Virtual Registry Services Information Packet

September 24, 2000

VeriSign Global Registry Service's proposal, which follows, contains information and data that are privileged and/or confidential to VeriSign Global Registry. This information and data are not made available for public review and are submitted voluntarily to **###** only for purposes of review and evaluation in connection with this proposal. No other use of the information and data contained herein is permitted without the express written permission of VeriSign Global Registry. Information and data contained herein is protected by the Virginia Trade Secrets Act, as codified, and any improper use, distribution, or reproduction is specifically prohibited. No license of any kind whatsoever is granted to any third party to use the information and data contained herein unless a written agreement exists between VeriSign Global Registry and the third party that desires access to the information and data. Under no condition should the information and data contained herein be provided in any manner whatsoever to any third party without the prior written permission of VeriSign Global Registry.

Contents

List of Figures

1 Introduction

The information in this document is intended to assist in the development of a proposal to Internet Corporation for Assigned Names and Numbers (ICANN) for a new top-level domain (TLD) to be awarded by ICANN on or about December 31, 2000. Sections in this document are provided in the same format as the **TLD Application: Registry Operator's Proposal, Section 15** of August 15, 2000.

2 Technical Capabilities and Plan

2.1 Registry Operator Technical Capabilities (D15.1)

2.1.1.1 Background

VeriSign Global Registry Services (VeriSign Global Registry) has been the provider of .com, .net, and .org domain names since 1991, when Network Solutions Inc. (NSI) provided the services. In August 1999 the Network Solutions Registry began operations as a separate business unit of NSI. In June 2000, VeriSign acquired NSI and renamed the Registry division, VeriSign Global Registry Services.

Historically, the VeriSign Global Registry has provided back-end domain name addressing, resolution, and distribution services for ICANN registrars. We are currently serving over 60 production ICANN accredited registrars and over 60 pre-production ICANN registrars.

The VeriSign Global Registry has an extensive infrastructure comprised of both technology and human capital. Having invested tens of millions of dollars in the infrastructure and having performed the Internet's Registry function since 1991, we have incomparable experience and expertise managing the growth and operations of a commercial registry. On a daily basis, VeriSign Global Registry bears the responsibility of making sure that every .com, .net and .org domain name is located globally, without interruption.

2.1.1.2 Key Achievements

VeriSign Global Registry has developed a successful business providing registry services that are unparalleled in the high-tech industry today. As purveyors of the domain name information that is so critical to the day-to-day Internet operations of millions of customers, VeriSign Global Registry requires a secure, high performance backend infrastructure that is available 100% of the time. An outage or publication of bad information would have devastating consequences for those companies and individuals that depend on the Internet. This is the environment that VeriSign Global Registry has operated in since 1991, and from which we have derived countless years of experience in DNS architecture, design, and deployment.

Utilizing this experience, VeriSign Global Registry will be able to design and deploy a scalable and robust registry solution to handle the needs of the new TLD service. Our current infrastructure is able to support the largest zone file in the world capable of serving trillions of active domain names.

2.1.1.3 Technical Personnel

Operating a successful registry requires knowledgeable operations, engineering, and technical management staff. The VeriSign Global Registry Services staff has grown and evolved to meet the challenges imposed by a rapidly growing Internet and demand for Internet identities in the form of resolvable domain names. Through a strict adherence to qualified operational policies and procedures, engineering excellence, change management, and quality assurance testing, the VeriSign Global Registry technical personnel have executed and supported the largest commercial registry in the world with over 20 million domains and growing. Following are descriptions of the key technical personnel in the VeriSign Global Registry.

2.1.1.3.1 Command Center Operators

These individuals are onsite at the VeriSign Global Registry production data center facility 24x7x365. They monitor system functions, using system and network monitoring and management tools described later in this document. When issues arise, they either address them in accordance with documented procedures, or escalate to Global Registry technical operations or engineering staff. Command Center Operators possess the following skills:

- Knowledge of UNIX utilities commands
- Knowledge of NT utilities commands
- Knowledge of network administration
- Knowledge of systems management and monitoring tool suite

2.1.1.3.2 Unix System Administrators

These individuals provide onsite or on-call maintenance of all production systems, as well as integration of new computing resources and applications in VeriSign's Registry environment. They maintain and implement server and storage devices, disk layouts, file system configurations, and operating system to support specific applications. They also work closely other Global Registry technical staff to develop and implement systems and software solutions. These administrators, individually and/or collectively, possess the following skills:

- Advanced knowledge of the Solaris and AIX operating system
- Hands-on experience with Sun and IBM servers operating in a High-Availability (HA) implementation
- Proficiency with UNIX utilities and scripting (PERL, shell, expect, etc.)
- Understanding of UNIX OS concepts such as paging, swapping, IPC, devices, and file system concepts.
- Experience with DNS, BIND, sendmail, Stronghold, Apache, and WHOIS

2.1.1.3.3 Engineering

These engineers are responsible for designing and supporting the registry and TLD infrastructure. They will be the first line of escalation from the Command Center and possess the following skills:

- In-depth knowledge of DNS and its BIND implementation
- Experience with TCP/IP networking, including NFS, Ethernet, IP addressing & subnetting, routing, and network troubleshooting
- Experience with a variety of routers, switches, and load-balancing solutions

2.1.1.3.4 Technical Management

Technical Managers and Technical Project Managers are responsible for planning and executing changes to the registry. They ensure adequate engineering and operations staffing of the registry, and are directly accountable for the ongoing operations of the registry. Following are the skills they possess:

- Complex project management experience
- Comprehensive knowledge of the registry infrastructure and operation
- Knowledge of change management and trouble management techniques
- Excellent interpersonal skills

2.2 Technical Plan (D15.2)

2.2.1 Overview

VeriSign Global Registry Services will provide the ability for the vendor to sell and support new a TLD domain name through their registrars with a registry infrastructure designed, deployed, and maintained by VeriSign Global Registry Services. To enable a smooth startup VeriSign Global Registry is offering its registry backend services in the form of a virtual registry. To the new TLD registrars and registrants, the new TLD vendor will provide the service. The VeriSign Global Registry will provide the database, zone generation, and zone distribution support as needed to the new names. Specifically, the VeriSign Global Registry will provide the hardware and software infrastructure to store the domain name database and generate the zone files on behalf of the new TLD registry customers. The vendor, who is responsible for recruiting the registrars owns the relationships with the registrars. The new TLD virtual services offerings fall under the VeriSign Global Registry Service Provider group of services and several similar types of services may emerge in the future. The new SRS will have the ability to support the new TLD with the same proficiency that current TLDs are supported.

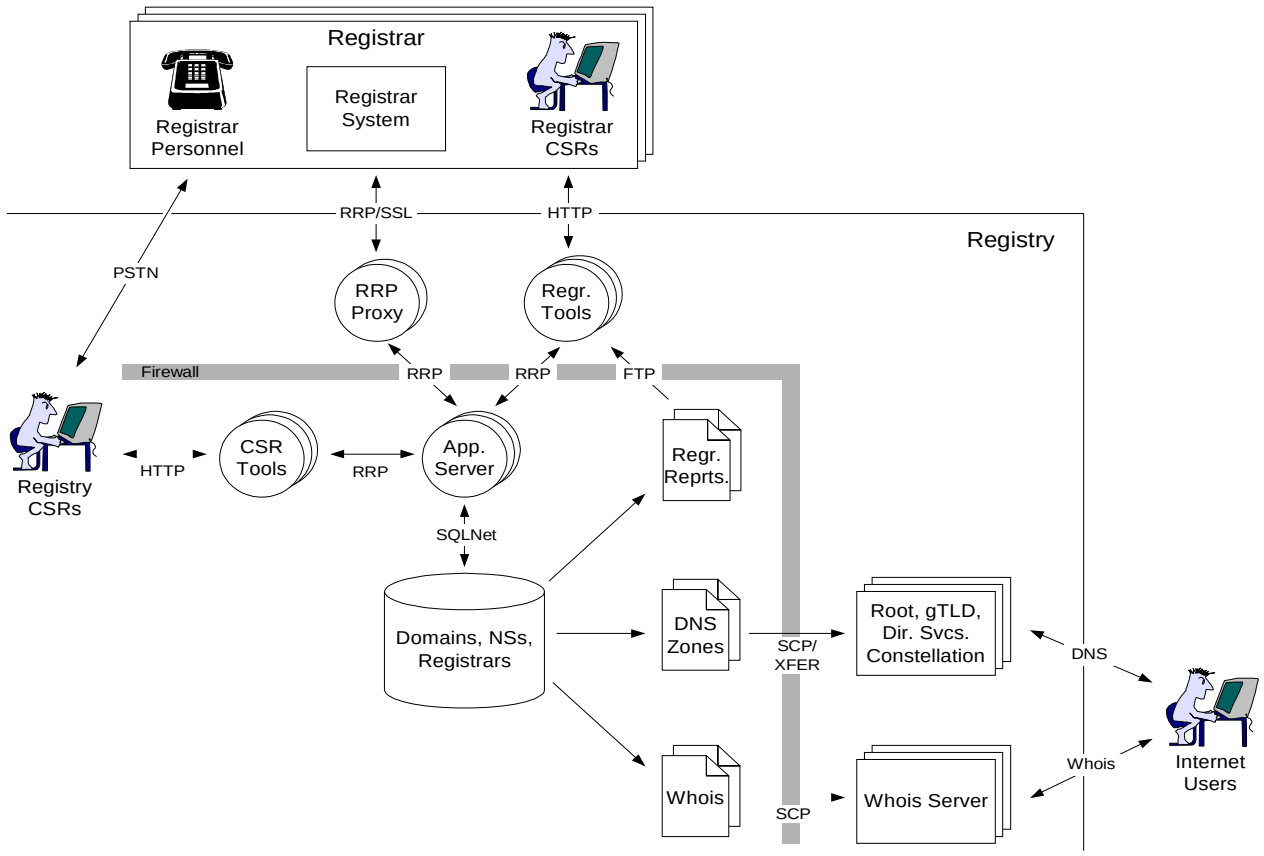

Figure 1 - Domain Name Registration and Resolution Overview

2.2.2 General Description of Facilities and Systems (D15.2.1)

A Shared Registration System (SRS) and Top-Level Domain (TLD) infrastructure are the two major components of the Registry. The Registry SRS enables the Registration Service, Directory Service (Whois), and Customer Service, while supporting the Domain Name Resolution Service by generating and distributing zone files. The TLD system provides the infrastructure and common platform for the Domain name Resolution Service.

The SRS is a protocol and associated hardware and software that permit multiple registrars to provide Internet domain-name registration services within the TLDs administered by the Global Registry. The SRS provides equivalent access to all registrars to register domain names in the TLDs administered by the Global Registry. The System will generate the zone files for the new TLD and distribute them to a TLD constellation to enable domain-name resolution across the Internet.

A Whois service will be provided through the SRS that will allow users to query the availability of a domain name.

Registrars access the System through a Registry Registrar Protocol (RRP) to register domain names and perform domain name-related functions such as registering name servers, renewing registrations, and deletions, transfers and updates to domain names registered by that registrar. Registrars have a web-based interface to access the System to perform administrative functions, generate reports, perform global domain name updates, and perform other self-service maintenance functions not available through RRP.

The Global Registry invoices the registrars for the domain names registered, renewed, and transferred. The Global Registry provides support to the registrars through Customer Support Representatives (CSRs). The CSRs have their own web-based interface to the registry, through which they can query and perform updates per the registrar requests after authenticating the registrar. Global Registry CSRs are trained to provide first-level customer support, and are proficient in customer care skills.

Other external interfaces include registry users who perform Whois queries to the System to determine the availability of a particular domain name or names. The Whois service is available via both a standard command-line interface and a web-based interface.

The TLD infrastructure will consist geographically dispersed TLD name servers. These name servers will be located within the Internet at the topological cores, which roughly correspond to major peering centers for the backbone network providers. Locating these servers at or near the major peering centers ensures low-latency access from networks that carry the bulk of the Internet traffic. Initially, there will be seven name servers located across Asia, the United States, and Europe. Overall performance of the Internet and the services that depend on name resolution is enhanced by this server placement strategy.

2.2.2.1 System location

Virtual registry services will be provided at VeriSign Global Registry Service's new state-of-the-art facility in Dulles, Virginia. The space will include the data center and most personnel involved with the proposed registry, including operations personnel, engineering, quality assurance staff, administrative support staff, and customer care support staff.

2.2.2.2 System/network Diagrams

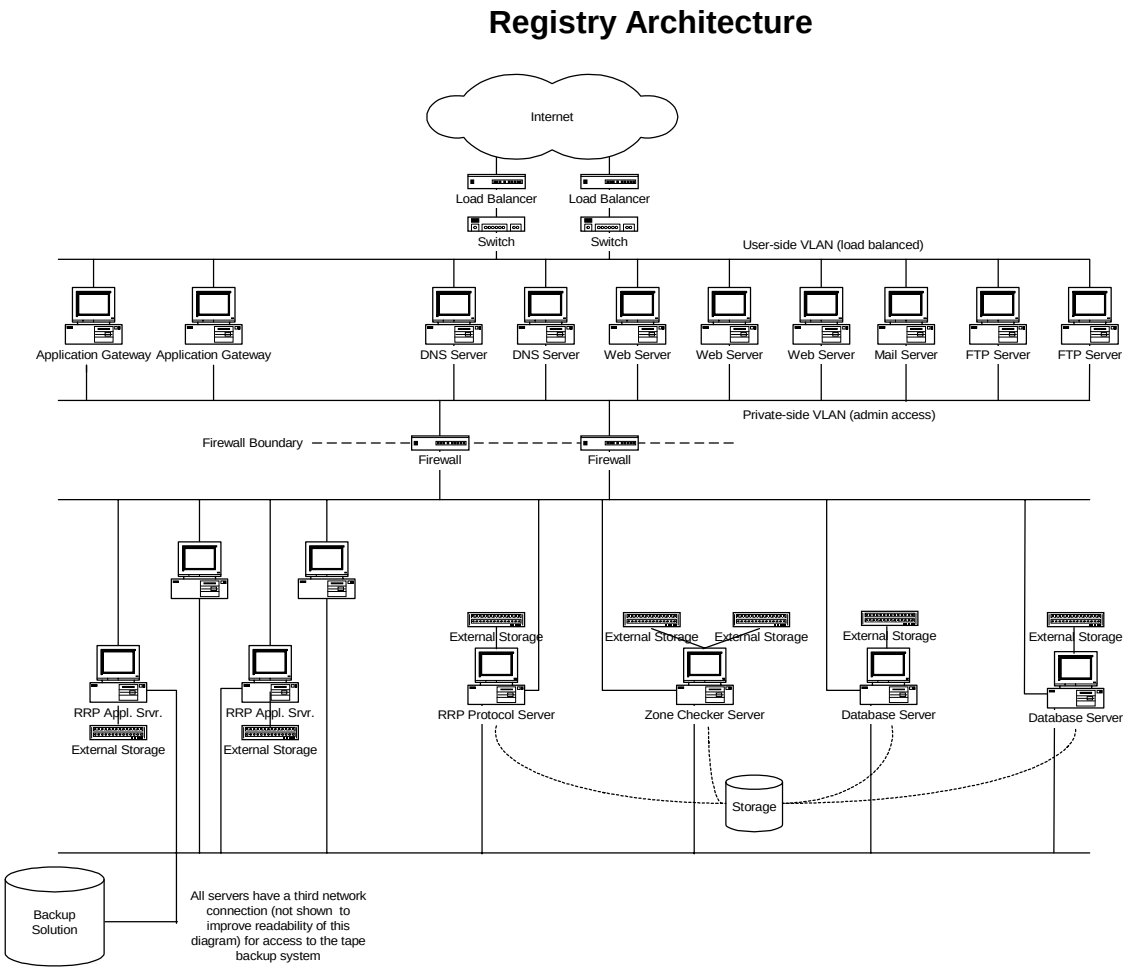

Figure 2 Sample Registry Architecture

2.2.2.3 System configurations

The registry and TLD system configurations will consist of multi-processor UNIX configurations with up to 16GBs of memory. Other equipment used to support the registry includes large capacity border routers, high-performance firewalls, load balancers, and switches. The entire system and network are built so that there is no single point of failure, and includes mechanisms to automatically fail over when errors are detected. A second level of redundancy is provided by an offsite Disaster Recovery (DR) facility where the registry processes can be migrated on short notice.

To accommodate future growth the configuration can be scaled for to handle additional registrar connections and registrations. There is an n-to-n relationship of RRP Application Gateways to RRP Application Servers; depending on where the bottlenecks occur additional servers can simply be added. Because changing the database systems is more complex, it is designed to support the full complement of registrations expected over the next four to five years.

Equipment, processes and procedures have been designed for the seamless operation and support of the registry and TLD systems. A Global Registry Command Center will be established and equipped with the latest monitoring tools for monitoring all the components on a pro-active basis in order to identify and resolve issues before they become problems. There will be an isolated Operations, Test, and Evaluation (OT&E) environment for registrars to test their interface to the SRS software. VeriSign Global Registry Services will also test any new versions of SRS software or hardware configuration upgrades before they are introduced into the production environment..

Also, due to the rapid growth of the Internet and the challenges it presents, VeriSign Global Registry plans to undergo complete infrastructure refreshes every three years.

2.2.2.4 System Capacities

The systems will be initially configured with up to 16GB of memory and 100GB of storage. This is more than sufficient to support the introduction of a new TLD. When needed, the systems are scalable both vertically through the addition of memory and disk space, and horizontally with additional systems.

2.2.2.5 System Interoperability

The Shared Registration System (SRS) is a protocol and associated hardware and software that permit multiple registrars to provide Internet domain-name registration services within the TLDs administered by VeriSign. It has been designed and is operated as a single, interoperable system, where each component is a critical element in the registry processing. An extensive evaluation and quality assurance process ensures compatibility and interoperability when new features, software, or hardware are added to the system.

2.2.2.6 System Availability

The objective of the registry design is to provide 100% planned system availability. This is accomplished through complete system and configuration redundancy, and a process commitment to not execute any system or application changes until they are thoroughly tested in isolated Quality Assurance (QA) and Operations, Test, and Evaluation (OT&E) environments.

2.2.2.7 Facility and Site Descriptions

2.2.2.7.1 VeriSign Global Registry Production Data Center.

This data center is located in VeriSign Global Registry building in Dulles, VA. The 10,600 sq. ft. data center is operated 24x7x365. Onsite staff from the Registry Command Center (RCC) operate and monitor the site and the equipment in the data center room. This data center is not located in any flood plains. Ceiling height is a minimum of 8.5 feet with ventilation being provided via under-floor airflow generated by eight air-cooled HVAC units of 25 tons each, providing for N+3 redundancy. Temperature is maintained at 70 degrees Fahrenheit +/- 2 degrees. Static conditions are maintained within equipment manufacturers tolerances.

Power to this facility is routed through a Uninterruptible Power Supply (UPS) capable of sustaining the data center for at least 15 minutes. However, the UPS is needed only for the few seconds it takes for a 750KW generator to start automatically. A second 900KW generator

is available as additional backup. Power is routed through eight power distribution units (PDUs) with each server being redundantly supplied via two separate PDUs. All racks and equipment are grounded.

2.2.2.7.2 VeriSign gTLD Remote Sites.

VeriSign Global Registry Services has distributed its authorative generic top-level domain (gTLD) name servers worldwide to best serve the Internet community. Each remote site is required to meet high standards for support of the gTLD servers. The geographically and topologically diverse sites provide space in secure, high-availability collocation centers designed and built using industry best models. At these sites, gTLD servers are housed in secure areas and supported by n+1 power and cooling capabilities. They are redundantly connected to the facility's switching fabric with full-duplex 100Mbps connections and have diverse access to large capacity backbone circuits. Access to the TLD servers is controlled by Access Control Lists (ACLs) on border routers that exclude all traffic from the Internet other than UDP and TCP queries. There are 99.7+% uptime requirements for connectivity, power, and cooling to ensure uninterrupted availability.

2.2.2.8 Internet connectivity

Refer to Network Capacities in Section 2.2.11.4.

2.2.3 Registry Registrar Model (D.15.2.2)

2.2.3.1 RRP Description

The VeriSign Global Registry under the auspices of the Shared Registration System program developed RRP. The protocol was initially deployed in April 1999 as part of a test bed implementation of the Shared Registration System with five registrars. Additional registrars began using the protocol in July 1999. RRP has been published as Informational RFC2832, and that open source software is available for both clients and servers.

The registry stores information about registered domain names and associated name servers. A domain name's data includes its name, name servers, registrar, registration expiration date, and status. A name server's data includes its server name, IP addresses, and registrar. RRP provides a mechanism to perform various functions to domain names, such as:

- Determine if a domain name has been registered.
- Register a domain name.
- Renew the registration of a domain name.
- Cancel the registration of a domain name.
- Update the name servers of a domain name.
- Transfer a domain name from another registrar.
- Examine the status of domain names that the registrar has registered.
- Modify the status of domain names that the registrar has registered.
- Determine if a name server has been registered.
- Register a name server.
- Update the IP addresses of a name server.

- Delete a name server.
- Examine the status of name servers that the registrar has registered.

Each RRP session is encrypted using the current Secure Socket Layer (SSL) v3.0 protocol. SSL provides privacy services that reduce the risk of inadvertent disclosure of registrar-sensitive information, such as the registrar's user identifier and password.

Registrars retain all registrant specific information.

2.2.4 Database Capabilities (D.15.2.3)

2.2.4.1 Size

The Global Registry uses Oracle RDBMS to store all of the domain names for a TLD. Since the size of the registry is determined by the number of domain names which are to be stored, the size will vary as new domains are added. Oracle is used by many organizations around the world to store large amounts of information – in many cases, significantly more than will be required for even the largest domain.

2.2.4.2 Throughput

The throughput of the system is dependent upon several different factors of the hardware being used; the number of processors, amount of memory, and disk drive configuration all play a factor. The current Registry configuration supported over 600 million transactions a month up in the second quarter 2000. By designing and deploying a scalable architecture for the new TLD, the registry will be equipped to handle the increased loads as demand for the new TLD warrants.

2.2.4.3 Scalability

Oracle has sufficient ability to scale in a variety of different methods based upon the requirements being placed upon it. However, based on the anticipated size of the new TLD domain, there will be no problem scaling the Oracle database. The VeriSign Global Registry Oracle database was supporting more than 19 million domains by 2nd Qtr. 2000.

2.2.4.4 Object Management

The registry implementation performs management of the registry objects at both the database and business layer levels. In general, the business layer validates any request to the database and an Oracle stored procedure is used to perform the actual changes to the database.

2.2.4.5 Domain Level Capabilities (D.15.2.3.1)

2.2.4.5.1 Change Notification

For each instance where a second level domain holder wants to change its registrar for an existing domain name (i.e., a domain name that appears in a particular top-level domain zone file), the gaining registrar shall obtain express authorization from an individual who has the apparent authority to legally bind the second level domain holder (as reflected in the database of the losing registrar). In those instances when the registrar of record is being changed simultaneously with a transfer of a domain name from one party to another, the gaining

registrar shall also obtain appropriate authorization for the transfer. This information shall be provided to the losing registrar if requested. The form of the authorization is left to the discretion of the gaining registrar.
The registration agreement between each registrar and its second level domain holder shall include a provision explaining that a second level domain holder will be prohibited from changing its registrar during the first 60 days after initial registration of the domain name with the registrar.

2.2.4.5.2 Registrar Transfer Procedures

The transfer procedure is an RRP command executed by the gaining registrar

2.2.4.5.3 Grace Period

The SRS automatically will renew domain names as their current registration periods expire. Following an auto-renewal, a Registrar has a 45-day grace period to delete the domain name. Any names not deleted during the 45-day grace period will be included on the auto-renewal invoice.

2.2.4.5.4 Reporting

The system will be able to produce a variety of reports to help monitor and analyze the type of operations performed on the system. These reports are summarized in the following table:

GENERATION DATE	Type/Description	AUDIENCE	HOW AVAILABLE
Daily	Describe registrar transactions pertaining to that particular registrar	Registrar-specific report to that registrar	Registrar tool or FTP site
Transfer	Describe domain transfers pertaining to that particular registrar	Registrar-specific report to that registrar	Registrar tool or FTP site
Common	Each row contains a full Registrar description.	ICANN, Third-Party Escrow Company	FTP Site
Weekly	Total domain name count, total name server count, total domains hosted by name server count	Registrar-specific report to that registrar	Registrar tool or FTP site

Table 1 Registrar Reports Summary

2.2.4.6 Registrar Add/Delete/Modify Procedures (D.15.2.3.2)

Adds, changes, and modifications to the domain name records are performed by the registrars through RRP. During the certification process the Registrars are instructed on how to process new registrations and make changes to existing records.

Refer to Section 2.2.15 for a complete description of the Registrar Tool that the registrars use to interact with the backend registry.

2.2.5 Zone File Generation (D.15.2.4)

2.2.5.1 Registrar Manipulation of Zone Data

Registrars can access their domain data via three methods (presented in order of automation):

1. RRP protocol as specified in the Informational RFC 2832.
2. Using a web browser and the Registrar Tool web interface, which in turn uses RRP to communicate with the registry database.
3. Contacting the Global Registry Customer Service Representative who uses the Customer Service Tool web based interface to access and manipulate domain and registrar data directly for unusual scenarios.

2.2.5.2 Zone File Generation Process Overview

Custom applications have been developed to securely and accurately extract domain registration data from the registry database to construct the appropriate zone files. The overall process is as follows:

1. A database "snapshot" is prepared
2. Custom applications are launched to extract data from the database and format the data into zone files
3. Validation checks are performed on the static zone files
4. Zone files are loaded on production-like servers and dynamic checks are performed against the server
5. Validated zone files are moved to the zone distribution process

2.2.5.3 Validation

After the zone files are created, a number of checks are performed against the files to ensure they contain valid data in the proper format. Serial numbers, data values, and file size checks are performed on the resultant static zone files.

The zone files are then copied to a name server (to simulate the distribution process) and loaded to verify the named application loads properly. After the process is started, the name server-logging file is reviewed to verify that no error messages resulted. Once the name server is operational, the following the serial numbers are verified again and sample queries are run against the database

2.2.5.4 Frequency

Zone files are generated at a minimum twice daily at 12-hour intervals. The database is constantly being updated but the zone files are generated from a point-in-time version of the database to avoid corruption of previously extracted data.

2.2.5.5 Security

The RRP Application Gateway (RRPAG) is a gateway to the RRP Application Server (RRPAS) from the outside world. The Application Server runs behind the firewall, whereas the Gateway

runs on a machine that is visible to the outside world and listens on a well-known port. Registrars connect to RRPAG using SSLv3.

The primary purpose of the Gateway is to provide transport layer security using SSLv3. The initial connection to the RRPAG is authenticated by RRPAG based on the X.509 certificate that it presents at the time of the connection. After a successful SSL handshake, the Gateway opens a dedicated connection with the Application Server for the connecting entity.

The database and zone generation and validation process is conducted on the registry internal network and systems protected by firewalls that restrict access to the network. A File Replication Tool that allows files to be copied via encrypted channels between hosts controls file replication between the systems behind the firewalls.

Access to the systems is limited to a "need-to-know" basis. Physical data center access is limited to selected Registry engineering and operations staffs. System logon IDs and passwords are provided only to technical staff in operations who are involved in the zone generation and distribution processes, and secure shell (SSH) is used for all logins. User logins are monitored and logged for audit purposes and to recreate any sequence of events if a failure occurs.

2.2.5.6 Interface

The zone generation process is done via custom interactive applications that are controlled by operations personnel. Some applications are automated but manual checks are performed at many points in the process to ensure proper construction of the zone files before they proceed to the distribution process.

2.2.5.7 User Authentication

All production registry systems require the use of SSH with public/private keys and encryption for interactive login sessions.

2.2.5.8 Logging

All transactions that impact the zone files are captured in activity and status log files using standard (e.g. Syslog) and custom-built logging utilities.

Processing logs will be created to capture processing statistics, such as number of records processed, passed, or failed, for each audit rule. The format of the logs will comply with the monitoring tool requirements so that the monitoring tool can be used to monitor the processing.

The CSR and Registrar Tools use the registration system's configuration-driven logging system. The developer and operator can specify how to log messages, given their origin, type, and severity. The log message provides valuable information to pinpoint when the event occurs and for what reason.

2.2.5.9 Backup

The EMC Data Manager (EDM) Symmetrix Timefinder Replication tool is used by the Global Registry to perform backups of the systems and databases. Timefinder is a utility that allows one to make exact physical copies of Symmetrix disk volumes, on a second set of Symmetrix disks called Business Continuance Volumes (BCVs). The BCVs can then be mounted on a server, producing an exact physical copy of the original disks. Timefinder is integrated with Oracle's online backup procedure to allow the replication of a database instance, as well as

greatly enhance the speed and functionality, of database backup and recovery. The copied data is then backed up to tape.

2.2.6 Zone File Distribution and Publication (D15.2.5)

2.2.6.1 Name Server Location

TLD name servers will be located in diverse geographic locations and on diverse Internet service provider (ISP) networks. The select TLD server sites will all be housed within leading Internet collocation centers located at or near major centers of peering among Internet backbone providers. Each of these sites will be chosen using a rigorous set of requirements covering network, security, power, fire suppression, and other key factors. In terms of network availability, the following requirements are met by all of the sites:

- *Diverse Internet connectivity* – minimum of two diverse circuits,
- *Extensive public and private peering* –number and quality of peering and transit relationships in force at each of the proposed facilities,
- *Fully redundant routing and switching infrastructure* – each facility network follows accepted best practices for high-availability including the use of multiple ingress/egress routers, dynamic routing protocols (BGP and OSPF), redundant layer 2 switching infrastructure, and HSRP (or VRRP) for default router redundancy, and
- *Facilities* – secure facilities with n+1 power and cooling capabilities
- *On site support* – each facility operator has a 24x7x365 NOC with on-site "hands and eyes" support.

2.2.6.2 Distribution Procedures

Zone files are distributed by a completely separate infrastructure than the zone generation process so the two processes do not impact one another. Once the extraction process generates zone files, they are transferred to dedicated machines for preparation and distribution to TLD servers.

Distribution of zone files is performed over an encrypted channel using SSH and an encrypted private VPN to all TLD servers. Distribution via this method uses compression to decrease transfer time, and uses MD5 to verify the integrity of the file received after the transfer process. Multiple instances of the process will be started to update all TLD servers within a narrow time interval. Name servers are restarted at staggered intervals to avoid disrupting DNS service and to also ensure the proper operation of name servers with the new zone files.

The distribution procedure will be semi-automated and closely controlled and monitored by operations personnel. NOC personnel monitor the distribution process from start to finish and can intercede at any time should a situation require the interruption of the process.

Note: The TLD zones will be distributed on a separate infrastructure from the .com, .net and .org infrastructure for diversity and to avoid interruption of service. The Service Level is designed to be comparable.

2.2.6.3 Validation

Operations personnel use a checksum algorithm on the final TLD zone file to verify its integrity with the reference zone file. Once the zones are verified, the name server will be

restarted. Operations personnel will monitor the name server error log files during application restart to verify the error free loading of new zone files. Dynamic queries will then run against the name server to verify proper operation and accurate responses.

2.2.7 Registrar Billing (D15.2.6)

Finance reports are used for financial analyses of VeriSign's Internet domain name registration business and for billing purposes. These reports facilitate VeriSign's invoice preparation and distribution processes and aid registrars in invoice reconciliation. Finance reports are available to Global Registry staff through the Registrar Tool of the Shared Registration System (SRS) and the reporting server FTP site.

Detail and summary reports are produced on a monthly basis for billing. Only summary reports are generated for revenue analysis and made available internally to the finance department. Detailed reports with domain names that meet specified criteria for registration renewals, transfers, and deletions are distributed to each registrar.

The billing model for the Global Registry will be in two tiers. Registrant billing will be the responsibility of the registrars. The Global Registry will bill the registrars monthly in arrears for each month's Registration Fees. All Registration Fees are due immediately upon receipt of Global Registry's invoice. Optionally, the Global Registry can require the registrars to post a letter of credit, deposit account, or other acceptable credit terms agreed by the parties for security.

It will be up to the vendor to determine the financial relationship with the registrars. If so chosen, a registrar can be required to establish its payment security through one of several vehicles, including a cash deposit, an irrevocable standby letter of credit, or a payment security bond. The size of the deposit is negotiable, but can be based on the number of expected registrations and the trending of the registration volumes by a registrar. These monies will be used as guarantees of payment against registration and re-registration of domain names. These terms are defined in the Registrar License and Agreement that the Global Registry will sign with each registrar.

Registrars will be invoiced monthly for net new, transferred, and extended registrations. To accommodate the five-day grace period for deletions, final billing reports are generated on the sixth business day of the following month. Invoices generally are distributed within two business days following the availability of billing reports. Invoice payments are due upon receipt and considered late after five days.

Registrars will also be invoiced for net auto-renewals. The SRS automatically will renew domain names as their current registration periods expire. Following an auto-renewal, a registrar has 45 days to delete the domain name. Any names not deleted during the 45-day grace period will be included on the auto-renewal invoice.

To accommodate the grace period for auto-renewal deletions, final billing reports will be generated 46 days after the close of the invoice month. Invoices generally are distributed within two business days. Invoice payments will be due upon receipt and considered late after five days.

2.2.7.1.1 Billing Tools

Registrar Tool - A registrar will be able to check its available credit using the Registrar Tool on the Global Registry's web site.

Low Balance Emails - Prior to beginning registrations, each registrar selects a "Low Balance Notification Percentage" value. The Low Balance Notification Percentage indicates at what point a registrar wishes to be notified of a low account balance. When a registrar's available credit is equal to or less than its Low Balance Notification Percentage times its total credit limit, the system sends automated email notifications to the registrar's routine email address. Emails are generated at 5:00 AM ET and 5:00 PM ET.

2.2.7.2 Technical Characteristics

The Global Registry provides billing reports to their registrar customers that will allow them to review and reconcile their accounts. These reports are generated automatically and made available through a secure web site or from a secure FTP server. The Global Registry also uses these reports to prepare monthly invoices, which are currently manually prepared and submitted. No changes will be made to the SRS for billing at this time until volumes increase to a point where manual processes are inadequate.

GENERATION DATE	Type/Description	AUDIENCE	HOW AVAILABLE
Weekly	Summary revenue. Subtotals by registrar within each report	Finance	E-mail distribution
1st of month	Summary revenue	Finance	E-mail distribution
6th of month	Summary billing & revenue	Finance	E-mail distribution
6th of month	Detail reports for registrations, transfers, extensions, and refund/no refund deletions for each transaction type; registrar-specific	Registrars (registrar-specific info only)	Registrar tool and FTP site
16th of month	Auto-renewal	Finance	E-mail distribution

Table 2 Billing Report Summaries

Examples of the reports to be generated for the registrars are as follows:

Monthly Billing Reports (Detailed and Summary as currently in SRS)

- Monthly Registration Report
- Monthly Transfer Report
- Monthly Auto-renewal Report
- Monthly Additional Years Added Report
- New Registration Deletion Report (Refund and Non-Refund)
- Auto-Renewal Deletion Report (Refund and Non-Refund)
- Additional Years Deletion Report (Refund and Non-Refund)
- Transfer Deletion Report (Refund and Non-Refund)

Revenue Reports (Monthly and weekly as currently in SRS)

- Registration Report
- Transfer Report

- Auto-Renewal Report
- Additional Years Added Report
- Auto-renewal Report

Table 3 Billing Report Examples

2.2.7.3 Accessibility and Security

There are two ways to access the registrar billing reports: through the Registrar Tool using a browser, and by logging on to a secure FTP site and downloading the reports. IP filtering based on source address restricts access to the FTP server to accredited registrars, and all logon attempts are logged and periodically checked.

All logon access to the registrar billing information is limited to specific points of contact at the registrars, who are provided unique IDs and passwords. Any changes to registrar contacts must be authorized and authenticated through Customer Support.

2.2.8 Data Escrow and Backup (D15.2.7)

2.2.8.1 Overview

The goal of the escrow process is to periodically encapsulate all registrar-specific information into a single escrow file and to make this file available to a third party for escrow storage.

Existing daily and weekly reports as well as a new registrars report will be used to construct the escrow file because these reports, when taken together, describe completely the entire set of registrars.

The escrow process employs a method of encapsulation whereby the daily, weekly, and registrar reports are concatenated, compressed, signed, and digested into a single file. The format of this encapsulation enables the single file to be verified for completeness, correctness, and integrity by a third party.

2.2.8.2 Escrow Process

Steps of the escrow process require that a format file be created for each report file. A “tar” utility is used to concatenate the files into a single data file, which is then compressed. For authentication, a digital signature is applied to the data file. A “checksum” algorithm is then used to check the data value and create a message digest for the digitally signed file. The message file is then concatenated to the data file to create a single file suitable for escrow.

2.2.8.3 Data Verification

The verification process uses layers of meta-data encapsulated in the escrow file to construct a verification report, which indicates whether an escrow file meets the above authentication requirements.

2.2.8.4 Data Format

Standard UNIX utilities are used to concatenate and compress the files into a single file for more efficient storage and recovery.

2.2.8.5 Restoration Process from Escrow Data

If file recovery from the escrow data is required, the tapes are retrieved from the offsite storage facility and the escrow steps reversed to uncompress and recover the files.

2.2.8.6 Backup Procedures

The domain name database is backed up fully on a daily basis.

2.2.8.7 Backup Hardware and Software

The VeriSign Global Registry uses EMC and Storage Tek hardware and Veritas software for backing up the files for escrow.

2.2.8.8 Escrow Agent Identity

The following information is confidential. The VeriSign Global Registry uses Iron Mountain Corporation for offsite storage.

2.2.8.9 Recovery Procedures

If escrow data is needed, VeriSign Global Registry's offsite storage is contacted and the appropriate tape or tapes are couriered back to the Global Registry.

2.2.9 Whois Service (D.15.2.8)

2.2.9.1 Hardware and software

2.2.9.1.1 Hardware

The Whois daemon will run on multiple servers that are scalable with more memory, CPUs and disk space as needed. These servers are actively/dynamically load balanced to provide optimum response time and reliability. Each server accepts connections from a variety of clients, and accesses a local copy of the Whois data files. This architecture is scalable as query traffic increases by adding additional servers and/or increasing the capacity of the existing servers.

2.2.9.1.2 Software

The Whois service is implemented via two major software components:

1. Data extraction and format applications
2. Whois server daemon

The Whois data extraction applications generate the Whois data files and indexes from a static read-only portion of the Registry database. These applications will run on servers located on the internal network of the registry and cannot be accessed by the Internet population.

The formatted Whois data files are then transported to the Whois server machines. All Whois servers have the same data and will be actively load balanced. These Whois servers handle Internet users queries directly after passing thru site load balancing equipment.

The Whois daemon runs on each of several servers, accepts connections from a variety of clients, and accesses a local copy of the generated files. The daemon is configured using configuration file that may be edited, then re-read on the fly. This configuration file controls much of the dynamic behavior of the daemon, including disclaimer and other query response output, maximum load, and speculation control. The daemon may be configured to have different properties for each of several ports, thus allowing users of different classes to obtain different qualities of service.

The Whois daemon gives the administrator control as is reasonable over the number, type, and behavior of incoming sockets. This control does **not** affect the rest of the daemon architecture—e.g., logging, error-handling, searching, state management, etc.

In the daemon, two fundamental objects must be configured: sockets and behaviors. Customizing these objects enable the Global Registry to tune the operation of the server to provide almost any level of service required.

2.2.9.2 Network Connectivity

Whois servers will be located in a segmented LAN configuration to segregate them from other internal registry functions for performance and security reasons. The Whois service is supported by the same Internet connectivity that supports the registrar-to-registry interaction. Multiple connections to multiple ISPs provide the capacity and redundancy required for high availability Whois services. See Section 2.2.11.4 for more network connectivity details.

2.2.9.3 Search Capabilities

The Whois implementation will use the standard Whois server application used by the Internet population. This application can be used to look up records in the registry database (via the Whois data files) to provide information about domains, name servers, and registrars. Searches for text strings embedded in domain information fields will be searchable as is limited by current standard Whois server implementations.

2.2.9.4 Coordination with Other Whois systems

An implementation of Referral Whois (RWhois) can be implemented in a controlled, test bed fashion if interaction of other Registrars/Registries Whois services is required. However, this service is not currently supported at the registry.

2.2.10 System Security (D.15.2.9)

2.2.10.1 Registry System/Network Security

The registry will be connected to the Internet via two border routers and multiple DS3 connections for diversity. Border routers will use Access Control Lists (ACLs) to control access from the Internet. RRP Application Gateway, Whois, and web servers will reside behind the border routers but outside the firewalls, and have access to them controlled by destination IP address and port number. Access to the application Gateway is also filtered by source address block, ensuring that no one other than the accredited registrars will gain access. One of the

TLD servers will also reside on this network and be accessible from the Internet to answer queries.

The Application Gateway servers will be configured with internal and external interfaces, each assigned to a different subnet. External interfaces will receive queries and registration requests from the Internet, whereas the internal interface will be used for communicating to the application and database servers. Acting as a proxy, the Application Gateway will accept and pass query requests and registration information through the firewall to the application server, thereby eliminating direct registrar access to the backend servers. This approach provides superior security from hackers or other Internet based threats.

Firewalls will be used to secure the internal network and the application and database servers. The firewall will be configured with rules to allow only data traffic between the Application Gateway on the external network and the application and the database servers on the internal network. Additional rules will allow the registry's internal management systems to access the servers for monitoring purposes and to refresh files as necessary.

Changes to the ACLs and firewall rules are tightly managed by operations, who use structured change management techniques to oversee changes when registrars are added or deleted, or other changes are made. The Global Registry utilizes security scanning software to constantly monitor its network for security leaks, and has contracted with an outside firm to run "friendly" scans against the network at least twice a year. Results of the scan are promptly reported to Global Registry Operations.

Security Breach Recovery

A security breach occurs when one or more systems are accessed (and potentially modified) by unauthorized personnel. Often such breaches occur via a network connection. Recovery from security breaches is straightforward, but is often consuming, and potentially disruptive to the services hosted on the affected systems. Certain security breaches may disable a service, for example Registration, for the duration of the recovery and cleanup activities. Following is a summary of the steps involved in recovering from a security breach:

1. Identify affected systems and remove them from the network to prevent further damage
2. Identify mode of access (how the attacker gained access)–for example, account ID and password compromised or service exploited.
3. Notify appropriate law-enforcement authorities of the event
4. Correct weaknesses exploited on all systems including those not breached
5. Collect and preserve evidence and other information for turnover to law enforcement
6. Cleanse affected systems by reformatting disks and re-installing operating system, software, and data from the most recent back-up prior to breach
7. Reconnect systems to network and restore services

2.2.10.2 Physical Security

Physical security for the Registry is of paramount importance based on the value of the services provided to the Internet community. In this regard, the following precautions will be enabled:

Base Building

- Exterior walls and floors is re-enforced concrete or masonry.
- Equipment space is compartmentalized into multiple zones to minimize fire and security risks.

- Building design standards exceed the minimum required by local building codes for seismic, wind, and snow loads.

Physical Security

- The building is isolated from easements, rights of way, and adjoining tenants.
- The building is securable, with a security guard placed at the entrance to the building or grounds to prevent unauthorized access.
- There is no exterior signs indicating the type of business should be visible from any public way.
- Backup generators have sound attenuation enclosures and located within a secured space.
- A single entrance serves as the main entrance, with biometric and/or electronic card readers, a mantrap and 24x7x365 security guards.
- Cameras will be located at all doors, the guardhouse, UPS room, transfer switch room, generator and condensing units yard, transformer locations, mantraps, perimeter, roof, and within the main I/T equipment room.

2.2.11 Capacities (D.15.2.10)

2.2.11.1 Average System Capacities

The VeriSign Global Registry carefully selected the system vendors, IBM and Sun, based on their reliability, serviceability, performance, and scalability. Their respective average system capacities are dependent on their individual configurations, which will change as requirements and demands change. An architectural goal of VeriSign Global Registry is that these systems operate under 50% utilization, so that they can handle 100%+ peak loads, as well as supporting fail over scenarios where one server may have to assume the workload of two. These systems are constantly monitored, and proactively upgraded when average system utilization exceeds a pre-determined threshold. Memory and disk space utilization are also monitored as part of this process and upgraded as needed.

2.2.11.2 Peak System Capacities

Peak system capacities are dependent on equipment configurations. VeriSign Global Services is designing the new TLD registry infrastructure to accommodate numbers and growth rates similar to .com. Effective June 2000 the VeriSign Global Registry was processing over 20 million transactions a day and had over 19 million domain names. Individual system capacities are scalable as needs required, but in addition, the registry systems are designed to be expanded by adding additional systems and load balancing between the systems. By expanding horizontally with additional systems as well as vertically with additional processors, memory and disk space, there is huge growth potential.

2.2.11.3 Database Capacities

The Oracle database will support up to xxxx records, which should be significantly more records than required even for the largest domain.

2.2.11.4 Network Capacities

The Global Registry has designed and constructed its network to deliver exceptional availability, performance, scalability, security, and maintainability. In terms of bandwidth and connectivity the registry supports four DS3 connections to the Internet from four different major ISPs. The border routers pass up to 1 million packets per second to and from the Internet.. The Global Registry monitors the circuits constantly for utilization and upgrades the circuits when they reach 50% average utilization.

Future upgrades to the registry production network will include increasing the size of the circuits to the Internet and replacing fast Ethernet links with gigabit Ethernet links.

2.2.11.5 System Scalability

As indicated in earlier sections, the key to a successful registry implementation is be able to scale as the demands on the systems increase. The VeriSign Global Registry has architected scalability into the registry design to ensure sufficient capacity to manage large amounts of growth. Individual systems can be upgraded or additional systems added to increase the capacity of the registry.

The TLD configurations are also designed to scale in the same manner as the size of the zones and the number of queries increase.

2.2.11.5.1 Personnel

The Global Registry operates on a 24x7x365 basis with a full complement of support staff for supporting the registry, back office, and TLD infrastructures. In critical situations, all the technical staff can be contacted via pagers or cell phones. Sufficient personnel are available to monitor and maintain current systems, troubleshoot, and develop additional features to the registry infrastructure. The Northern Virginia area is also a major technology center with access to a deep pool of engineering and operations talent.

2.2.12 System Reliability (D15.2.11)

2.2.12.1 System Reliability, Availability, Serviceability

The registry system is designed to be highly reliable with state-of-the-practice architectural elements and operational procedures applied throughout. Using elements such as component redundancy, load balancing, high-availability (HA) configurations, hot spares, aggressive vendor maintenance contracts, and optionally, multi-site operations, the Registry is able to ensure the uninterrupted availability of registry services. The registry is designed to meet the following goals:

- Provide uninterrupted service redundancy to mitigate the risk of most system failures
- Minimize the length of service interruptions that may occur as a result of a catastrophic event
- Prevent data loss

In addition to the core registry infrastructure, the TLD name servers are distributed in multiple locations throughout the world. Although each TLD site depends on the facility where it resides, the TLD system as a whole does not depend on the registry site except for updated

zone files. Even with a loss of the registry, the global TLD servers will continue to provide basic Domain Name Resolution Service with then current zones.

2.2.12.2 Database Integrity

The Global Registry uses the Business Continuity Volume (BCV) software feature of the EMC Symmetric Array to periodically perform backups, Ad-Hoc and regularly scheduled reporting, and corruption detection. Backups and restores are performed using the EMC EDM backup product providing complete images of the Oracle database that are posted to tape on a daily basis. Both ad-hoc and regularly scheduled reports are constructed from a physically separate reporting server connected to the Symmetrix array using BCV technology for the daily Oracle database image. Exhaustive Oracle block level corruption detection and application-level data scrubbing are performed on the BCV image so operations personnel can detect corruption, determine actionable root cause of failure, and implement solution alternatives early in the process. Both the primary and secondary sites have equal and compatible backup and restore technology.

2.2.12.3 System Support

The Global Registry provides a variety of tools to support the system. For problems that occur within the normal operation of the system (e.g., Customer Service requests), a web-based tool is available that allows for a variety of domain operations to be performed. For troubleshooting of system problems, a Global Registry Diagnostic Tool is used which interrogates each of the system components to verify their proper functioning. This includes:

- Determining that systems are responding to network requests
- Tests database for proper operation (DB connectivity, verifies create/read/edit/delete operations)
- Testing of Application Servers

2.2.12.4 Processes and Procedures

VeriSign Global Registry documents and uses standard operating procedures (SOPs) in running the registry. Each step in the process of registering domain names, generating zone files, distributing zone files, and maintaining the backend infrastructure is tested in an isolated QA environment before being released. The QA environment is designed to closely emulate the operational environment, and QA Engineers stress test hardware, software, and processes and procedures to ensure they will integrate cleanly and not be the cause of an interruption of service. The results of the tests are thoroughly documented and test results are reported back to Engineering and Operations. This process is a closed loop process; any problems encountered during testing are fed back through the process, corrected, and retested.

For the most part, registry processes are automated. Where operations intervention is required, there are strict guidelines and checklists to ensure that all steps process correctly. The RCC monitors all the processes on a 24x7x365 basis. When a problem occurs, the RCC staff follows pre-defined procedures to identify and resolve the problem. If the problem cannot be quickly resolved, there is an aggressive escalation path to quickly involve the appropriate technical management and staff.

Registrars are required to be accredited by ICANN. Once accredited, they must pass certification by the VeriSign Global Registry to begin registering domain names. This process

is an essential ingredient ensuring that registrars will not face complications when beginning to register domain names in production mode. To assist when needed, there are CSR's available on a 24x7x365 basis to answer questions and provide transactional assistance when required.

2.2.12.5 Change management

We use change management systems and processes in both Engineering and Operations departments to keep the VeriSign Global Registry Systems in operation. This includes periodic planned outages to perform maintenance on the registry systems. As indicated above, integrating changes into the registry requires passing a rigorous testing and evaluation stage before being allowed.

VeriSign Global Registry also employs technical project managers to plan and track execution of changes made to the Registry. They conduct a risk analysis of any proposed change, and ensure that all affected parties are involved in any change.

2.2.12.6 Service Level Agreement (SLA) Summary

The VeriSign Global Registry strives to provide a world-class level of service to its customers. A Service Level Agreement provides metrics and remedies to measure performance of the Registry and to provide accredited and licensed registrars with credits for certain substandard performance by the Registry coupled with a Registrar License and Agreement

Shared Registration System ("SRS") Availability shall mean when the SRS is operational. By definition, this does not include Planned Outages or Extended Planned Outages. Planned outage shall mean the periodic pre-announced occurrences when the SRS will be taken out of service for maintenance or care. The Global Registry will achieve 99.4% or better availability for the SRS system.

Unplanned outages are generally defined as the amount of time recorded between a trouble ticket first being opened by the Global Registry in response to a registrar's claim of SRS unavailability for that registrar through the time when the registrar and Global Registry agree the SRS Unavailability has been resolved with a final fix or a temporary work around, and the trouble ticket has been closed. Unplanned outages are also defined as any time that exceeds the planned outage time or the planned outage time interval.

SRS Unavailability shall mean when, as a result of a failure of systems within the Registry's control, the Registrar is unable to either:

a) Establish a session with the SRS gateway that shall be defined as:

- Successfully complete a TCP session start,
- Successfully complete the SSL authentication handshake, and
- Successfully complete the registry registrar protocol ("RRP") session command

b) Execute a 3 second average round trip for 95% of the RRP check domain commands and/or less than 5 second average round trip for 95% of the RRP add domain commands, from the SRS Gateway, through the SRS system, back to the SRS Gateway as measured during each monthly Timeframe.

The Whois service will be updated once a day and availability will be equal or better than that defined for the SRS system.

TLD servers will be updated a minimum of once a day and the collection of servers as a whole will provide 100% query service availability to the Internet population. The TLDs geographic and network diversity ensures that multiple servers will be operating at any given time.

If any service levels are not met during a defined interval (e.g. Month), a credit based on the volume of add domain transactions will be given to the affected registrar(s). The maximum credit provided will be limited to 5% or 10% depending on the metric that was exceeded or not met.

2.2.13 System Outage Prevention (D.15.2.12)

Although high-availability features are designed into all Global Registry systems and services, efforts are concentrated on make core services "bullet-proof". These core services include those that are required for the smooth operation of the Internet and are immediately evident to the Internet community in the event of a failure. Core services include:

- Domain Name Resolution Service
- Registration Service
- Directory Service
- Customer Service

Other services that are important to the operation of the Global Registry, but whose failure or degradation would not affect operation of the Internet include:

- Offline Backup/Restore
- Mail
- FTP Reports
- Logging
- Diagnostic Processes

2.2.13.1 Primary and Secondary Systems

The VeriSign Global Registry employs IBM and Sun UNIX systems in high-availability configurations to ensure no single point of failure. In addition, the Global Registry uses offsite tape storage and an offsite disaster recovery facility that is constantly updated with current information. This site would be utilized during full outage and some partial outage scenarios. See Section 2.2.2 for more system information, and Section 2.2.14 for more fail over information.

Note: Not all registry services include secondary facility support.

2.2.13.2 TLD Systems and Constellation

The TLD configurations are designed so there are no single points of failure. This is accomplished through the use of redundant components, both at the system and component level. For example, multiple switches and load balancing devices will back one another up in the event one fails, and the devices will be configured with dual power supplies when available. Configurations are designed so that when a failure is detected, the service will fail over to the

backup systems. High-availability operational procedures as established in RFC 2870, "Root Name Server Operational Requirements", will be used as guidelines for building and maintaining the name servers.

There will initially be seven (7) geographically distributed TLD name servers to support the new TLD. These name servers will be strategically placed at topological cores of the Internet; those areas that serve the greatest number of hosts and users. As well as topological, there will be geographic diversity to ensure that manmade or natural disasters in a single region will not affect the ability to answer queries by the remaining servers. It is anticipated that the name servers will be placed in the following locations:

1. Asia (2)
2. North America (3)
3. Europe (2)

TLD query rates will be constantly monitored, and the TLD name servers re-deployed as necessary to best serve the needs of the Internet users of the new TLD.

The DNS software is also designed to handle a failure of one or more name servers, so a failure of one or more servers in the constellation will not materially affect TLD resolution services.

2.2.13.3 Network Architecture

The network infrastructure is designed with redundant devices, multiple physical routes and physical diversity. The objective is to isolate single-point failures with no interruption of services or degradation in performance. In most cases, isolation of failures is automatic and occurs within a few seconds of the event. It would take a minimum of two simultaneous network-component failures to disable the network infrastructure. Certain component failures (such as firewall failure) may require manual intervention to complete the fail-over.

Internet connectivity is enabled through multiple direct high-speed connections to Tier 1 backbone providers and ISPs. Part of the selection process for ISPs is their participation at public and private peering points; the greater the number of peering relationships, the better situated they are to serve the largest segments of users. Diverse connections ensure that a failure of one ISP's network will not disable access by registrars, although there may be a temporary delay as the connections are reestablished through other carriers.

2.2.13.4 System Monitoring

The VeriSign Global Registry will utilize a range of standard and custom enterprise systems management tools to monitor and manage the registry production systems and the globally dispersed TLD constellation. These tools are used both by the Network Operations Center and the Global Registry Operations staff for system and network monitoring. A brief description of each tool and its use is outlined below.

WebNM is an SNMP-based monitoring is tool used to monitor system attributes such as:

- CPU utilization
- Memory utilization
- Hardware faults and failures
- Packet loss
- Network latency

- Network traffic analysis
- Operating System services

Tool features include monitoring real-time system availability for servers and network devices, an interactive web interface, and graphical displays of historical performance data. Thresholds can be set from which alarms are generated and forwarded to the RCC.

Concorde SystemEdge is an agent based monitoring tool that uses SNMP to monitor system specific attributes, including:

- File system size
- CPU usage
- Load average
- General system information (CPU types, OS type, Memory size, etc.)
- Any Operating System processes

This tool features include an integrated alert manager, an interactive web interface, system self-monitoring, and logfile monitoring. Thresholds can be set from which alarms are generated and forwarded to the RCC.

A DNS Remote Real Time Monitor was developed by the Global Registry to monitor the real-time traffic flow of root and TLD DNS servers. It monitors the following attributes:

- Response time of last DNS query
- Authoritative for zone
- Zone serial number and when serial number changes
- Real-world query to server and compare to expected result

TeamQuest is a performance analysis, diagnostic, management and modeling product suite. It incorporates highly detailed operating system statistics, process accounting, custom data, and RDBMS performance data, including:

- Identification of server problems
- Drill-down investigation of events, alarms, and unusual system behavior
- Root cause analysis of system performance issues
- Trend analysis
- Correlation of cause and effect
- Compliance with service level objectives
- Understanding the impact of substantial changes or new applications
- Modeling (Analytical Queuing Analysis or Discrete Event Simulation)

2.2.13.5 Trouble Reporting

When problems are either reported to or observed by the RCC, the RCC staff will open a trouble ticket and perform preliminary analysis to determine the severity, diagnose the root cause and correct the problem if possible. Problems are assigned one of the following categories:

- Severity 1 – service outage; severe or potentially severe impact
- Severity 2 – service degradation; impact is not severe
- Severity 3 – component outage; redundant components or workarounds prevent any service impact.

If the RCC cannot resolve the problem, it will immediately escalate to either the on-call System Administrator (SA) or on-call DNS engineer in VeriSign Global Registry Technical Operations (depending on the nature of the problem). In the unlikely event that the problem cannot be resolved at this level, the problem is escalated to VeriSign Global Registry Engineering. A workaround may be provided until the issue is resolved.

2.2.13.6 System and Physical Security (refer to D.15.2.9)

2.2.13.6.1 Physical Security

VeriSign Global Registry Production Data Center

The VeriSign Global Registry production data center is protected by onsite security staff 24x7x365 and the use of card readers. Only VeriSign Global Registry employees are permitted unescorted access to the building. Additionally, the data center room is further restricted (via card readers) to only those employees who perform hardware installations or maintenance. Between the hours of 7pm and 7am all card access is disabled, and anyone requiring access to the data center must obtain a special entry badge from the Global Registry Command Center.

Remote Sites

All remote gTLD sites provide 24x7x365 onsite security that meets or exceeds the security at the VeriSign Global Registry. Global Registry equipment is contained in locked cabinets and, in some cases, locked cages. Most sites also provide separate data center rooms with limited access to each room.

2.2.13.7 High-Availability (Refer to D.15.2.11)

Please refer to Section 2.2.2

2.2.13.8 Facilities

VeriSign Global Registry is located in a new state-of-the-art facility in Dulles, Virginia. The 10,600 square foot data center will house primary Registry systems and personnel. Please refer to Section 2.2.2.7 for more primary site details.

The secondary data center is located at a facility in suburban Maryland that provides secondary site support services. There are multiple high-speed direct connections to this site from the VeriSign Global Registry Production Data Center to facilitate backup and fail-over scenarios. The facility is supported by n+1 power and cooling, and is staffed 24x7x365.

2.2.13.9 Natural and Man-Made Disaster Impact and Fire Suppression

VeriSign Global Registry Production Data Center.

This data center, located in northern Virginia is not in an earthquake zone, and therefore does not need protection against earthquakes. It does provide protection from flooding, but only limited protection from other natural disasters. Fire suppression is provided by an FM200

system that is smoke activated. As a backup, a heat-activated water sprinkler system will engage sprinkler heads individually.

Secondary Data Center

Same as above except that protection from all natural disasters is provided in a structurally reinforced facility.

Remote Sites.

Some remote sites provide for earthquake "hardening" depending on specific location. All the sites are in data collocation centers that are designed to withstand natural disasters endemic to the respective area. The sites all have fire suppression systems similar to that employed in the VeriSign Global Registry production data center, with a non-water based system as primary and water as backup.

2.2.13.9.1 Power Backup/HVAC and Redundancy

Redundant UPS units protect the data center. Additional redundant power features include:

- A 750KW diesel generator to sustain the data center for 48 hours
- Four-fuel suppliers to deliver additional fuel if necessary
- A tap box provides the capability to hook up an additional diesel generator
- Building protected by a single UPS and a 900KW generator capable of carrying the load in the event of a failure of the 750KW generator
- Power distributed through eight PDUs
- Separate PDUs to protect against a single PDU or circuit breaker failure

Heating, ventilating and cooling (HVAC) units are air cooled, and so no cooling water pipes are located within the data center. Additionally, the current eight HVAC units provide sufficient redundancy that up to three could fail and the remaining units would maintain the data center within designed tolerances.

2.2.13.10 Network Diversity

WAN network connectivity has been designed with physical and logical diversity as a design goal. A minimum of four 1st tier Internet Service Providers have been selected to guarantee network and routing diversity in case one or two carriers experience problems. Physical diversity is realized by working with the local access provider(s) to ensure diverse physical routing of circuits was used where possible.

Local Area Network diversity is enabled through diverse pathing and employing routing and switching configurations that automatically detect failures and re-route packets transparently. The network is designed to exclude any single point of failure.

2.2.14 System Recovery Procedures (D.15.2.13)

As described in System Reliability Section of this document, the Global Registry will employ infrastructure and operational processes to mitigate the possibility of a crippling failure. However, there also are a variety of methods available to handle various system problems that might occur.

Business continuity and reliability are not after market products. They are designed into services and systems from the outset. The VeriSign Global Registry application of business continuity design elements, coupled with rigorous test and validation procedures, ensure that the critical services provided by the Global Registry, and the systems that support them, are sufficiently robust to mitigate the risk of potential business interruptions.

To support the scope of this section, registry services are separated into Critical Services and Non-critical Support Functions. The Registry Critical services are those required for the smooth operation of the Internet. They include:

- Domain Name Resolution Service
- Registration Service
- Whois Service
- Customer Service

Critical Services are defined as those services that directly support registrars and DNS resolution services available to all Internet users at large. Non-critical Support Functions are other processes for which the external impact of an outage would be minor or nonexistent.

Note: There are references in the System Recovery Procedures of a secondary site to support system recovery in the event of full or partial primary system failures. Although the primary VeriSign Global Registry site provides complete system and network redundancy to eliminate single points of failure, secondary site support is only available at an additional charge. Please work directly with your VeriSign Global Registry Services Business Development representative on pricing out this option.

2.2.14.1 Failure Scenarios

2.2.14.1.1 DNS Service Failures

Two types of failures can impact providing DNS services to the Internet at large:

1. Zone file generation failure
2. TLD server failure

Zone File Generation Failure

Full fail-over

A full fail-over means all processes are manually shifted in a *controlled* manner to operate on the secondary site. During a full fail-over, any zone-generation processes running at the primary site may be terminated (as necessary) to allow for the secondary site to take over these functions. Any zone files currently under construction are treated as unreliable and are discarded. If fail-over to the secondary site occurs while the zone-generation process is not running, no steps are necessary for the fail-over to occur.

Partial fail-over

A partial fail-over means all processes are shifted to operate on the secondary site in an *uncontrolled* manner. During a partial fail-over, terminating zone-generation processes running at the primary site may or may not be necessary.

If the zone-generation process is not running at the time at which fail-over to the secondary site occurs, no steps are necessary to fail-over zone generation. If, however, the fail-over occurred during zone file distribution, then the administrator will execute procedures to initiate the file distribution process to the sites affected.

Zone Data Corruption

Zone data is validated before it is placed in the registry database. If the data in the database has been corrupted, then the administrator will perform database-cleansing procedures. In addition, an attempt would be made to determine if the corrupted data has been propagated to the TLD servers. If it has, the administrator will follow procedures for reverting the TLD servers to a previous copy of the affected zone file(s).

Zone files are distributed within and outside the registry systems and their contents are validated at each step. If the validation ever disagrees with the master copy, then the replication is considered to have failed and the flawed copies are destroyed. If a host intrusion on the zone file tagging area or any of the root and TLD servers is detected, then the one(s) on the affected host(s) should be compared with the master copies on the zone generation machine inside the registry firewall. Standard Operating Procedures regarding the rollback of corrupt zone files on a root or TLD server should be followed to repair the damage.

TLD Server Failure

Hardware Failure

Various components at the TLD locations are configured in a high availability configuration. Should a redundant component fail, the “backup” component is designed take over automatically. If a specific hardware component is not redundant, RCC personnel will work with onsite personnel to isolate the problem. Once the failed component is found, RCC personnel will initiate procedures to replace or repair the defective component. Due to the “load balancing” nature of the DNS protocol, standard DNS processes dynamically accommodate any single TLD failure and a different TLD server would be utilized.

Name Server Application Software Failure

The RCC will constantly monitor the health of the TLD constellation to maintain performance and availability goals. Once an anomaly is detected by RCC management systems, RCC personnel to isolate the problem will initiate troubleshooting procedures. Name server log files on the TLD server and archived log files will be reviewed to determine the nature of the problem.

Once the problem is corrected, log files are reviewed and queries are performed against the server to verify proper operation. Depending on the size of the zone files being used, the name server application will resume operation within 2 to 20 minutes after a restart of the application has been initiated.

Corrupt Zone Data

Extensive procedures have been developed to ensure that zone data files located on the TLD servers are error-free. Some situations may occur where one or more zone files resident on the TLD server get corrupted accidentally or intentionally. Once a determination is made that a

current zone file is corrupt, RCC processes will be executed to restart the name server application using local copies of previously used zone files.

2.2.14.1.2 Registration Service Failure

The registration services is primarily supported by the Shared Registration System (SRS), which consists of a protocol and the associated hardware and software that permits multiple registrars to provide Internet domain-name registration services within the TLDs administered by the Registry.

A number of entities interface with the SRS, primarily registrars and Registry Customer Service Representatives (CSRs). Registrars access SRS through the Registry-Registrar Protocol (RRP) to register domain names and perform domain-name related functions such as the registration of name servers, renewal of registrations, deletions, transfers, and updates to domain names registered by that registrar. Registrars also have a web-based interface to access SRS to perform administrative functions, generate reports, perform global domain-name updates, and perform other self-service maintenance functions not available via RRP. The Global Registry provides support to the registrars for the SRS through the CSRs. The CSRs have a separate web-based interface to the registry systems, through which, after authenticating the registrar, they can query and perform updates per the registrar requests.

The SRS consists of the following components:

- RRPAG (Registrar-Registry Protocol Application Gateway)
- RRPAS (Registrar-Registry Protocol Application Server)
- Oracle Relational Database
- Assorted Batch Processes
- Dynamo/CSR Tool Server
- Registrar Tool Web Interface

The majority of disasters result in some sort of physical damage to the SRS hardware, facilities or communication channels; however, some of these disasters are less obvious in nature. For example, a denial of ser-vice of attack could adversely affect the performance of gateway servers, rendering them useless for the duration of the attack. A hacker could compromise security and subsequently jeopardize the integrity of the SRS data. A software virus could infect one of the production servers and adversely affect performance, or result in data corruption.

There are different levels of severity associated with each of the potential disaster scenarios. For example, a small flood may destroy only a small section of a data center, bringing down one set of components in the system. On the other hand, a severe flood could damage or destroy the entire building, resulting in a complete loss of the primary data center. The disaster recovery process that would be followed for the former case may differ from the process followed for the latter. After reviewing the potential failure scenarios carefully, there were four categories of failure:

1. Full Fail over
2. Partial Fail over
3. Non-Fail over
4. Business Reconstruction

Full fail-over

There are many types of failures that would result in a full, fail-over from the primary site to the secondary site. For example, if the primary site were unavailable to the registrars because of a fiber cut, then a full fail-over would be necessary. If the primary site data center was destroyed or rendered unserviceable as a result of a severe natural disaster (e.g. flood, tornado, earthquake, etc.), then a full fail-over would obviously be warranted.

Since the other secondary site components should all be in stand-by mode, they would not need to be reconfigured. All of the secondary site processes should be started. The registrars should be notified of this fail-over and instructed to use the secondary address(es) only to access the SRS.

Partial fail-over

Certain types of failures can occur which would be considered a disaster, but would not require a full fail-over to the secondary site. An example of this type of disaster would be some sort of primary site Oracle HA cluster failure. The servers themselves could be physically destroyed, or the power supply to the cluster could be interrupted indefinitely. Whatever the reason for the failure, a partial fail-over to the secondary would be required. A partial fail-over is when one or more components fail over to the secondary site, but a portion of the primary site remains operational.

Certain types of failures or disasters will not require a fail-over to the secondary site at all. If the hardware and physical network are still available, then it's probable that the failure is due to user behavior, a security breach, or a software issue of some sort. These types of failures would most likely affect both the primary and secondary site and should be directly rectified, if possible. For example, if performance of the system were degraded as a result of a denial of service attack, both the primary and secondary sites would be affected by the attack. In this situation a full or partial fail-over to the secondary site would not make any sense.

2.2.14.1.3 Whois Service Failures

Directory service consists of two major components: Whois servers and the Whois data extraction process.

The Whois daemon runs on each of several servers, accepts connections from a variety of clients, and accesses a local copy of the directory service database to answer these queries. The Whois data extraction process generates the directory service database from the Registry database.

Directory service is able to run at both the primary and secondary sites. Whois queries are load balanced to the directory-service servers across both sites. Also, the directory service process is run in test mode at the secondary site to verify functionality and accuracy in case site fail over is required.

Full fail-over

In full fail-over, the directory service is manually switched over from primary site to secondary site. Since Whois daemons on both the sites provide directory service, if all the daemons at one site fail, the daemons at the other site continue to provide the service. There is no fail-over required.

If the Whois file generation system becomes unavailable, the Whois file generation service is failed over to the secondary site and the Whois daemon servers are shut down on the primary site. The Whois file generation process on the secondary site is configured to run in production mode. It generates the Whois database, validates it and replicates it on Whois daemon servers on the secondary site only.

If the database becomes unavailable on the primary site, the Whois file generation process is disabled on the primary site. The Whois daemon servers are shut down on the primary site. Whois file generation process is enabled on the secondary site to run in production mode. It generates the Whois database, validates it and replicates it on Whois daemon servers on the secondary site only.

Uncontrolled fail-over

In an uncontrolled fail-over there is no opportunity to gracefully shut down the service on the primary site. In this scenario, the Whois daemon and Whois file generation both go out of service due to unforeseen circumstances. Disaster results in service being unavailable. In such a situation the ser-vice is manually enabled on the secondary site. The Whois file generation process is enabled on the secondary site to run in production mode. It generates the Whois database, validates it and replicates it on Whois daemon server on the secondary site only.

Non-fail-Over

Denial of service (DoS)

Directory service can also become unavailable because of a DoS attack. The Whois daemon has built-in defenses against DoS attacks. It is configured to block IP Addresses that send more than a pre-configured number of queries per second. Failing over to the secondary site is not a solution because directory service load is distributed across both the sites and hence both the sites are under this attack. Denials of service attacks are best solved at border router level. The offending IP Address is blocked at the border router itself. This saves the directory service resources from identifying the offending IP Address and blocking them.

If a hacker compromises the Whois daemon servers and the service is consequently unavailable, a full fail-over to the secondary site is initiated.

Data Corruption

If the Whois database at one of the Whois daemon servers is corrupted on the primary site or the secondary site, then that server is shut down, uncorrupted data copied over from the one of the other Whois daemon servers and the shut down server is brought up. If all the Whois daemon servers at one site have a corrupted database, all of the Whois daemons are shutdown; uncorrupted data is copied over from the other site and the shutdown servers are brought up. If all the Whois daemon servers at both the sites have corrupted database, all the Whois daemons on both the sites are shutdown. The Whois database is reverted to the previous days known good database and the Whois daemons are restarted. The Whois database is re-generated on the primary site. Once Whois database generation is complete it is replicated on Whois daemon servers on both the sides. All the Whois daemon servers on both the sites are restarted to refresh their data.

2.2.14.1.4 Customer Service System Failure

Customer Services provides the 24-hour technical support via telephone and e-mail. One-on-one support includes both general information and problem resolution. CSRs have their own Web-based tool (CSR Tool) for querying and modifying the database. This tool gives the CSRs the ability to query registration information at the request of the contacting registrar. CSRs with appropriate access levels can modify the registration information to correct errors made by the registrars. If a problem occurs that is beyond the scope of the CSRs to rectify, a well-defined escalation process is followed to alert appropriate Operations and Engineering personnel.

Impacts of Failures

The following scenarios address the system-level disaster recovery processes (tools and E-mail). There are two failure points in the systems: CSR web-server fail-over and underlying database fail-over. Along with the system fail-over decisions, the decision must be made whether to relocate the CSRs to the backup location, entailing rerouting of telephone communications.

Full fail-over

In full fail-over, it will be necessary to complete any write transactions (database modifications) in progress in the CSR tool. After the write trans-actions are complete, the next action depends on the area where the failure was detected:

- If the failure occurs in the CSR web servers, the underlying network routing mechanisms will automatically route further actions to the operational web servers.

- If the failure occurs in the underlying database, the web servers will have to be pointed to the secondary database.

- If the decision is made to relocate the CSRs, the CSRs will physically move to the secondary site and begin their operations at that site. No system changes are necessary.

Partial fail-over

For an uncontrolled fail-over, the process is the same as for a full fail-over, except that there is the possibility that transactions in progress have not completed successfully. Once the underlying systems have successfully failed over, the CSRs will have to query the database to determine if their last action was completed successfully (using the CSR Tool). At this point, it may be necessary for the CSRs to contact the customer to ensure that the data is correct.

Non-fail-over

Denial of service (DoS)

Since the CSR Tool operates on an internal network, it is not susceptible to many typical service interruptions (loss of communications lines, DoS attacks, etc.). For the identified areas of vulnerability, the actions are:

- *CSR Tool* –follow the process for uncontrolled fail-over.
- *Database* – follow the appropriate process for database fail-over.

Data Corruption

The CSRs are a resource that can determine data corruption (e.g., customer notices a failure in a registered domain or name server). However the CSR tools have no inherent capability of detecting or correcting data corruption. In the event of large-scale data corruption, the procedure to be followed would be the procedure for recovering the database.

2.2.14.2 Data Restoration

2.2.14.2.1 Data Recovery

To protect and recover data associated with critical services, the VeriSign Global Registry will employ a Synchronous Remote Data Facility (SRDF) product in conjunction with the Oracle Database Management System (DBMS). SRDF provides for significant operational flexibility in the following areas:

- *Disaster Recovery* – SRDF performs real-time data replication between the primary database and a backup database. Should the primary database system fail, a back-up database can be on-line within minutes.
- *Eliminating Back-up Window Constraints* – With SRDF, system backups can be performed without taking the database down.
- *Fast Restore* – Restoring data from the point-in-timeback-up is significantly faster than restoring from tape, stored on-site or off-site.
- *Scheduled Maintenance* – SRDF enables the Global Registry to implement the simplex (single site) mode.
- Disaster Recovery Testing – SRDF allows simultaneous recovery and data synchronization at the primary site.
- *The SRDF data* - synchronization process is highly effective supports six states of synchronization between the primary and disaster-recovery site.

2.2.14.2.2 TLD data restoration

Each TLD location maintains a tape backup of its system configuration in case of a hardware failure. If multiple name servers are present at the location, once the downed system has been repaired/replaced, it is rebuilt from system tapes. The zone data is either copied to the TLD server from the RCC or is transferred locally in the case of a multiple name server location.

TLD servers also keep backup copies of previous valid zone files in case the current zone file becomes corrupt or the application has problems using the current zone file. Restoration of name server operation will occur with the backup copies of the zone data until a valid current

2.2.14.3 Network Recovery

The network infrastructure (both WAN and LAN) is designed to isolate single-point failures with no interruption of services or degradation in performance. In most cases, isolation of failures is automatic and occurs within a few seconds of the event. Certain component failures (such as firewall failure) may require manual intervention to complete the fail-over.

The RCC will be proactively monitoring all equipment and WAN circuit activity at local Registry data centers as well as remote TLD sites to prevent outages. Once an outage occurs, the RCC will act immediately to isolate the problem and initiate actions to repair the problem.

2.2.14.3.1 Denial of Service Recovery

Denials of Service (DoS) attacks occur when one or more systems flood a network or individual services on that network with disruptive traffic. These attacks may come from many source addresses–a so-called distributed DoS attack–or from a single address. In either case, recovery options are limited and involve quenching the source of the attack either by filtering traffic at network routers or tracing the attack back to the origin and taking the originating server(s) off the network.

2.2.14.3.2 Security Breach Recovery

A security breach occurs when one or more systems are accessed (and potentially modified) by unauthorized personnel. Often such breaches occur via a network connection. Recovery from security breaches is straightforward, but is often consuming, and potentially disruptive to the services hosted on the affected systems. Certain security breaches may disable a service, for example Registration, for the duration of the recovery and cleanup activities. Following are some typical steps in recovering from a breach of security:

1. Identify affected systems and remove them from the network to pre-vent further damage
2. Identify mode of access (how the attacker gained access)–for example, account ID and password compromised or service exploited
3. Notify appropriate law-enforcement authorities of the event
4. Correct weaknesses exploited on all systems including those not breached
5. Collect and preserve evidence and other information for turnover to law enforcement
4. Cleanse affected systems by reformatting disks and re-installing operating system, software, and data from the most recent back-up prior to breach
5. Reconnect systems to network and restore services

2.2.14.4 Disaster Recovery Test Procedures

To be provided.

2.2.14.5 Redundancy/diversity (refer to D.15.2.11)

Please refer to Section 2.2.13 for information on system redundancy.

2.2.14.6 Staff (refer to D.15.2.14)

Please refer to Section 2.2.15 for information on VeriSign Global Registry personnel.

2.2.14.7 Reference to GAO DR Document

The VeriSign Global Registry as part of its Cooperative Agreement with the U.S. Department of Commerce (DoC) submitted a document extensively describing the scope of backup and recovery procedures available to protect the gTLD data and ensure uninterrupted operations of the Registry.

2.2.14.8 Facilities (refer to D.15.2.12)

Please refer to Sections 2.2.2.7 and 2.2.13 for information on facilities.

2.2.14.9 Process and Procedures (refer to D.15.2.11)

The VeriSign Global Registry maintains a four-tiered data storage architecture for production data that includes the following:

1. Primary on-line data and Critical Data Archive (CDA)
2. Periodic disk copies for quickly restoring production data and read-only and batch archives
3. On-site tape backup and archive
4. Off-site tape backup and archive

The primary on-line data is dynamic data that is created and maintained on a real-time basis as the Global Registry performs normal business operations. The dynamic data may change from as often as hundreds times a second to periodic ad-hoc changes. Full-copy disk mirroring protects most primary tier-1 online data. Critical Data Archive (CDA) is also a process for storing tier-1 data, but represents data that has been moved off of the production OLTP database for capacity reasons. Tier-2 data is less critical because it is copied periodically from the production systems.

Periodic, or tier-2, disk copies for several purposes. First, they serve as the backup for tier-1 data. Secondly, they provide the ability to execute read-only instructions and batch activities without impacting performance on the main production OLTP database.

Offsite, or tier-3, on-site backups and archives are stored in automated tape libraries. These tapes contain not only backups of data, but system configurations as well. Retention periods vary based on the nature and criticality of the data.

Offsite, or tier-4, tape backups and archives are copies of a subset of the on-site backups. There is nothing off-site that does not also exist on-site. Critical backups (for disaster recovery) and long retention archives are stored offsite.

2.2.14.10 Documentation

The VeriSign Global Registry are thoroughly documented in the following documents:

- Backup and Archive Policies
- Technical Operations Plan
- Technical Recovery Plan
- Tape Backup Procedures
- Off-Site Tape Storage Procedures

2.2.15 Registrar Technical Support (D15.2.14)

2.2.15.1 Customer Service

Customer Services provides 24-hour technical support via telephone and e-mail. One-on-one support includes both general information and problem resolution. CSRs have their own Web-based tool (CSR Tool) for querying and modifying the database. This tool gives the CSRs the

ability to query registration information at the request of the contacting registrar. CSRs with appropriate access levels can modify the registration information to correct errors made by the registrars. If a problem occurs that is beyond the scope of the CSRs to rectify, a well-defined escalation process is followed to alert appropriate Operations and Engineering personnel.

VeriSign Global Services contracts with a translation service to provide real-time translation for over 155 languages. When a call with a non-English speaking contact is made to Customer Service, the language translation service is conferenced in and the problem or issue addressed immediately.

2.2.15.2 Registry Command Center

The VeriSign Global Registry Command Center (RCC) provides 24x7x365 global systems monitoring and support. Automated systems monitoring tools and technology (See System Outage Prevention Section 2.2.13) continually assess the health and well being of servers, networks, and applications. This often enables the Command Center to detect and address anomalies before they result in service outages. Strong problem management and escalation procedures ensure that issues are identified, escalated and quickly resolved.

2.2.15.3 Registry Technical Operations

The VeriSign Global Registry Technical Operations staff provides 24x7x365 onsite or on-call support of all production systems operated by the VeriSign Global Registry. This includes the following operational systems management disciplines:

- Performance & Capacity Planning
- Data Center Planning & Management
- Deployment Planning & Execution
- Data & Systems Backup, Restore & Archive
- Business Continuity & Disaster Recovery
- Problem & Change Management
- Asset & Configuration Management
- Metrics Collection & Reporting

The Technical Operations staff is continuously on-site or on-call to address urgent problems and/or service degradation. Routine inquiries and requests (such as reports, metrics, etc.) are handled during standard business hours.

2.2.15.4 Remote TLD Site Technical Support

At each of the TLD sites, there are contractual arrangements in place for technical support at each remote site. This support includes 24x7x365 “smart hands” support from staff employed at the site as well as quick response by vendor field engineers.

2.2.15.5 Tools (CSR Registrar Tool, for Whois refer to 15.2.8)

The Global Registry provides web-based tools that are used by both the registrars and Registry Customer Support Representatives. Registrars can used the Registrar Tool to access domain name and name server status and availability information, update registrar information, and generate Registrar Daily Transaction and Weekly Snapshot Reports. The CSR Tool provides the ability to add, delete, or modify domain name and name server information.

Registrar Tool

The Registrar Tool site provides the registrars with access to registrar specific information about transactions with the Global Registry. It is accessed through the Global Registry web site and uses SSL as supported by version 4.0 and above of Netscape, Microsoft Internet Explorer and AOL browsers for securing the connection. The registrars can perform the following tasks with the tool:

- Domain Administration: The Manage Domains area provides the tools to administer domains by doing a Query on the status of a specific domain or a Check for the availability of a desired domain.
- Name Server Administration**:** The Manage Name Servers area provides tools to Query a name server or to determine the number of domains it hosts or Check a name server's availability.
- Registrar Administration**:** The Manage Registrar Information area provides tools to Query and update your registrar information and query, add, and update registrar contact information.
- Reports**:** The Reports area provides download capability for the Registrar Daily Transaction Reports and the Weekly Snapshot Reports.

CSR Tool

The CSR version of the tool provides all the above functionality, but has additional capabilities to allow the CSRs to access the database and make changes directly to the domain name and name server records. This real-time capability provides superior service by enabling the CSRs to address and resolve issues immediately. Following are the functions that can be performed by CSR's with the CSR Tool:

- Query, add, update, delete, transfer, renew, and purge a domain on behalf of the registrar
- Query, add, update, and delete a name server on behalf of the registrar
- Delete domain Credit
- Query, add, and update a registry user
- Update a registrar's credit
- Produce various reports
- Administer a registrar's account. This includes querying, adding, an updating registrar information, as well as querying, adding, updating registrar contact information.

The CSR tool will not allow CSRs to register new domain names on behalf of a registrar. Registrars must enter this information themselves.

To further empower the registrars, the Registrar Tool will be enhanced in the near future to provide all the functionality in the CSR Tool, except for the ability to add domain names.

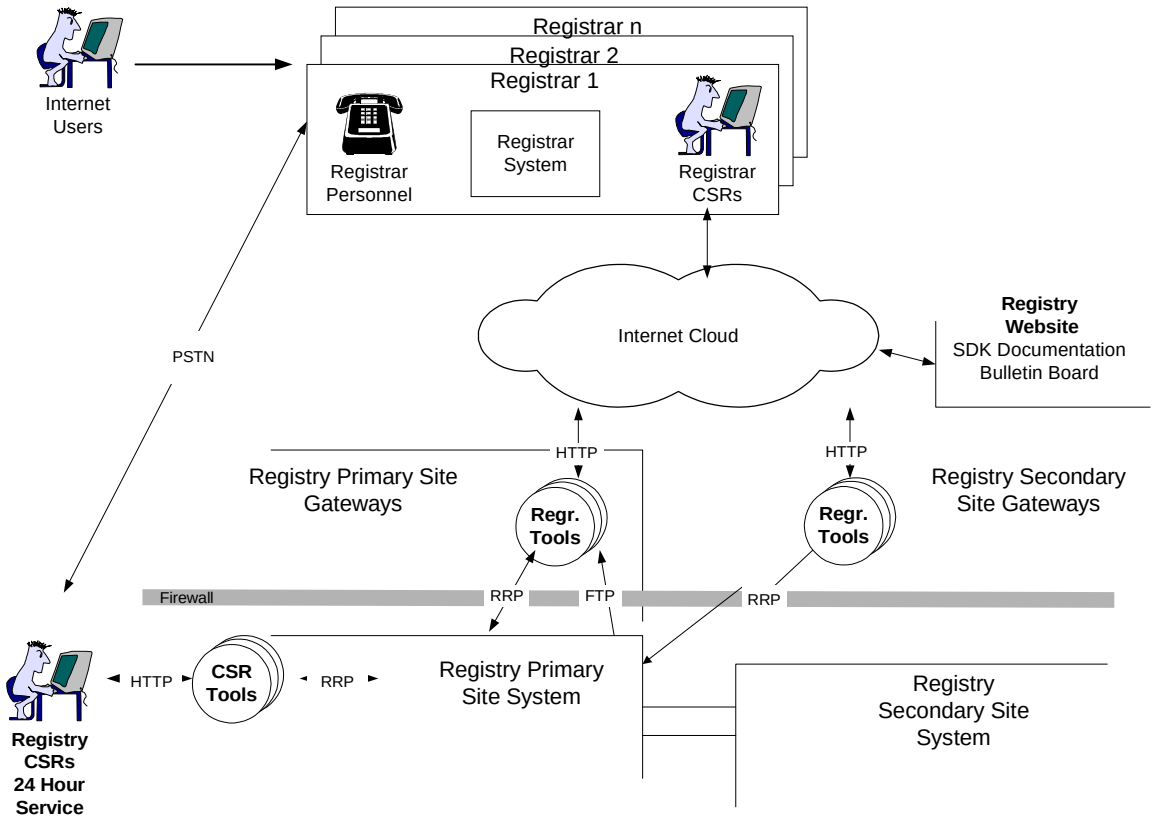

Figure 3 Customer Support Process Diagram

2.2.15.6 Personnel Accessibility

The Global Registry has multiple layers of personnel dedicated to ensuring the uninterrupted operation of the SRS, TLD, and other systems, and to provide registrar support around-the-clock. There are pre-established escalation procedures that ensure that the appropriate person can be contacted at all times to quickly and effectively deal with any issues that may arise. This includes 24x7x365 access to vendor support that includes significant on-site coverage to reduce mean time between failures. Phone, email, and pager support are all used at various points in the escalation process.

Resource	Registry On-Site	Contact
Customer Service Representatives	24x7x365	Phone, email
Technical Operations	24x7x365	Phone, email, pager
Engineering	8x5 plus 24x7x365 on-call	Phone, email, pager
Management	8x5 plus 24x7x365 on-call	Phone, email, pager
OEM Vendor Support	8x5 plus 24x7x365 on-call	Phone, email, pager

2.2.15.7 Operations Testing and Evaluation Support (OT&E)

The OT&E environment will provide a protected environment in which to validate the operability of prospective registrars. It will replicate the production software environment separate from all production data and operations and allows for debugging of interoperability issues. It also will be an ongoing test area for evaluating future system upgrades.

The OT&E process will ensure that a registrar's system is compatible with the Global Registry's systems. To participate in the process, the following steps will occur:

1. Registrar requests OT&E activation
2. Registrar tests their registration system in the OT&E environment
3. Registrar requests formal evaluation time during which they must demonstrate fully operational, well-behaved registration system
4. Registry evaluates results of the formal evaluation and either confirms successful completion or returns failure results; if failed, registrar fixes problems and returns to step 2
5. Registrar passes OT&E and is activated in the production environment.

The OT&E environment will have an RRP gateway outside a firewall. All other activities will be directed through the Registry Application and Database servers with other equipment added as needed. Initial capability will be hosted on multi-processor UNIX servers.

2.2.16 Non-Technical Registrar Support

2.2.16.1 Account Management

Account Management is responsible for maintaining and nurturing the relationship between the VeriSign Global Registry and the registrars (our clients). This team is dedicated to constantly interfacing with the registrars and providing feedback to the Global Registry regarding the level and quality of service. As often as possible, the Account Managers meet face-to-face with the registrars to discuss the relationship and explore ways to improve it.

2.2.16.2 Customer Affairs Office

The Customer Affairs staff is responsible for the contractual relationship with the registrars, and for support during the ramp-up process. They are also responsible for interpretation and compliance with ICANN guidelines, and communicate this information both internally and to the registrars.