

NeuStar will provide, redundant database system capable of managing large databases and high transaction processing loads reliably, with scalable growth to accommodate change.

The database system supports asynchronous replication of data between two co-active Enhanced SRS data centers geographically dispersed. The benefit to the Internet community is reliable, stable operations and scalable transaction processing throughput to accommodate Internet growth.

The heart of the Enhanced SRS is its database systems, which provide not only simple data storage and retrieval capabilities but also the following capabilities:

- **Persistence**—storage and random retrieval of data,
- **Concurrency**—ability to support multiple users simultaneously,
- **Distribution (data replication)**—maintenance of relationships across multiple databases,
- **Integrity**—methods to ensure data are not lost or corrupted (e.g., automatic two-phase commit, physical and logical log files, and roll-forward recovery),
- **Availability**—support for 24 x 7 x 365 operations (requires redundancy, fault tolerance, and on-line maintenance), and
- **Scalability**—unimpaired performance as the number of users, workload volume, or database size increases.

As applications architectures such as Enhanced SRS become increasingly dependent on distributed client/server communications and processing, system designers must carefully plan where the bulk of the data processing occurs: on the database server, applications server, or client. Our final design will distribute the processing workload in a way that maximizes scalability and minimizes downtime.

This proposal section (O.3) is divided into three major subsections:

O.3.1 Functional Overview—describes the characteristics of the three primary Centralized usTLD databases (i.e., size, throughput, and scalability); database procedures and functions for object creation, editing, and deleting; change notifications; transfer procedures; grace-period functions; and reporting.

O.3.2 Database System Description—describes the database system components, server platforms, and scalability for the three primary databases.

O.3.3 Security and Access Privileges—describes the access controls for granting and denying users and administrators access to the databases.

O.3.1 Functional Overview

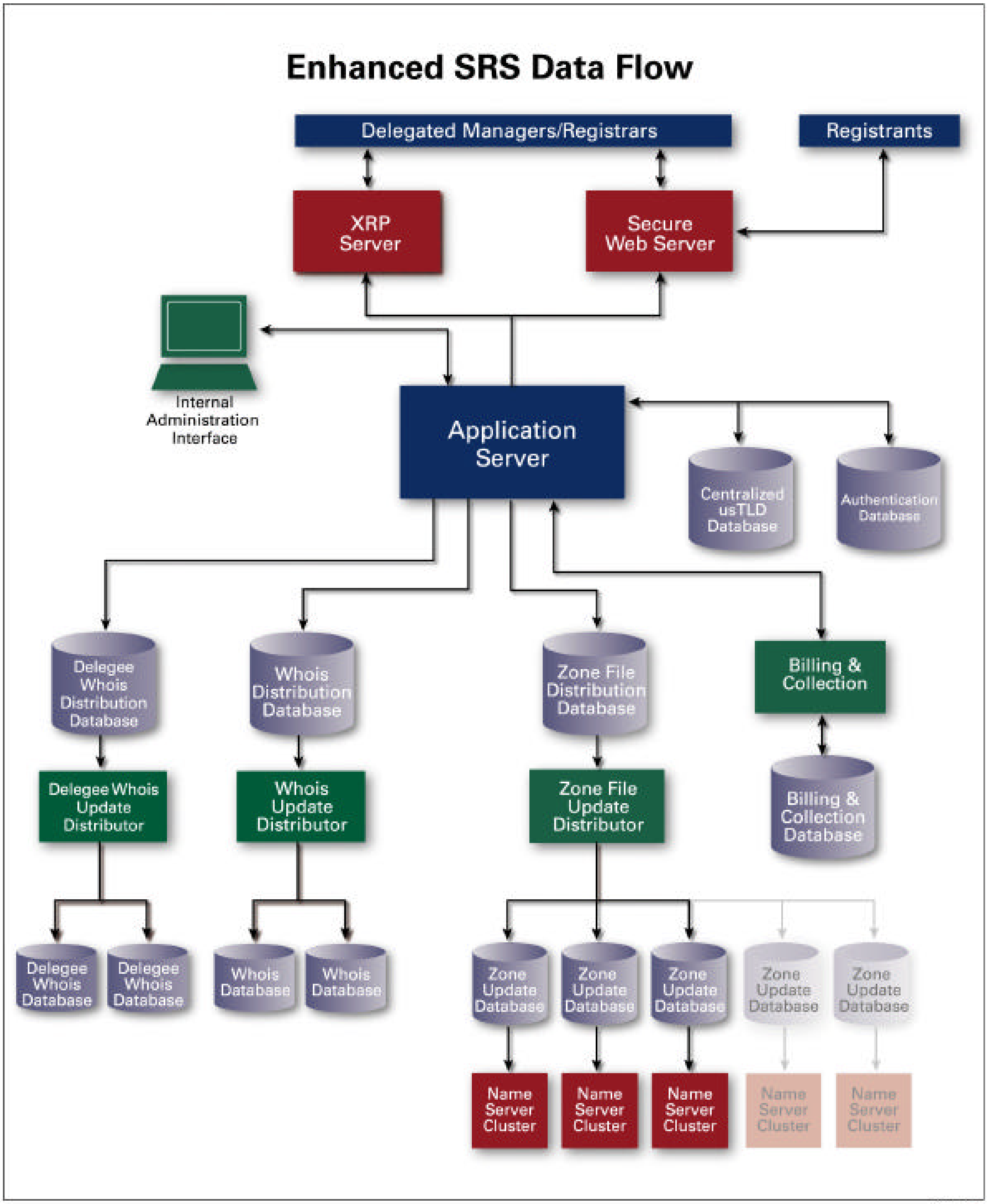
As shown in Exhibit O-7, NeuStar's registry will include four major databases:

- **Centralized usTLD Database—**The primary function of this database is to provide highly reliable persistent storage for all of the registry information required to provide domain registration services. The Centralized usTLD Database is highly secured, with access limited to authenticated registrars, trusted application server processes, and the registry's database administrators. The Centralized usTLD Database, includes registrant data, registrar data, delegee data and is used to create the Whois databases.
- **Billing and Collection Database—**This database will provide the information required for NeuStar to render billing and collection (B&C) services to the registrars, delegated managers, and registrants. Access to its data is limited to the trusted B&C system processes and to registry database administrators. Customers can view billing data through a secure Web portal with a B&C Applications Programmer Interface (API).
- **Whois Database—**The Whois database is a searchable database that any Internet user can access to view details pertaining to domain names. The Whois database maintains data about registrants, associated registrars/delegated managers, domain names, nameservers, IP addresses, and the associated contacts. The Whois database is updated from the Centralized usTLD Database through an intermediate database and replication process.
- **Delegee Database—**The delegee database maintains data about delegated managers, delegated subdomains, nameservers, IP addresses, and the associated contacts. The delegee Whois database is created from the delegee database and is a searchable database that any Internet user can access to view details of delegated subdomains stored in the Enhanced SRS.

In addition to these databases, the registry will maintain various internal databases to support operations such as authorizing login user ids and passwords, authenticating digital certificates, and maintaining access control lists.

In implementing the Centralized usTLD Database systems, our system designers will carefully analyze the differing requirements for the three major databases and select the optimum solution for each. Design techniques and considerations will include:

- Multiple logical data models that we will optimize for the different types of information that each system needs to serve registrars efficiently;
- Content that will include data related not only to domain names and domain name registration but also to registrars, registrants, nameservers, Whois servers, and the Billing and Collection system;
- Differing volumes of database transactions and database sizes;
- Differing business needs;
- Differing performance and availability requirements; and
- Replication of databases to achieve high availability and facilitate backup/recovery.



034.usTLD

Exhibit O-7. *Enhanced SRS Data Flow illustrates the data flow for processing requests and the data distribution to external systems.*

Database Size, Throughput, and Scalability

The following table lists design parameters for the initial design of the three major databases. The term *scalability* in the table refers to the database's ultimate capacity expressed as a multiple of the initial design capacity in terms of size and transaction processing power. NeuStar will closely monitor the overall performance and capacity of the database and will pro-actively make adjustments as required to keep the database performing at optimal levels. Given technological advances, there really is no practical limit to the overall capacity of the database.

Redacted

Redacted

Database Procedures and Functions

The database system is critical to the processing of Enhanced SRS business transactions. The Centralized usTLD database and B&C databases are accessed during many registry transactions. If a transaction is completed successfully, the system not only updates these two databases but also the Whois distribution, Delegee distribution and Zone distribution databases (as necessary). Below is a list of some of the functions performed by the Centralized usTLD Database and the Registry:

- Object Creation—Domain name, and nameserver registration.
- Object Editing—Modifying domain name, information delegee, or nameserver data and creating or modifying associations.
- Object Deletion—Domain name cancellations.
- Object Existence and Information Query—Obtain information on domain name, nameserver, or contact name.
- Object Transfer—Transfer a domain name to a different registrar.
- Automatic Domain/Subdomain Renewal—Extend a domain name registration for one year.
- Requested Domain Renewal—Process a renewal request.
- Grace Period Implementation—Allow various time periods before actions become final.
- Registrar/Delegee/Registrant Administration—Add, delete, or change to a usTLD Registry user account or billing profile.
- Billing Notifications—Account-related information sent to registrars, registrants, delegated managers, and designated registry staff.
- Reporting—Account and billing information that can be viewed online or e-mailed.

- Mass Updates—Special procedures (e.g., changing a registrar's name on each of its domain name files if it is acquired by another registrar, or changing a delegated manager's name on each of its delegated subdomains).

  A typical mass update is a global change of a registrar's name, which may occur when one registrar purchases another. NeuStar will design procedures for mass database changes initiated by registrars, delegees, or other authorized entities.

O.3.2 Database System Description

Although the four primary Centralized usTLD databases—Enhanced SRS, Whois, Delegee, and Billing—will differ, depending upon the services they support, the Enhanced SRS on the whole, will be structured to:

- Manage large quantities of data,
- Support applications that use data models with complex relationships,
- Perform complex operations on these objects, and
- Process large volumes of transactions from users.

NeuStar forecasts that, as with most OLTP applications, the anticipated volume of Enhanced SRS transactions will have a high ratio of "reads" to "writes." We will design the databases and applications by partitioning the workload to improve response times and scalability.

Centralized usTLD Database

The Centralized usTLD Database will support and provide information for primary domain registration services. The following table lists the data stored in the Centralized usTLD Database.

Centralized usTLD Database Data

Primary Element	Details
Domain Names	• Domain Name Attributes (Status) • Associated Name Servers • Associated Registrar • Associated Delegated Manager • Associated Registrant Data
Nameserver	• Nameserver Attributes (Status) • Associated IP Addresses • Associated Registrar • Associated Delegated Manager • Associated Registrant Data
IP Address	• IP Address Attributes (Status) • Associated Nameservers • Associated Registrar • Associated Delegated Manager • Associated Registrant Data
Registrar List	Registrar Names
Registrars	• Registrar Name

Centralized usTLD Database Data

Primary Element	Details
	• Registrar Contact Details • Registrar URL (Home page) • Registrar Whois URL (Web Port 80) • Registrar Whois URL (Port 43, if applicable) • Registrar Attributes (Status)
Delegated Manager List	Delegated Manager Names
Delegated Managers	• Delegated Manager Name • Delegated Manager Contact Details • Delegated Manager URL (Home page) • Delegated Manager Attributes (Status)

NeuStar will configure the database system to provide appropriate response times. We will plan capacity to ensure that as business requirements increase and demand for domain names grows, the system will be able to handle the workload within the agreed upon response times.

Centralized usTLD Database Platform

For the Centralized usTLD Database platform, NeuStar will use a business-critical-proven, high-performance, data center computing platform with the following characteristics:

- A high-end online transaction processing (OLTP) server,
- RISC 550 MHz CPU,
- 64-bit, 2- to 32-way cross-bar SMP,
- 8 x 8 non blocking multi-ported crossbar,
- Up to 32 GB of memory,
- Up to 19-GB I/O throughput,
- Maximum internal storage of 288 GB,
- Maximum external RAID storage of 50 TB,
- Redundant hot-swappable power supplies,
- Dual-attach Gigabit Ethernet Adapter, and
- Event management software for remote management.

The Centralized usTLD Database server will use the Unix 64-bit operating system with controlled-access security.

NeuStar will have vendor support agreements to keep the systems running and to repair or replace components immediately if problems occur.

Scalability

In planning for growth, NeuStar will design a database system with the ability to add resources on an as-needed basis without interrupting processing. Because database growth can occur in several areas, we will monitor each of the following parameters and plan for growth accordingly:

- **Physical size—**As the physical size of the database increases, so does the need for disk storage. Our database platform and database will support extending the internal storage capacity to 288 GB and the external capacity to 50 TB. The system will permit online configuration with minimum downtime.
- **Memory—**As the volume of users increases, so does the need for increased buffer and lock-pool storage. The database platform will scale up to 32 GB, which is sufficient memory for supporting the system capacity.
- **CPUs**—To handle increasing volumes of registrar requests, the database platform will scale up to 32 processors.

Billing Database

The Billing database provides information for Billing and Collections services, including:

- **Registrars' billing profiles—**accessed and modified by the Registrar Administration function;
- **Registrars' accounts—**queried, credited, and debited while processing transactions from registrars;
- **Registrants' billing profiles—**accessed and modified by the Registrant Administration function;
- **Registrants' accounts—**queried, credited, and debited while processing transactions from registrars; and
- **Catalogs—**Pricing information for different transactions; queried during the charging process.

Billing Database Platform

The Billing database platform will have the following characteristics:

- A high-end server;
- RISC 550 MHz CPU;
- 64-bit, 2- to 6-way SMP with up to 32 GB ECC RAM;
- Scalable up to 72 GB internal disk capacities and 71 TB external RAID;
- Redundant hot-swappable power supplies;
- Dual-attach Gigabit Ethernet Adapter; and
- Event management software for remote management.

The database server's operating system will be Unix 64-bit.

NeuStar will have vendor support agreements to keep the systems running and to repair or replace components immediately if problems occur.

Scalability

In planning for growth, NeuStar will design a database system with the ability to add resources on an as-needed basis without interrupting processing. Because database growth can occur in several areas, we will monitor each of the following parameters and plan for growth accordingly:

- **Physical Size**—The database and database platform can have their storage capacity extended and systems configured online with minimum downtime. The database platform will have the ability to scale up to 72 GB capacity, and external storage capacity up to 71 TB.
- **Memory**—As the volume of users increases, so does the need for increased buffer and lock-pool storage. The database platform will scale up to 32 GB, which is sufficient memory to support the system capacity.
- **CPUs**—To handle increasing volumes of registrar requests, the database platform will scale up to 6 processors.

Whois Database

Anyone can query the Whois database. Each database entity includes information on the following items for all Internet domain names registered in the usTLD:

- Domain name,
- Nameserver,
- IP address,
- Registrar/Delegated Manager, and
- Registrant contact information associated with the domain name.

Whois Database Platform

Each Whois server cluster will be supported by a clustered pair of database servers. The Whois database platform will have the following characteristics:

- A high-end server;
- RISC 550 MHz CPU;
- 64-bit, 2- to 6-way SMP;
- Up to 32 GB ECC RAM;
- Scalable to 72 GB internal disk capacity;
- Scalable to 71 TB external RAID;
- Redundant hot-swappable power supplies;
- Dual-attach Gigabit Ethernet Adapter; and
- Event management software for remote management.

The database server will use the Unix 64-bit operating system with.

Scalability

NeuStar will design the Whois database to grow with increasing demand over time. Because database growth can occur in several areas, we will monitor each of the following parameters and plan for growth accordingly:

- **Physical Size**—The database and database platform can have their storage capacity extended and system configured online with minimum downtime. The database platform will have the ability to scale up to 72 GB capacity, and external storage capacity to 71 TB.

- **Memory—**As the volume of users increases, so does the need for increased buffer and lock-pool storage. The database platform will scale up to 32 GB, sufficient memory to support the system capacity.
- **CPUs—**To handle increasing volumes of registrar requests, the database platform will scale up to 6 processors.

Delegee Database

Anyone can query the Delegee database. Each database entity includes the following information for all delegated subdomains registered in the usTLD:

- Subdomain name,
- Nameserver,
- IP address,
- Delegated manager, and
- End-user contact information associated with the subdomain.

Delegee Database Platform

Each Whois server cluster will be supported by a clustered pair of database servers. The Whois database platform will have the following characteristics:

- A high-end server;
- RISC 550 MHz CPU;
- 64-bit, 2- to 6-way SMP;
- Up to 32 GB ECC RAM;
- Scalable to 72 GB internal disk capacity;
- Scalable to 71 TB external RAID;
- Redundant hot-swappable power supplies;
- Dual-attach Gigabit Ethernet Adapter; and
- Event management software for remote management.

The database server will use the Unix 64-bit operating system.

Scalability

NeuStar will design the Whois database to grow with increasing demand over time. Because database growth can occur in several areas, we will monitor each of the following parameters and plan for growth accordingly:

- **Physical Size—**The database and database platform can have their storage capacity extended and system configured online with minimum downtime. The database platform will have ability to scale up to 72 GB capacity, and external storage capacity to 71 TB.
- **Memory—**As the volume of users increases, so does the need for increased buffer and lock-pool storage. The database platform will scale up to 32 GB, sufficient memory to support the system capacity.

- **CPUs—**To handle increasing volumes of registrar requests, the database platform will scale up to 6 processors.

Database Administration

NeuStar personnel who administer and maintain the database will perform their tasks at times and intervals scheduled to ensure maximum system availability. Typical database-administration tasks include the following:

- Monitoring and tuning,
- Creating and deleting entire databases,
- Starting and stopping,
- Backing up and recovering,
- Adding additional data volumes,
- Defining clustering strategies,
- Reorganizing,
- Adding and removing indexes,
- Evolving the schema,
- Granting access,
- Browsing and querying, and
- Configuring fault tolerance.

Database Backup/Restore

Proposal Paragraphs O.7 (Data Escrow and Backup) and O.14 (System Recovery Procedures) describe our proven backup/restore processes, which we will employ for the Enhanced SRS operation. Backup frequency and logging processes will minimize data loss in case of system outage.

Disaster Recovery

Each Centralized usTLD database component will asynchronously replicate its database in the other co-active Enhanced SRS Data Center. As Proposal Paragraphs O.7 (Data Escrow and Backup) and O.14 (System Recovery Procedures) explain, in the unlikely event of a catastrophic outage at one data center, the Enhanced SRS operations will failover to the replicate database.

O.3.3 Database Security and Access Privileges

Proposal Paragraph O.10 explains NeuStar's security measures in detail. The major technical security-related controls to ensure data integrity and security on the database platforms include the following:

- Server operating system with access control provides protection against unauthorized access. It employs user ID and password, along with file access control lists.
- Database security with user profiles enable us to grant or deny access privileges to customers, database users, and database administrators. The controllable level of granularity extends down to the individual data field.

- NeuStar will establish security policies and routine logging/auditing/monitoring functions to ensure that there is no unauthorized access. We will periodically review security to ensure that the system is functioning as needed.
- Access to the database is via trusted processes on both the application server and the Billing server.
- NeuStar will establish routine auditing/monitoring features to ensure that there is no unauthorized activity, and we will periodically review our security features to ensure that the system is functioning as needed.

O.4 Zone File Generation

NeuStar proposes generating zone files in near-real-time, thus ensuring timely synchronization of nameservers.

The zone file is a flat database file consisting of the technical information that the DNS requires to function correctly: the domain name, nameserver host name, and IP address.

Zone file generation is the term traditionally used to describe the process of generating a zone file from the registry database, deploying it to the primary root server, and then propagating it out to the secondary servers.

However, NeuStar's model does not periodically generate a zone file and then publish the new file to a set of nameservers. This Proposal describes our process for creating updates for the nameserver files; Section O.5 contains information about distributing and publishing the updates. To make the two sections complete and self-sufficient, each contains certain information that is also found in the other.

Benefits of the Proposed Solution

NeuStar's zone file generation and propagation processes will update zone files in near-real time within defined service levels. Near-real-time updates provide the following significant advantages:

- They eliminate the synchronization problems that now occur when information is modified.
- They enable us to define and monitor service levels for the maximum allowable time between zone file updates.

O.4.1 Secure Access to Update Zone File Data

Under our proposed solution, the Centralized usTLD Database in the Enhanced SRS data centers store all data used to generate and distribute the zone file updates. For security reasons, neither registrars nor internal data center staff can access this database directly; the application server tier controls all database access. Registrars/Delegees access the database (through the application servers) using the XRP protocol via the protocol servers. The following procedures govern creating and modifying database information:

- Registrars are solely responsible for creating, modifying, and deleting information that update the zone file. The XRP protocol is the only gateway available to registrars for zone file editing. This protocol is accessed using the NeuStar XRP servers.

- A registrar gains access to a domain name (and associated nameserver) by registering that domain name or when the appropriate Transfer of Registrar is enacted. For a Transfer of Registrar, access control is revoked from the losing registrar after the transfer.
- Access control to zone file data for XRP "Delete/Modify Domain Name" commands is granted only to the registrar/delegee who has management rights over the domain name.
- In the case of an XRP "Create/Modify/Delete Nameserver" command, access control is granted only to the registrar/delegee that has management rights over the nameserver's parent domain name (i.e., ns1.neustar.us has the parent domain name neustar.us).

Other proposal sections provide additional security-related information:

- Section O.5 contains information about deployment security, and
- Section O.10 contains information about other security issues, including system and network security and access control authentication and authorization.

Frequency of Zone File Generation

NeuStar will generate zone file updates (diffs) at regular intervals within defined service levels. Our solution enables us to meet any reasonable service level merely by adding incremental hardware items and reconfiguring system software settings.

Any zone file update procedure must not degrade the performance of the core registration system. NeuStar's solution will enable us to agree to service levels that guarantee the zone file distribution database is updated within defined intervals (initially set to 15 minutes) without adversely affecting core registration operations.

Logging and Data Backup

All zone files and updates are generated using information from the Centralized usTLD database. All updates are recorded as database transaction logs. Proposal Sections O.7, O.13, and O.14 contain information about the primary database backup and escrow systems, data center replication, and data recovery procedures.

O.4.2 Zone File Generation Architecture

Zone file information is stored in the Centralized usTLD Database (along with all other registry data) and replicated to a zone distribution server. The database stored on the zone distribution server is in turn replicated out to a database at the nameserver data centers.

Zone File Replication

Each time the zone distribution database is modified, and before the zone file update is replicated out to the nameserver data centers, the system performs a series of quality assurance checks. If any quality assurance checks raise an alert, operations staff must approve the deployment before the update is sent to the nameservers. The quality assurance checks include:

- Greater than a pre-established maximum number of modifications since the last update, and
- Greater than a pre-established maximum number of modifications since the last update for a special set of domain names used by key e-commerce sites. The alert threshold will be much lower for these domain names than for the previous check.

Standards Compliance

Each nameserver will run software that correctly implements the IETF standards for the DNS (RFC1035, RFC2181).

NeuStar expects to implement all applicable best-practice recommendations contained in RFC2870 (Root Nameserver Operational Requirements).

O.5 Zone File Distribution and Publication

NeuStar proposes near-real-time updates of the zone file data, which will facilitate synchronization of the nameservers as well as the monitoring of service levels.

This proposal section (O.5) describes the process of updating zone file information at the various nameserver data centers using information from the zone distribution servers at the two co-active Enhanced SRS data centers. The preceding proposal section (O.4) describes how the databases on those zone distribution servers are updated. To make the two sections complete and self-sufficient, each contains certain information that is also found in the other.

The databases on the zone distribution servers will be constantly replicated over a VPN to the zone update database at each nameserver data center. Each nameserver data center will, in turn, use its zone update database to update its zone file databases. Updating will comply with defined service levels.

To ensure availability and provide scalability and redundancy, each nameserver data center will have a cluster of two or more nameservers behind a load balancer. This configuration enables NeuStar to rapidly accommodate increases in query load by simply adding servers to the cluster at the affected nameserver data centers.

Benefits of the Proposed Solution

NeuStar's zone file generation and propagation processes will update the zone files in near real time within defined service levels. Near real-time updates provide the following significant advantages:

- They eliminate the synchronization problems that now occur when information is modified.
- They facilitate the deployment of innovative new technologies, such as dynamic update, because NeuStar will have technical control of the nameservers.

O.5.1 Locations of Data Centers Housing Zone File Nameservers

Exhibit O-1 (shown previously) provides the locations of the three nameservers. We will monitor network utilization and geographic traffic flows and will deploy new nameservers in additional geographic locations when appropriate.

At the nameserver data centers, a zone update database constantly receives replication update packages from the zone distribution database server at the Enhanced SRS data centers. This zone update database is not 'hit' when the nameservers process requests; the nameservers use it only to update their zone file databases.

NeuStar will deploy a modified version of BIND. It has been modified to remove capabilities not required for TLD root server operations and to speed up the remaining functions. The DNS software will comply with the latest IETF standards [RFC1035, RFC2181].

O.5.2 Zone File Publication/Update Architecture

As we introduced in Proposal Paragraph O.4, NeuStar proposes near-real-time update of the zone file. That paragraph discusses how the zone file information is stored in the Enhanced SRS master database and then replicated to a zone distribution server database.

Exhibit O-8 illustrates the zone file distribution process. The database on the zone distribution server at the Enhanced SRS data center is constantly replicated over our VPN to the zone update database at each nameserver data center. The update packages are compressed, encrypted, and sent with an appended checksum.

Every update package includes a checksum key, which is a generated checksum of the entire database up to and including modifications in that package. Each time a package updates a nameserver, the checksum is compared to the final state of the zone file data to ensure that the nameserver zone file corresponds to the zone file in the Enhanced SRS data center's database. If the checksums indicate an error, the nameserver asks the Enhanced SRS data center to replicate a full zone file to the nameserver. The update package replication process means that the full zone file should never need to be redeployed; however, NeuStar will provide this capability to recover from an unforeseen event. Should this capability be needed, propagating zone file updates may result in a 60-minute delay.

Exhibit O-9 depicts how each nameserver updates its zone file databases from its zone update database.

Frequency of Zone File Publication/Update

Any technical solution that includes real-time DNS updates must recognize that the most important function of the nameservers is responding to DNS queries. This requirement outweighs real-time updating of the zone file. NeuStar's solution is based on this reality. Our real-time update process includes establishing and monitoring key parameters.

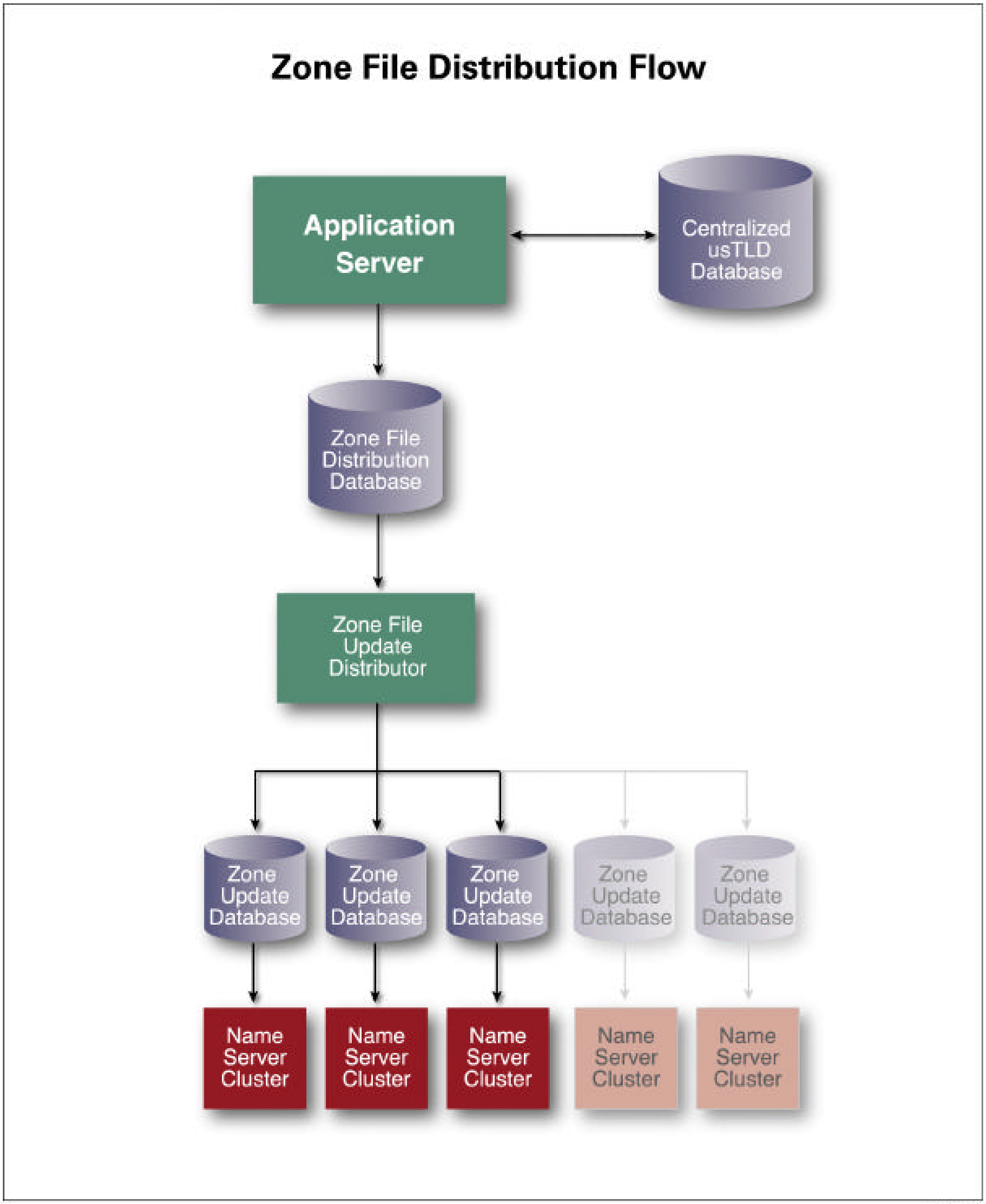
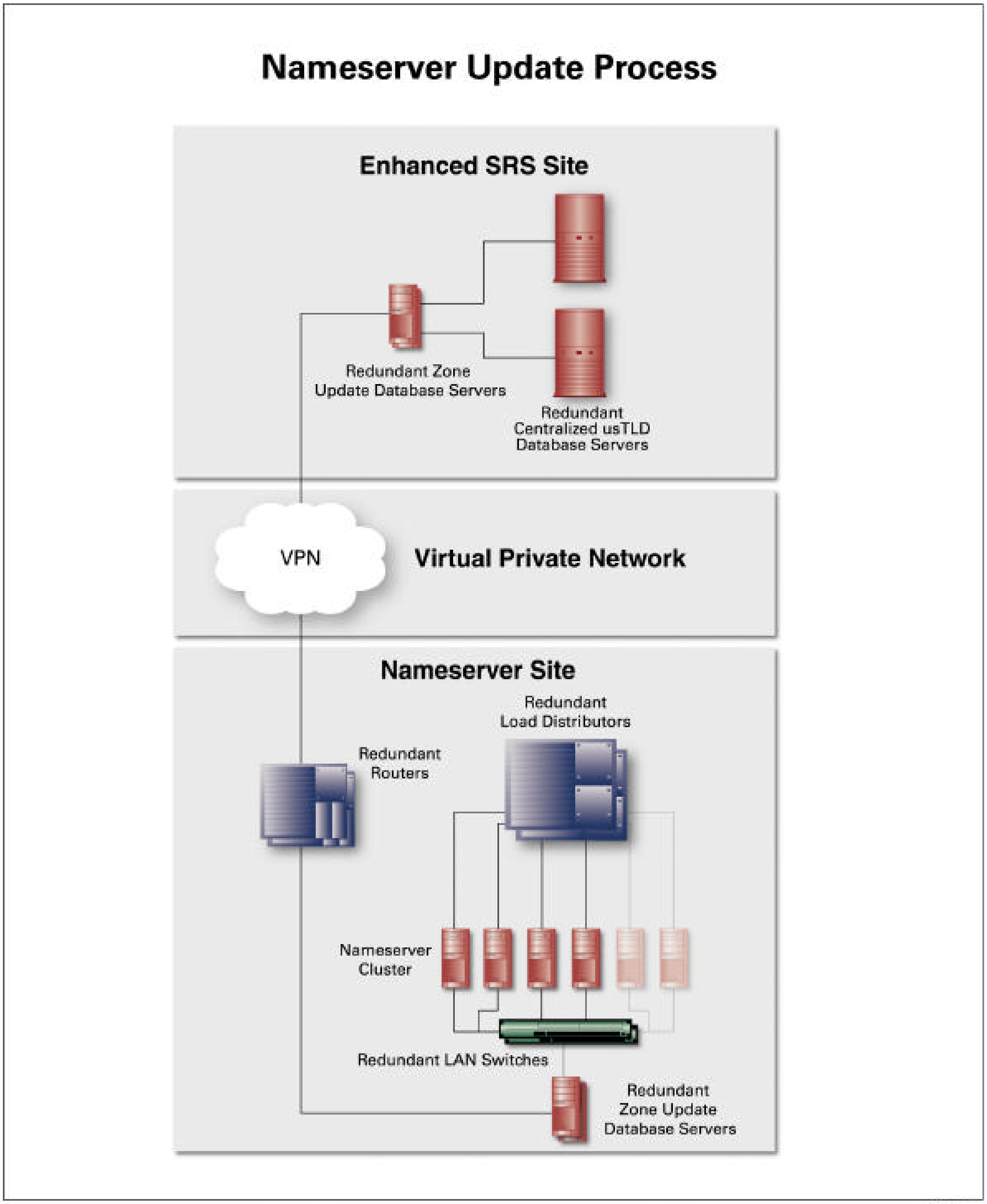


Exhibit O-8. *NeuStar's process for near real-time updating of the nameserver zone file databases ensures that consistent and timely data are always available.*


Nameserver Update Process
Enhanced SRS Site
Redundant Zone Update Database Servers
Redundant Centralized usTLD Database Servers
VPN
Virtual Private Network
Nameserver Site
Redundant Load Distributors
Redundant Routers
Nameserver Cluster
Redundant LAN Switches
Redundant Zone Update Database Servers

036.usTLD

***Exhibit O-9.** Maintaining a zone file database at each nameserver data center allows zone file servers to respond to DNS inquiries by accessing their own local zone file database. This maximizes efficiency and increases redundancy.*

Monitoring and Logging

Our central network management system will log all modifications to the Centralized usTLD database, all zone file update actions, and all attempts at intrusion or other security-related events.

Standards Compliance

Each nameserver will run software that correctly implements the IETF standards for the DNS (RFC1035, RFC2181).

NeuStar expects to implement all applicable best-practice recommendations contained in RFC2870 (Root Nameserver Operational Requirements).

O.6 Billing and Collection System

NeuStar's proven experience in successfully selecting, implementing, and operating complex Billing and Collection (B&C) systems for communications and domain name registry services ensures that our usTLD registry billing services will be feature rich, accurate, secure, and accessible to the entire customer base.

The B&C system will maintain customers' accounts, create account statements, and audit and track information for both customers and the industry.

The fundamental goal of the system is to maintain the B&C data and create reports that are accurate, accessible, secured, and scalable. B&C will enable detailed transaction-based charging to the customers, based on extensive resource accounting and usage data recording performed in the Registry System. The B&C system must produce timely and accurate account statements and billing reports that are accurate, easy to understand, and contain only clearly defined charges from the Catalog of services and prices. Such account statements are ultimately more economical because they are less likely to provoke costly billing disputes.

NeuStar offers a simple B&C process as depicted in Exhibit O-10. It is based on debit and/or credit card accounts established by each of our clients. We will withdraw all domain registration service payments from the incurring customer's debit or credit card account on a per-transaction basis. We will provide fee-incurring services (e.g., domain registrations, registrar transfers, and domain renewals) for customers only so long as their accounts are in good standing. NeuStar's B&C system will be sufficiently flexible to adapt to different billable events, grace-period implementations, and pricing structures.

NeuStar's B&C system will be located at the two redundant Enhanced SRS data centers in Virginia and Illinois. These systems will handle the key B&C functions, including:

- Debiting and crediting registrars' accounts,
- Initiating low-balance notifications,
- Performing credit card transactions,
- Enabling customers to view their accounts, and
- Tracking and reporting historical information.

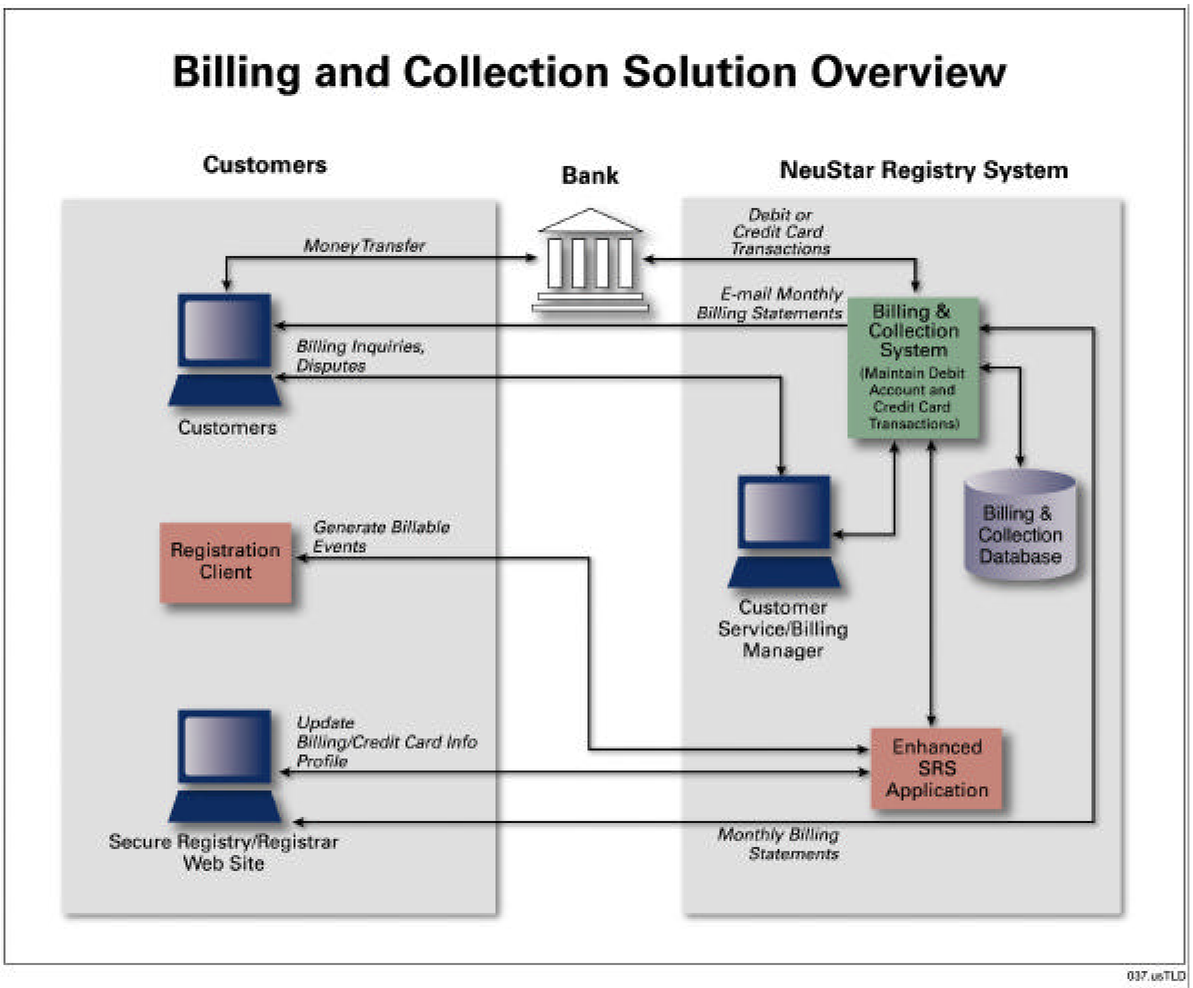

Billing and Collection Solution Overview
Customers
Bank
NeuStar Registry System
Money Transfer
Debit or Credit Card Transactions
E-mail Monthly Billing Statements
Billing & Collection System (Maintain Debit Account and Credit Card Transactions)
Billing Inquiries, Disputes
Customers
Billing & Collection Database
Generate Billable Events
Registration Client
Customer Service/Billing Manager
Update Billing/Credit Card Info Profile
Enhanced SRS Application
Secure Registry/Registrar Web Site
Monthly Billing Statements
037.usTLD

***Exhibit O-10** NeuStar's billing and collection solution will ensure that all usTLD billing and collection requirements are met with the highest level of service.*

O.6.1 Technical Capabilities and Characteristics

NeuStar will customize an off-the-shelf product to ensure data processing accuracy, accessibility, flexibility, and scalability to accommodate increasing transaction volumes and additional billable events. Our finance and technical experts are experienced in customizing systems to evolve smoothly from performing simple to more complex tasks, and from small-scale to large-scale operations. We selected this solution after conducting a detailed analysis of the options for administering the registry's B&C system. Our proposed system will:

- Meet all registry B&C objectives, including
  - Generating the large amount of detailed resource accounting information needed to support detailed usage-based charging of registrars, delegees, and registrants
  - Tracking and reporting historical information
- Be cost effective
- Be operational within the scheduled implementation dates.

Billing and Collection System Description

Exhibit O-11 illustrates the major components of the B&C system and its interfaces with other Enhanced SRS subsystems.

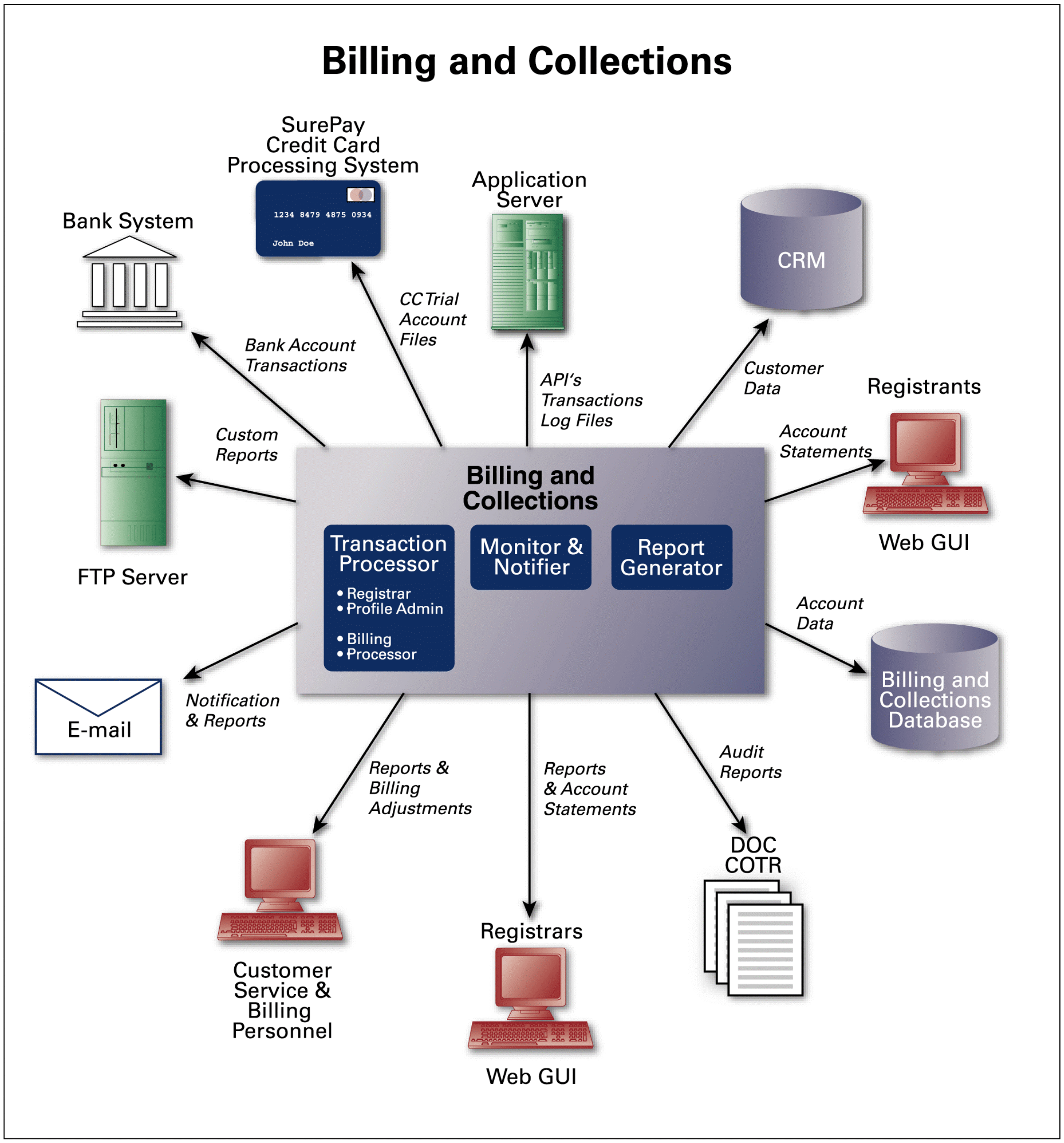
B&C database—This database, which is separate from the Registry's Centralized usTLD Database, contains the data shown in the following table. Proposal Paragraph O.3 discusses the capabilities, management, administration, and backup of all databases, including the B&C database. This subsection discusses only the design aspects of the B&C database.

Transaction Processor—This processor, which responds to inputs from the external application server and from the B&C operations GUI, is the only component that has access to update the B&C database. The transaction processor will process transactions in real time, responding to API calls from application servers, and also will process transaction log files obtained from external servers. The transaction processor has two main subcomponents:

- **Customer Profile Administrator—**The component that responds to the customer-administration component of the application server, and
- **B&C Processor—**The component that processes all domain registration related requests and other billable events from external servers.

B&C Database Contents

Primary Element	Details	Primary Element	Details
Catalog	• Transaction type • Amount charged • Start date • End date • Additional information	Transaction data	• Transaction ID • Customer ID • Transaction type • Start date • End date • Domain name • Registrant contact information
Customer Information	• Customer name • Customer ID • Customer e-mail address • Customer address	Account history	• Customer ID • Amount received • Date of amount received • Transaction type
	• Preferred payment method • Credit card information	Account Information	• Customer ID • Current Amount
	• Account setup date • Operational date • End date	User Administration	• User ID • User role



038.usTLD

Exhibit O-11. *The application architectural overview provides a high-level view of the billing and collection system necessary to support registry functionality and its interactions with external systems.*

Monitor and Notifier—This component monitors the registrars' accounts for sufficient funds and monitors domain name expirations and renewals. When it detects actionable items, it notifies the transaction processor and the registry's Customer Service organization.

Report Generator—This component will generate monthly account statements and various reports, including annual reports. This is also the component that Customer Service will use to generate custom reports requested by a customer. After generating custom reports in a batch process, the report generator sends them to the FTP directory, where they are stored for the customer to download.

Billing and Collection System Interfaces

As Exhibit O-11 above indicates, the B&C system will have four types of interfaces:

Application Programmer Interfaces (APIs)—That connect billing functionality with selected non-B&C functions of the registry (e.g., registrar administration, domain registration, accounting system entries, and e-mail processes). The APIs, which connect to the application server, will provide good query capabilities, triggers for billable events, and a means for customizing or extending B&C functionality. The APIs will enable the B&C system to perform B&C functions in near real time (i.e., at the same time that the registry system is processing the request). The APIs will be well defined, including parameters used and resultant status codes. All error codes will be well documented, and B&C activities will be logged for tracking and audit purposes. API functions include the following:

- Validating the application using application ID & password,
- Accessing a customer's account to verify its balance and perform a financial transaction (credit card or debit account),
- Adding a domain registration,
- Canceling a domain registration,
- Transferring a domain registration,
- Requesting a custom report, and
- Administering a customer's billing profile.

GUI Client—For the B&C system's registry operations personnel, who will use this interface for system administration and reporting functions, including:

- Establishing and administering customer accounts;
- Administering B&C functionality, including making adjustments; and
- Generating routine and special reports.

Secure Web-based Portal—That enables customers to use readily available Web browsers (Netscape Navigator 4.0 or above, or Microsoft Internet Explorer 4.0 or above) to monitor their account balances and view reports over the Internet. Using this interface, customers can view the balance in their debit accounts, their credit card transactions, and their domain registration records in detail. Customers are granted permissions via the database security features to access data pertaining to their own accounts, but they cannot access data from other customers' accounts. Customers also are able to select the interface by which the query or report will be delivered; depending upon the type of report or query, the available interfaces can include on-screen, FTP, or e-mail. The interface will be by way of a secure network using the Enhanced SRS Web server, HTML, and an off-the-shelf reporting tool. Features of the Web GUI include:

- Open, non-proprietary, standards-based GUI technology (http + SSL);
- Economical, readily available client software for users;
- Secure access;
- Flexible design;
- Online help;
- Consistent presentation style;
- Ease of navigation, with menu-type options; and
- Data entry checking.

Transaction Log Files—Are automatically created by and transferred from external systems such as the application server and database systems.

Billing and Collection Procedures

The B&C system processes data that are generated during the following three types of procedures:

- Customer administration—The B&C system will manage the B&C profile for customers, along with the account and contact information.
- Transactional services—Actions that trigger a B&C event. Customers' requests result in "transactions" at the application level and "events" in the B&C process.
- Non-transactional services—Actions including balance forecasting and account balances.

The following tables provide details of each type of process flow. Where they state that the B&C system sends a special notification to a customer, it also sends a copy to the usTLD Customer Service organization.

Registrar Administration

Function	Billing and Collection Process Flow
Initial Account Setup	Registry receives the registrar's Registry Service Agreement and the license fee. Registry establishes an account in the B&C system, enters all contact information, but account status is non-operational.
Operational Account Setup	Registry verifies registrar's acceptability and invoices for the annual maintenance fee. Registry receives maintenance fee payment and changes account status to operational. Registry notifies registrar to prepay the established debit account or collects credit card information
Debit Account Prepayment	Registry receives customer's payment, opens debit account, and credits received amount to that account.
Change in B&C Profile	Registry receives the request. If registry approves, it updates customer's B&C profile in B&C system.
Credit Extension	Registry receives the request.

	If registry approves, B&C system extends the credit.
Change in Payment Methods	Registry receives the request. If registry approves request, B&C system records the change.

The following are the transactional services recognized by the B&C system:

- Add Domain,
- Cancel Domain,
- Renew Domain (Customer Request),
- Renew Domain (Automatic),
- Cancel after Automatic Renew (Customer Request),
- Transfer Registrar,
- Mass Updates, and
- Custom Reports.

The following are the non-transactional services recognized by the B&C system:

- Annual Maintenance Fee,
- Low Account Balance,
- Insufficient Funds,
- Balance Forecasting,
- Account replenishment,
- Credit card transaction failure,
- Monthly Statements, and
- Online B&C Reports.

O.6.2 Security

Proposal Paragraph O.10 provides extensive details about security issues, such as system, network, and physical security and specific issues, such as access control, authentication, and authorization. This subsection discusses only security provisions that are specific to B&C. Like the overall registry system, the B&C system will implement security at the Network, System, and User levels, as follows:

Network-level Security—The primary network-level communications technology underlying the B&C system is the IP protocol. The only interfaces that have access to the B&C system are the secure Web GUI to monitor account status and the FTP server to download reports. A firewall forms the secure interface between our secure internal network and the untrusted Internet. Firewalls use filters to permit or deny packet flow on the basis of the origin and/or destination of the packet's addresses and ports.

Users who want to obtain access to the secure Web portal that we provide to the registrars must first obtain access to the secure Web server within the Enhanced SRS. When the user's Web browser attempts to establish an https (secure Web application protocol) session with the registry, our system initiates the SSL (secure sockets layer). Part of the initialization sequence is a public key exchange or identification. Once the SSL initialization is complete, it establishes a secure, encrypted channel between the user's Web browser and the registry's Web server, and exchanges digital certificates to ensure the integrity and authenticity of the session. The use of a secure Web browser/server ensures that no clear text, including passwords, is sent over the public or shared data network.

System-level Security—Secure user login facilities ensure that secure Web server users are fully authorized and authenticated. The Enhanced SRS secure Web server presents a login menu on the user's Web browser. The login menu includes 20 lines of warning message stating that this is a private computer system and authorization is required for access. The default warning message will be: "NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution!"

When users attempt to log in to the secure Web server, they must enter their user ID and their password. The login/password information forwarded back to NeuStar's usTLD Web server is encrypted through the SSL channel previously established.

User-level Security—Every B&C system user (individual and application, external and internal) has a unique user login account on the system, with unique user identification codes (user IDs) and passwords to authenticate users and an access control list to control their access to system resources and applications. User profiles are set up and maintained in the database system so that users' access to the B&C system is controlled by their user profile and the access privileges granted therein. NeuStar will establish and maintain well-defined security procedures for adding and deleting users and modifying their logon account, access control lists, and user profile access privileges, depending on the user's functional role. The following subsection contains additional information about user roles and privileges.

O.6.3 Access Privileges

The B&C system and network employ multi-tiered access control to ensure that all B&C resources—such as transactions and data—can be accessed and used only by authorized users. As previously discussed, access to the proposed B&C system via the network is fully secured behind a perimeter firewall and user ID and password system, while physical access is controlled using electronic keys and palm readers. Once authorized users gain access to the system, their privileges are controled by the operating system access control lists and the database system user profile that determines what functions, system resources, and data the users are allowed to access and use. Access privileges are broadly defined and controlled for the following user groups:

- Registry employees, and
- usTLD customers.

The following subparagraphs discuss the access privileges of each group.

Registry Employees

Only internal usTLD registry staff members using cardkeys can gain access to the registry facility. Registry employees who are authorized to access the B&C system do so using workstations connected through the registry LAN. Except for the system administrators, these employees access the system using the B&C client interface, which will be established specifically for staff members to perform billing adjustments, maintenance, and related functions.

Each internal user of the B&C system is also associated with a user role that will permit or deny access to different functions in the B&C system. The System Administrator will create the roles that allow users to access certain functionality. Initially, we expect to define user roles within NeuStar's B&C-operations organization as follows:

- System Administrators perform system upgrades, maintenance, and user administration.
- B&C System Administrator configures the B&C system (e.g., user groups and their access rights, batch-process schedule, and configurable business rules).
- B&C System Operator establishes users, monitors back processes, provides system support, and monitors and corrects billing errors.
- Customer Service personnel view a registrar's billing history and collect information for the B&C manager.
- B&C clerks create transactions, such as invoices and collections, but do not make adjustments.
- B&C Manager creates adjustments, catalog changes, and customer changes.
- B&C Database Administrator performs mass database updates.

Customers

Customers have only view access to their B&C account status, account statements, and reports. They have to contact B&C personnel within the registry's Customer Support organization for any billing adjustments, custom reports, or special arrangements.

Query Capabilities—The Web GUI will provide authorized registrars with the ability to query the B&C database for information. As previously described, to access the Web GUI, the registrar must obtain network access to the registry Web server and then proceed through the identification and authentication process using a valid logon ID and password. A registrar's access to the B&C information is limited to his own accounts; the registrar is denied access to the information about any other registrar's account. The Web GUI supports the following standard queries and reports:

- List of all domain names owned by the customer,
- Account balance,
- Monthly account statements,
- List of all domain names with renewal dates within a defined period, and
- Detail transaction report for defined period.

Customers can submit nonstandard queries or requests for special reports by contacting NeuStar's Customer Service organization via e-mail, phone, or fax. Customer Service will place any custom reports on a secure FTP server from which the requesting customer can download them.

Adjustments—For billing issues or adjustments in profile or account statements, customers must contact NeuStar's Customer Service organization via e-mail, phone call, or fax. The B&C Manager has the capability to perform any billing adjustments or similar services requested by a customer.

Notifications and Statements—The registry will e-mail to each customer a detailed monthly transaction statement, an account summary, and a detailed list of all fee-incurring charges. In addition, the B&C system will automatically e-mail "Low Account Balance," "Insufficient Funds," and "Credit Card Transaction Refusal" notifications to any customer when needed.

O.6.4 Backup and Recovery

We will employ the same backup and recovery procedures for the B&C system that we use for the overall registry system. Proposal Paragraph O.7 provides detail on the following procedures:

- We will perform daily backup to DLT tapes, which will be stored in a secure off-site location.
- We will also perform periodic archives of history files and data, which we will also store in a secure off-site location.

If the B&C system fails (i.e., the API interface to the application returns an "Error status"), a built-in recovery mechanism will ensure that transactions and data are not lost. The application server will log all undeliverable B&C transactions, with transaction identifiers, to an internal file. After the problem is corrected, the file will be transferred to the B&C system for processing.

O.6.5 Billing and Collection Audits

NeuStar will provide the infrastructure to collect all data needed for accounting and auditing reports that meet commercially accepted standards and will provide this data, as appropriate, to COTR-designated auditors. Data will be available for the current fiscal year and for an agreed number of preceding years. NeuStar will assist COTR-designated auditors by providing all required statements and reports. Annually, NeuStar's internal auditors will audit the registry's B&C system, records, and supporting documentation to verify the accuracy of billing for usTLD services.