TOP | THE .ORG TLD IS A PUBLIC TRUST | »

.org « A Joint Effort of the INTERNET MULTICASTING SERVICE and INTERNET SOFTWARE CONSORTIUM »

Transmittal »	FITNESS DISCLOSURE »
Proposal »	SUPPLEMENTARY MATERIALS »
Confidential Information »	DOCUMENT FORMATS »

.org Proposal Form

Executive Summary

This is a joint bid between the Internet Multicasting Service (IMS) and the Internet Software Consortium (ISC). We are both public benefit corporations with a long history of operating public works and creating freely available software for key infrastructure services on the Internet.

The .org Top Level Domain (TLD) is the home for the noncommercial organizations of the world, and we would operate the .org registry service as a public trust:

- We have designed a rock-solid service in strategic exchange points throughout the world. We will build this service on our existing infrastructure and operate a stable, high-performance, high-availability registry service for the .org TLD.
- We will operate this service with strong support for registrars, the registrants in the .org TLD, the general Internet community, ICANN, and our other constituencies.
- We will build on our deep familiarity with the subject area and our extensive experience in provisioning complex Internet services. We will provide a smooth transition with no break in service.
- The .org TLD registry service that will support all IETF recommended protocols. Our software, including packages for registry servers, registrar clients, Whois, namespace management, and secure DNS solutions will be freely available with no restrictions in source and binary form.
- We will work with our extensive network of partners throughout the world to provide substantial input to the standards process and advances in core technologies.
- We will work with our extensive network of partners around the world to differentiate .org make this TLD a home for the noncommercial organizations of the world.

IMS and ISC have provided important contributions to Internet infrastructure and have worked together closely for years. Our team is in place and builds on substantial past experience:

- We produce BIND, the software used to provide DNS service on the vast majority of key Internet servers.
- We operate the "F" root server and serve DNS for 21 TLDs.
- We have extensive experience with large, complex databases and were responsible for implementing and operating Internet databases from the ITU, the U.S. Patent and Trademark Office, and the U.S. Securities and Exchange Commission.
- We have built large global communities, such as the Internet 1996 World Exposition, a yearlong event that deployed over US$100m in in-kind contributions to enhance global Internet connectivity and stability. The Exposition included the participation of people from 85 countries and received over 5 million visitors from 130 countries.
- Our team is well known for advancing the state of the art in Internet services and applications, including tpc.int, HTCP, the DNS, and BEEP.

Revenue generated from the operation of the registry will first cover core operations, then service debt, and then fund public works projects for the benefit of .org registrants and core Internet infrastructure. No funds will be used for unrelated programs and we have no shareholders. An experienced board of directors, a public process, and extensive reporting will provide full accountability and transparency for the operation of this registry.

We will provide ICANN with tools that will spur greater competition in the marketplace for registry services and support innovation in related areas.

Table of Contents

1. General Information About the Applicant

TOC

?

C1. The first section of the .org Proposal (after the signed copy of this document) covers general information about the applicant. Please key your responses to the designators (C2, C3, C4, etc.) below.

C2. The full legal name, principal address, telephone and fax numbers, and e-mail address of the applicant, and the URL of its principal World Wide Web site.

Internet Multicasting Service, Inc.
P.O. Box 217
Stewarts Point, CA 95480
United States
Email: carl@media.org
Phone: +1.707.847.3720
Facsimile: +1.415.680.1556
URI: http://not.invisible.net/

Our partner in this application is:

Internet Software Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
United States
Email: paul@isc.org
Facsimile: +1.650.779.7055
Phone: +1.650.779.7000
URI: http://www.isc.org

? **C3.** A general description of the applicant's business and other activities.

The Internet Multicasting Service is a not-for-profit, public-benefit corporation that conceives and implements large public works projects and new services on the Internet for the benefit of the general public:

- As an independent initiative, IMS posted the full text of all U.S. Securities and Exchange public reports and ran the service for two years. At the conclusion of the two-year operation, IMS transitioned the service to the SEC, which operates it today as one of the U.S. government's busiest WWW and FTP services. IMS also ran a service with the full text of all U.S. Patents until the USPTO was able to get their own service up and running and currently maintains a 50-gigabyte public archive of U.S. government databases.
- IMS ran the first radio station on the Internet, including the operation of the first large-scale streaming and audio services on the net. The service provided 24-hour/day streaming content, including gateways from the U.S. Public Radio Satellite System and live feeds from the National Press Club and the floor of the U.S. Congress. IMS helped pioneer live broadcast production of events including an extensive presence at events such as Interop, INET, the IETF, the United Nations 50th Anniversary, and performances from arts venues such as the Kennedy Center and the Lincoln Center.
- IMS conceived and ran the Internet 1996 World Exposition, one of the first large global community events on the Internet. With partners in the Netherlands, Japan, and many other countries, the event involved thousands of people in the planning and implementation and included a full-time secretariat of 6 people coordinated by NIKHEF in Amsterdam. The world fair's infrastructure included the operation of the first international DS3-based Internet circuits, and required the deployment of over 2 terabytes of disk on machine clusters located in 8 countries.
- IMS has long provided program management for an advanced development program that has provided a steady stream of innovative ideas for the net. IMS coordinated the tpc.int project, the first public use of the Internet to carry telephony traffic on a large scale. IMS provides a home for the development of BEEP[34] and other emerging technologies.

The Internet Software Consortium is a not-for-profit, public-benefit corporation that produces core software and operates core infrastructure for the benefit of the general public:

- ISC produces BIND, the freely available software that is used to run most of the Domain Name System. BIND version 8 is mature production software used on most of the world's major computers including most of the Internet's root nameservers. BIND version 9 is new production software now shipped with several UNIX and LINUX distributions as the default enterprise nameserver application.
- ISC produces several other notable software packages, including the leading freely available DHCP implementation and INN, a complete freely available Usenet system.
- ISC runs the "F" Root Server and provides TLD DNS hosting for 19 ccTLDs, 3 legacy gTLDs, and the root.
- ISC provides hosting for the Lynx Web Browser, the NetBSD Foundation, the OpenLDAP Foundation, the IETF User Services Area, the XFree86 Project, and the Linux Kernel Archives.
- ISC sponsors the widely quoted Domain Name Survey.

From 1993 to 1997, ISC was under the fiscal sponsorship of the Internet Multicasting Service. ISC was incorporated in 1997 and began accepting funds in 1998.

? **C4.** The applicant's type of entity (e.g., corporation, partnership, etc.) and law (e.g., Denmark) under which it is organized. Please state whether the applicant is for-profit or non-profit. If it is non-profit, please provide a detailed statement of its mission.

The Internet Multicasting Service (IMS) is a Delaware Corporation (File 2335603) chartered in 1993. The Federal Employer ID of IMS is 52-1827912. IMS was classified as a 501(c)(3) non-profit in 1993 by the IRS and received a final 5-year 501(c)(3) ruling in 1998. IMS is registered in the State of California as corporation number C2369286 and has been granted exemption from state franchise and income taxes under section 23701(d) of the California Revenue and Taxation Code. IMS is a non-profit public benefit corporation and is not organized for the private gain of any person. The charter of the Internet Multicasting Service is "the creation and operation of public works on the global Internet computer network, including the creation and operation of new services, multimedia content and database, and network protocols for the benefit of the general public and the public Internet infrastructure."

The Internet Software Consortium is registered in the State of California as corporation number C2063422. ISC is a non-profit public benefit corporation and is not organized for the private gain of any person. The specific purpose of the ISC is "supporting the development of freely-available computer software programs which implement core Internet protocols and standards."

C5. Dun & Bradstreet D-U-N-S Number (if any) of the applicant.

The D-U-N-S Number for the Internet Multicasting Service is 82-508-2589.

The D-U-N-S Number for the Internet Software Consortium is 02-368-9651.

C6. The number of employees currently employed by the applicant.

IMS pays 3.5 Full Time Equivalent employees and has additional contractors and volunteers.

ISC pays 6.3 Full Time Equivalent employees and has additional contractors and volunteers.

C7. The applicant's total revenue (in US dollars) in the last-ended fiscal year.

IMS Total Revenues
(US Dollars)

Year	Amount
1993	$316,550
1994	$801,191
1995	$939,733
1996	$831,785
1997	$147,307
1998	$300,447
1999	$3,300
2000	$1,686
2001	$80,183
2002	$500,104 (YTD)

ISC Total Revenues
(US Dollars)

Year	Amount
1998	$629,684
1999	$1,724,715
2000	$684,614
2001	$1,301,141
2002	$68,208 (YTD)

C8. Full names and positions of (i) all directors, (ii) all officers, (iii) all relevant managers, and (iv) any persons or entities owning five percent or more of the applicant.

The directors of the Internet Multicasting Service are Rick Adams, Dave Farber, Carl Malamud, Rebecca Malamud, Marshall T. Rose, and Pindar Wong.

The officers of the Internet Multicasting Service are Carl Malamud and Rebecca Malamud. They will be the program managers for the .org program.

The directors of the Internet Software Consortium are Teus Hagen, Evi Nemeth, Paul Vixie, and Stephen Wolff.

The officers of the Internet Software Consortium are Paul Vixie, and Lynda McGinley. The program managers for the .org program will be Paul Vixie and Suzanne Woolf.

Neither IMS nor ISC have any stockholders. Both are public benefit corporations.

? **C9.** Provide the name, telephone and fax number, and e-mail address of person to contact for additional information regarding this application. If there are multiple people, please list all their names, telephone and fax numbers, and e-mail addresses and describe the areas as to which each should be contacted.

Carl Malamud (carl@media.org)
Internet Multicasting Service, Inc.
P.O. Box 217
Stewarts Point, CA 95480
United States
Phone: +1.707.847.3720
Facsimile: +1.415.680.1556
URI: http://not.invisible.net/

C10. Intentionally omitted.

2. Statement of Capabilities of the Applicant and Contracted Service Providers

TOC

? **C11.** As stated in the Criteria for Assessing Proposals, "ICANN's first priority is to preserve the stability of the Internet" and "ICANN will place significant emphasis on the demonstrated ability of the applicant or a member of the proposing team to operate a TLD registry of significant scale in a manner that provides affordable services with a high degree of service responsiveness and reliability." This section of the .org Proposal offers the applicant the opportunity to demonstrate its ability to operate the .org registry in that manner.

Throughout this document, operation of the .org registry, including providing all associated Registry Services, as defined in subsection 1.16 of the model .org Registry Agreement, is referred to as the "Registry Function."

2.1 [C12] Outsourcing

? **C12.** State whether the applicant intends to perform all aspects of the Registry Function, or whether the applicant intends to outsource some or all aspects of the Registry Function to other entities that will provide services or facilities under contract with the applicant. If any portion(s) of the services or facilities will be provided by another entity under contract, please describe which portion(s), state the time period during which they will be provided under contract, and identify what entity will be providing the services or facilities.

We will not outsource any of the functions listed above. To provide a single point of accountability for ICANN, the Internet Multicasting Service will serve as prime contractor. However, as evidenced in the attached Joint Statement of Authority, and by our long history of working together, this should be considered a joint bid between two established non-profit organizations.

2.2 [C13] Services and Facilities

? **C13.** Identify by name each entity other than the applicant that will provide any of the following:

- all services and facilities used to perform the Registry Function;
- any portion of the services and facilities used to perform the Registry Function accounting for 10% or more of overall costs of the Registry Function; or
- any portion of any of the services and facilities used to perform the following parts of the Registry Function accounting for 25% or more of overall costs of the part: database operation, zone file generation, zone file distribution and publication, billing and collection, data escrow and backup, customer (registrar) support, and Whois service.

Applicant will perform all functions. Note, however, [C18.5] Specific Cooperation Required from VeriSign

2.3 [C14] Scope and Terms of Contracts

? **C14.** For each entity identified in item C13, please state the scope and terms of the contract under which the facilities or services will be provided and attach documentary evidence that the entity has committed to enter into that contract.

As stated in [C13] Services and Facilities, applicant will perform all such functions.

2.4 [C15] Abilities of the Applicant

? **C15.** Describe in detail the abilities of the applicant and the entities identified in item C13 to operate a TLD registry of significant scale in a manner that provides affordable services with a high degree of service responsiveness and reliability. Your response should give specifics, including significant past or present achievements and activities of the applicant and the entities identified in item C13 that demonstrate the described abilities. It should also include information about key technical personnel (qualifications and experience), size of technical workforce, and access to systems development tools.

Our ability to operate a TLD registry of significant scale is based on:

- significant past experience operating critical infrastructure on the Internet. Our services operate with an extremely high degree of service responsiveness and reliability.
- our experience in coordinating large-scale community efforts and operating large-scale services with demanding requirements.

Specifically:

The services we build and operate require very high degrees of stability, performance, in a highly complex operating environment.

- We build and operate services at the center of the Internet. The "F" Root Server is operated with a high effective availability using proven clustering techniques and serves a peak of around 6,000 queries per second. We have been operating this service since 1993.
- We have significant operating experience inside of key exchange points (indeed our team has designed several of the most important exchange points). We understand routing, the DNS, and how to work with exchange points, transit providers, ISPs, large end nets, and all other elements of the core Internet infrastructure.
- We've worked with the most demanding database applications, including those with very high hit rates from the net. Our EDGAR and Patent databases were the largest WAIS databases on the net at the time. We have also built and run some of the largest XML-based databases in the world, including a full transformation of EDGAR into XML. Our experience working with very large databases spans 20 years, starting with the first Ingres relational databases and includes significant operational experience with current systems, including XML databases, full-text engines, and relational databases.
- We are experienced software developers who have produced numerous packages in widespread use on the net. Our BIND and DHCP packages are in use throughout the world in commercial and noncommercial organizations, spanning end-user to critical infrastructure applications. We produce well-documented, well-maintained, freely available code that is used by developers and operators throughout the world.
- We are intimately familiar with the DNS. In addition to running the "F" Root Server and hosting other TLDs, our team has made significant contributions to the evolution of the DNS and we understand how to work with all the other players that keep this global service running. We work on a daily basis with gTLD registries, registrars, ccTLDs, root server operators, transit providers, and corporate networks.

We are used to serving many constituencies. In addition to our experience working with software developers and operators around the world, we have worked with many kinds of communities and stakeholders.

- Even in rapidly changing regulatory environments, we keep the trains running on time. Our core focus is stability of Internet services. For example, even while the policy around U.S. government databases on the Internet was in great flux, there was no break in EDGAR service for users.
- Our software, such as BIND, is produced in a world where technology evolves rapidly as the standards bodies incorporate new ideas and operators accumulate real-world experiences. We actively participate in bodies such as the IETF, RIPE, WIDE, and NANOG and are able to keep production services operating with rock-solid stability, yet still have them evolve over time.

- Our team has significant operational experience working with ICANN, the IANA, the registrars, the registries, the IESG, and the IAB.
- Our team has significant operational experience running services for end users, particularly services that attract new end users. Our radio, government database, and world's fair services all brought the Internet to new classes of users. We will use our ability to create new and work within existing global communities to help differentiate the .org TLD.

Our team is well known for advancing the state of the art. We'll do that with the .org registry in particular and registries in general.

- For over 10 years, our team has worked together closely to bring new advances to the net, including the use of the public Internet for transmission of facsimiles and radio programs, access to government data, the production of live streaming events, and many other innovations.
- All of our past projects have been operational services, but we also understand that it is crucial to document what we do so that others can provide those services themselves. We are active participants in the standards-making process, and our team has published a large number of RFCs[19], Internet-Drafts[38], books[48], and web sites.[65] We will use those talents to help differentiate the .org TLD and to participate in a variety of standards efforts.
- Our Core Technologies Program will be used to spur innovation in this field. As part of this bid, we are also releasing two new Internet-Drafts in the field of namespace management, an effort directly relevant to the future of Whois services for end users and for core infrastructure functions such as the IANA.

Our program managers have held senior management positions with full responsibility for large organizations in industry, government and public service:

- We have a 10-year history of managing 501(c)(3) non-profits that provide public works projects on the Internet.
- We have held CEO, board-level, and senior management positions in industry.
- We have worked at ICANN, the IANA, and have held management positions in the IETF.
- Our experience working with U.S. government databases has made us very familiar with the policy making environment in Washington, and we have long experience working with policy bodies in the European Community, Asia, and other regions of the world, as well as with international bodies such as the ITU.
- Public services are in the public eye, and we have extensive experience in formulating messages that people can understand. We are very familiar in working in the media, on the net, and in person to explain what we do and listen to what people want.
- We have extensive experience with large, complex transitions. Our program managers helped transition legacy systems from organizations such as the SEC and the ITU onto the Internet. We also have experience transitioning our own services over to new organizations.

The Internet is a global network and our team our team has extensive international experience:

- We work closely with Internet coordination bodies around the world, including APNIC, RIPE, WIDE and many others.
- We are used to working with global communities of users, and will use those skills to make .org an attractive home for the noncommercial organizations of the world.
- Our bid anticipates placing service nodes in exchange points throughout the world. We have operated in these exchange points for many years and have the work experience and the personal relations to make our .org registry service a globally distributed service.

Our team has the experience and ability to operate as a public trust a rock-solid and responsive .org registry service. We will help differentiate .org, making it a home for noncommercial organizations. All of our work will be freely available, spurring innovation and competition in the registry and registrar markets.

3. Technical Plan (Including Transition Plan)

TOC

> ? **C16.** The third section of the .org Proposal is a description of your technical plan. This section must include a comprehensive, professional-quality technical plan that provides a full description of the proposed technical solution for transitioning and operating all aspects of the Registry Function. The topics listed below are representative of the type of subjects that will be covered in the technical plan section of the .org Proposal.
>
> **C17.** Technical plan for performing the Registry Function. This should present a comprehensive technical plan for performing the Registry Function. In addition to providing basic information concerning the proposed technical solution (with appropriate diagrams), this section offers the applicant an opportunity to demonstrate that it has carefully analyzed the technical requirements for performing the Registry Function. Factors that should be addressed in the technical plan include:

3.1 Summary

This technical plan for the design and implementation of the .org registry was constructed in accordance with the guidance provided by "gTLD Registry Best Practices" and the ".org Proposal Form". Additional detail required for implementation, but not requested specifically in the RFP has been separated from the main text for clarity, and is included in appendices.

The .org registry will initially be operated as a "thin" registry, but with a core registry schema that will accommodate both thin and thick registry models. We will implement a transition from the initial thin registry to a thick registry in conjunction with ICANN and the registrar community, as described in [C18] Transition Plan.

Our plan for initial deployment and transition of Shared Registration System (SRS) protocols is described in [C18] Transition Plan, and accommodates VeriSign's Extensible Provisioning Protocol (EPP) and Registry-Registrar Protocol (RPP) RRP deployment plans to ensure that the impact on gTLD registrars is minimized.

Software created to operate the registry, including software which provides RRP and EPP client and server functionality, will be released under an open-source license and will be made available for use by other registries and by registrars.

All services will be designed where possible to be provided multilingually in languages chosen to best serve the registrar community. A strong support structure for registrars and other interested parties is provided.

3.2 [C17.1] General Description of Proposed Facilities and Systems

> ? **C17.1.** General description of proposed facilities and systems. Address all locations of systems. Provide diagrams of all of the systems operating at each location. Address the specific types of systems being used, their capacity, and their interoperability, general availability, and level of security. Describe buildings, hardware, software systems, environmental equipment, Internet connectivity, etc.

We will operate the .org registry on a dedicated technical and support infrastructure, including new hardware, separate co-location and bandwidth contracts, and a dedicated technical staff of 10-12 professionals in customer support, systems administration, and software development. The technical plan makes extensive use of the team's expertise in the design, implementation, and operation of advanced server systems and networks, highly available public services such as the DNS, custom network applications, and advanced performance monitoring.

The central site, housing customer support, management, and software development activities, will be at ISC's primary location in Redwood City, California. This location has abundant suitable space at preferred rates, the local availability of excellent Internet connectivity, and close proximity to the San Francisco Bay Area talent pool of trained, experienced technical personnel. Improvements to the property, primarily in HVAC, electrical capacity, and telecom, will support our customer support center, development and other activities, with room to grow as needed for relatively low cost.

The production sites that will be supporting services for registrars and the public will be located at well-known, well-connected Internet co-location facilities. In the first year, two production sites in addition to the central site in Redwood City will support .org. As loads stabilize and DNS for .org is transitioned away from VeriSign's servers and towards ours, additional satellite installations will be deployed in other strategic locations to improve reachability and performance.

In recognition of the volatility of the co-location and bandwidth markets at this time, final determinations have not been made as to the locations of the production servers. A number of facilities would meet our requirements, which include highest quality security and reliability, ample space, low-latency and high bandwidth transit facilities, and the availability of many large, well-connected peering partners. Initial locations will be on east and west coasts of the United States, with additional facilities at suitable locations in Europe, Asia, South America, and Africa, with specific locations determined by the best connectivity for the largest number of users and customers.

The major production sites will consist of systems dedicated to public information services, to registrar services, and to database services, along with a redundant pair of servers supplying non-Internet access for "out-of- band" management of the servers, routers, and switches via modem and serial connection. The HP Alphaservers specified are well-known for speed, high capacity, and reliability, and the model specified, DS20L, are significantly over-provisioned for the anticipated loads (see [C17.10] Peak Capacities). Tru64 is a UNIX variant that has been in production use for highly available network services for many years and is interoperable with any standards-compliant UNIX and standards-compliant network service.

FIG 1 CONFIGURATION OF CORE PRODUCTION SITES

```
    ,---------------.                     ,--------------.
    | Database      |                     | Public        |
,---+    Server     +---------,  ,--------+    Server    |
|   +---------------+         |  |        +--------------+
|   | Database      |         |  |        | Public        |
| ,-+    Server     +-------, |  | ,------+    Server    |
| | `---------------'       | |  | |      `--------------'
| | ,---------------.       | |  | |
| | |  RAID         |       | |  | |      ,--------------.
| `-+    ARRAY      |       | |  | |      | Registrar    |
`---+               |       | |  | | ,----+    Server    |
    `---------------'       | |  | | |    +--------------+
                            | |  | | |    | Registrar    |
  ,---------------.         | |  | | | ,--+    Server    |
  | Mgmt station  |         | |  | | | |  `--------------'
  |               +-------, | |  | | | |
  +---------------+       | | |  | | | |
  | Mgmt station  +-----, | | |  | | | |
  |               |     | | | |  | | | |
  `---------------'  ,--+-+-+-+--+-+-+-+--.
                     |       Switch       |
                     +--------------------+
    ,---------------.                     ,--------------.
    | Database      |                     | Public        |
,---+    Server     +---------,  ,--------+    Server    |
|   +---------------+         |  |        +--------------+
|   | Database      |         |  |        | Public        |
| ,-+    Server     +-------, |  | ,------+    Server    |
| | `---------------'       | |  | |      `--------------'
| | ,---------------.       | |  | |
| | |  RAID         |       | |  | |      ,--------------.
| `-+    ARRAY      |       | |  | |      | Registrar    |
`---+               |       | |  | | ,----+    Server    |
    `---------------'       | |  | | |    +--------------+
                            | |  | | |    | Registrar    |
  ,---------------.         | |  | | | ,--+    Server    |
  | Mgmt station  |         | |  | | | |  `--------------'
  |               +-------, | |  | | | |
  +---------------+       | | |  | | | |
  | Mgmt station  +-----, | | |  | | | |
  |               |     | | | |  | | | |
  `---------------'  ,--+-+-+-+--+-+-+-+--.
                     |       Switch       |
                     +--------------------+
                     |       Switch       |
                     `-----+--------+-----'
                           |        |
                       ,---+--------+---.
                    ,--+     Router     |
                    |  +----------------+
      |   |      Router      +--,
      |   `-----------------'   |
      |                         |
      |                         |
     ################################
    #         Public Internet       ##
    #   (via provider switch fabric) ##
     ################################
```

NOTES

1. Some redundancy is removed for clarity. In particular, the switches are fully redundant and each component shown as wired into one is wired into both.
2. IP addressing and routing are not shown.
3. Equipment is expected to stack into one rack including space for cable management and air circulation.
4. Some specifics of out of band management stations are removed for clarity. Connectivity will include a modem for outside access and serial ports cabled to each major component.

High-availability features of the hardware specified include redundant power supplies, hot-swappable disk, redundant Ethernet ports with failover capabilities, dual connections from each server into fully redundant Ethernet switches, and dual connections from each switch into a fully redundant pair of routers configured for automatic failover between them. A dual power RAID5 store between the database servers provides for highly reliable disk capacity. The maintenance policy will provide for on-site spares for both disk and power supplies. In addition, we remove the chance that maintenance access to the installation could be cut off by a network failure of any kind by including a full "out-of-band management" kit of dedicated redundant servers. This provides the ability to dial in to the installation and reach any of the servers or network gear via a serial connection in the unlikely event that it's entirely unreachable via the network.

Support services specified to enhance the availability and reliability of each production installation includes support contracts on the hardware, "eyes and hands" contracts with the facilities where they are housed, and 24x7 on-call availability of server system and network specialists on staff.

Facilities for the production systems are specified as carrier-grade, including dual entrance for fiber providers, redundant power, high availability HVAC, and access control requiring biometric identification of visitors or escorted access.

Production software is specified as open source where possible, including well-known standards-compliant implementations of relational databases, DNS, systems monitoring and management, and secure access. Systems development will also be based on established open-source tools. (Additional detail on our software architecture and tools will be included in responses to follow.)

Network access is specified to include diverse Internet access from initial launch. The technical team's experience with the connectivity needs and strategies of ISPs have led to an architecture that makes extensive use of BGP peering with ISPs to improve reachability to far reaches of the Internet and to reduce the costs associated with paid transit.

3.2.1 Functional Specification

The .org registry has been designed and implemented using a component model, using documented and consistent APIs between modules which will allow individual components to undergo development, testing and upgrade with a substantial degree of independence from the system as a whole. This approach, combined with community review and participation through open-source licensing and publication of all components, will lead to an optimally stable and secure infrastructure.

3.2.1.1 Provision of Services

FIG 2 SOFTWARE ARCHITECTURE

```
                    ,--------------.                ,-------------.
                    | IXFR, TSIG   +----------------+ IXFR, TSIG  |
                    +--------------+                +-------------+
                    |  Zone File   |                | Auth Name-  |
                    |  Generation  |                |  servers    |
                    +--------------+                +-------------+
                    | dbase access |                |    DNS      |
                    `------+-------'                `-------------'
                           |
                    ,------+-------.                   ,--------------.
                    |   Registry   +-------------------+ dbase access |
        ,-----------+   Database   +-------------.     +--------------+
        |           |              +-------.      \    | transaction  |
        |           `------+-------'       |       \   |   engine     |
        |                  |               |        \  `----+---+-----'
,-------+-------. ,-------+------. ,-------+------.  \      |   |
| dbase access  | | dbase access | | dbase access | ,-+-----+---+---.
+---------------+ +--------------+ +--------------+ | dbase | trans  |
| Query Service | | Web Services | | Notification | +---------------+
+---------------+ +--------------+ |   Engine     | |      SRS      |
|     Whois     | |  HTTP, HTTPS | +--------------+ `---------------'
`---------------' `--------------' |     SMTP     |
                                   `--------------'
```

NOTES

1. All registry data is stored in the registry database; transactions will not complete until positive confirmation of data commit has been obtained.
2. The database access component provides a consistent access API to the registry database. Maintaining a clean functional boundary between the access layer and applications which need to manipulate data in the registry allows flexibility in the choice of database, which in turn makes the registry more scaleable.
3. The Whois component accepts Whois queries from clients, and performs read-only queries against the database in order to obtain data to return to clients. The Whois component will dynamically limit useful responses supplied to clients that present excessive query loads.
4. The transaction engine processes requests that might effect changes in the registry database, in response to instructions received from the SRS components. A common interface layer is provided for the various SRS components to send requests to the transaction engine.
5. The SRS components accept requests from clients over appropriate interactive transport protocols, and translates SRS-specific dialogues into interactions with the transaction engine. We expect the supported set of SRS protocols to include RRP and EPP, as described in [C18] Transition Plan. Where message-passing provisions are provided in the SRS protocol, the database access component will be used to provide access to SRS components to the registry (e.g. the EPP <poll> command; see Message Passing to Registrars.)
6. Two web applications require access to the registry data:
    - Public Whois-type registry query tool.
    - Registrar portal.

   Other applications may be developed which use the common web services framework.
7. Zone file generation is described in [C17.4] Zone File Generation.
8. Certain registry operations require the registry to send notifications to clients that are not associated with a client-initiated transaction request. The notification engine polls for such notifications in the database, and performs appropriate actions. E-mail is the initial notification mechanism supported (see Message Passing to Registrars).

3.2.1.2 Transaction Security

Periodic database dumps stored according to the general backup and data security policy will allow reconstruction of the registry database to be performed in the event of catastrophic failure. Additional facilities have been implemented to ensure that transactions performed against the database following a database dump can also be preserved, providing a mechanism to facilitate complete disaster recovery.

FIG 3 TRANSACTION SECURITY

```
,--------------.
| dbase access |
+--------------+      ,-------------.
| Transaction  +------+ Transaction |
|    Engine    |      |     Log     |
`--------------'      `-------------'
```

NOTES

1. A simple, flat, textual log of every transaction processed by the Transaction Engine is maintained, such that all transactions successfully committed through the Database Access component are recorded. The Transaction Log will provide transaction security and, together with periodic database dumps, will allow accurate reconstruction of arbitrary snapshots of the registry database.
2. The transaction log is deliberately implemented separately from the database and the database access components in order to safeguard against systematic defects in either of those modules.

3.2.1.3 Active Service Monitoring

FIG 4 ACTIVE SERVICE MONITORING

```
                                                       | Auth Name-   |
                                     | Web Services |  |   servers    |
                                     +--------------+  +--------------+
|     Whois     |  | RRP |  | EPP |  |  HTTP, HTTPS |  |     DNS      |
`-------+-------'  `--+--'  `--+--'  `-------+------'  `------+-------'
        |             |        |             |               |
,-------+--------+----+---+----+---+---------+-------+--------+------.
|     Whois      |  RRP   |   EPP  |  HTTP, HTTPS    |      DNS      |
+----------------+--------+--------+-----------------+---------------+
|                                                                    |
|                 Service Consistency and Test Engine                |
|                                                                    |
+----------------+                                   ,---------------+
|     Syslog     |                                   |  IXFR, TSIG   |
`-------+--------+-----------------------------------+-------+-------'
        |                                                    |
,-------+--------.                                   ,-------+-------.
|     Syslog     |                                   |  IXFR, TSIG   |
+----------------+                                   +---------------+
| Event Handler  |                                   |   Zone File   |
                                                     |   Generation  |
```

NOTES

1. The Service Consistency and Test Engine component performs a set of test actions against each supported service, and validates the success of the actions and the results of the action, where appropriate. The services under test are live, production services.

3.2.1.4 Event Monitoring

FIG 5 EVENT MONITORING

```
                    ,----------------.
                    |    Service     |
,----------------.  |  Consistency   |  ,----------------.
| Platform Logs  |  | & Test Engine  |  | Service Logs   |
+----------------+  +----------------+  +----------------+
|    Syslog      |  |    Syslog      |  |    Syslog      |
`-------+--------'  `-------+--------'  `-------+--------'
        |                   |                   |
        |           ,-------+--------.          |
        `-----------+    Syslog      +----------'
                    +----------------+
        ,-----------+ Event Handler  |
        |           `-------+--------'
        |                   |
,-------+--------.  ,-------+--------.  ,----------------.
| Event Storage  |  |   Real-Time    +--+  Engineering   |
`----------------'  |   Monitoring   |  |  Escalation    |
                    `----------------'  `----------------'
```

NOTES

1. The event handler is a multiplexer, and distributes incoming event data to one or more event processors.
2. All events are stored for future reference.
3. The real-time monitoring component provides some correlation and summarization of incoming event data.
4. Certain events or combinations of events will cause the real-time monitoring component to perform automatic issue escalation, to allow proactive problem resolution.

3.3 [C17.2] Registry-Registrar Model and Protocol

3.3.1 General Approach

? **C17.2.** Registry-registrar model and protocol. Please describe in detail, including a full (to the extent feasible) statement of the proposed RRP and EPP implementations. See also item C22 below.

The principal guiding objective for the design of initial registry-registrar interactions is that the transition from the VeriSign .org registry to our registry should be as simple as possible for registrars to accommodate, and hence that changes in registrar systems should be reduced to the smallest set possible. For this reason the initial registry-registrar model and interface specification has been made as similar as possible to that currently operated by VeriSign.

The initial interfaces provided to registrars for manipulation of the .org registry will be the RRP[1], with a planned transition to EPP[14] as described in [C18] Transition Plan.

The initial live set of data incorporated into the registry will similarly match that maintained by the VeriSign registry. This implies a "thin" registry model.

The registry schema (see [C17.3] Database Capabilities, will support the superset of requirements of the existing VeriSign registry data set, those requirements imposed by RRP and EPP ([14], [15], [16] and [17]), and the requirements of a thick (contact-populated) register.

A managed, gradual transition from a thin registry to a thick registry (one in which contact information is stored in the register) will be carried out as described in [C18] Transition Plan.

3.3.2 RRP Implementation

We are prepared to go live with an implementation of RRP that will satisfy all the mandatory requirements specified in [1]. However, we will also require VeriSign to disclose details of their live, production SRS infrastructure in such a way that our initial SRS implementation will conform as closely as possible to that used by existing VeriSign registrars.

Registrars may perform the following registration service procedures using RRP to communicate with the .org registry:

- 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 nameservers 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 nameserver has been registered.
- Register a nameserver.
- Update the IP addresses of a nameserver.
- Delete a nameserver.
- Examine the status of nameservers that the registrar has registered.

This is the complete set of operations defined in RRP 1.1.0.

The WFR (waiting for authentication retry) and WFC (waiting for command) states in the RRP state machine will include timeouts, which will be specified in documentation made available to registrars. The RRP server will disconnect from the client if the specified timeout in WFR or WFC is exceeded.

The RRP implementation will allow specification of nameservers associated with other top-level domains for .org registration.

The RRP implementation will support a default initial registration period for domains, which will be used in the event that the registration period is not specified in a request to register a domain. This period, together with the range of acceptable values for a specified registration period will be specified in documentation made available to registrars.

The .org registry will notify a potential losing registrar when another registrar has made a transfer request. See Message Passing to Registrars for a description of message passing from the .org registry to registrars.

The .org registry may automatically approve transfers on behalf of potential losing registrars ("default approval") when the potential losing registrar fails to acknowledge the transfer request with an RRP transfer approval or rejection command within a certain time period. The time period used will be specified in documentation made available to registrars.

3.3.3 EPP Implementation

We are prepared to deploy an EPP service will satisfy all the mandatory requirements specified in [14], [15], [16], and [18]. Object service availability will initially be limited to domain names [15], and hosts [16], in accordance with the "thin" register model. As described in RRP Implementation for RRP, specific details of our deployment of EPP in phase II of our transition plan will be made available following advice from VeriSign on their EPP deployment plans, so as to minimize the Operational Test & Evaluation (OT&E) and systems implementation burdens for .org registrars.

3.3.4 Message Passing to Registrars

It is sometimes necessary for the registry systems to send messages to registrar systems, for example to notify a potential losing registrar of a transfer request. It is not possible to send these messages using RRP.

The .org registry will support the following message-passing mechanisms:

- Plain-text e-mail, in a near-identical format to those currently sent by VeriSign (see Registry/Registrar E-Mail Templates for format specifications).
- A summary archive, accessible via HTTPS and SCP, which include details of the date stamps and content of all messages passed from the registry to the registrar in the preceding calendar month.

- The EPP <poll> command, once EPP is deployed (see + [C18] Transition Plan).

3.3.5 Registrar Portal

The .org registry will provide an authenticated portal, accessible over HTTPS, to registrars. This portal will provide:

- Access to relevant documentation.
- Access to support information.
- The ability to customize the individual registry-registrar interface, such as specifying a message-passing mechanism and viewing message history (see Message Passing to Registrars).
- The ability to view a transaction log specific to the registrar's interaction with the registry.
- The ability to update the registrar's contact information.
- The ability for a registrar to manage, and delete domains; initiate and approve transfers, process renewals, create and update nameservers. The portal will not allow for domain creation, domains may only be created via the supported protocols.
- The ability to retrieve daily, and monthly reports.

3.4 [C17.3] Database Capabilities

? **C17.3.** Database capabilities. Database size, throughput, scalability, procedures for object creation, editing, and deletion, change notifications, registrar transfer procedures, grace period implementation, reporting capabilities, etc.

The database schema for the register accommodates the superset of requirements imposed by the VeriSign register inherited at transition, RRP, EPP, a thin (contact-free) register and a thick (contact-populated) register model.

The registry database will be implemented on an RDBMS platform which is SQL-capable, and supports real-time replication between diverse registry sites, row-level locking, transaction rollback, ACID semantics, ANSI SQL support, Unicode support, triggers, stored procedures, and hot backup. The provision of a database access layer across the registry components will allow a registry based on our software to be built around a variety of different database products and on different operating platforms.

Database Size

- The RAID5 array will be initially sized at 200 Gbytes, which we estimate to be roughly 40 times larger than necessary to store the present .org database and all associated meta data.

Throughput

- The capacity in number of transactions per second of a database is related to the hardware and software platform where the database resides. The two protocols we propose to use, RRP and EPP, have very different styles of transactions; however they both result in similar database transactions. Our estimates of a reasonable capacity for the database from our operational experience in building OLTP systems are:
    - Query Transactions: 1,000,000/day
    - Write Transactions: 5,000,000/day
    - Check Transactions: 9,000,000/day

Scalability

- We have provisioned the hardware and database disk space capacity to handle 20% growth over each of the next 5 years and still use less than 10% of available resources. Should we find a need to extend the size of the database, the file system and SQL database can be extended to span new storage as needed.

Procedures for Object Creation, Editing, and Deletion

- All object operations will be performed through the protocols served by the front-end protocol servers, i.e., RRP or EPP for registrars. Customer Support will have the capability through a management console to assist customers with previously encountered problems and questions, such as a request to revive a mistakenly deleted domain name.
- All operations are logged. Operations through a management console require privileged access and second sign-on verification code through the use of a Supervisor or Manager PIN code.
- Engineering may have special access to the database for unique one-time operations that may be applied through direct SQL manipulation. An example of one of these circumstances is when a registrar is purchased by another registrar and 50,000 domains must be transferred from one registrar ID to another. Such a

transaction would be handled by engineering through direct database manipulation. All one-time engineering modifications will be tested in a mirrored test environment before any bulk changes are applied to the production system.

Change Notifications

- Reports of all changes to objects managed by a registrar will be made available to the registrar through daily and monthly reports.

Registrar Transfer Procedures

- There are multiple sets of transfer procedures, depending on the SRS protocol being used. Transfer procedures associated with different SRS protocols support different capabilities, but efforts will be made to establish transfer procedures and policies such that any available SRS protocol will provide registrars with full functionality. See [C18] Transition Plan for SRS protocol transition plans.

Grace Period Implementation

- In the application of grace periods we will implement policy that favors the registrar not the Registry in areas that effect the financial requirements for monies on account with the registry.
- When domains are about to auto renew a 45-day grace period is applied to the debit to the registrars account. We will apply the debit for the domain at the time the domain is renewed or at the end of the 45-day auto renew grace period.
- A 5-day grace period applies to newly created domains. If the domain is deleted within 5 days the registrar is credited for the deleted domain. There are several proposals dealing with Domain Deletion and revival policies developed by ICANN. We will implement what is decided in this policy area.
- The registry will enforce a 60-day waiting period before a newly created domain can be transferred from one registrar to another.

Reporting Capabilities. The following reports will be made available to each active registrar through the web portal (via the HTTPS protocol) and via SFTP or SCP. The reports will use XML for their format.

- The Domains Report will list all domains currently associated with the registrar and all relevant Domain related fields such as Domain Status, Nameservers, and, when relevant, contacts.
- The Nameservers report will list all associated nameservers with a domain and the corresponding IP Addresses. It will also list any orphaned A records.
- The Contacts report will list any orphaned Contacts.
- The Transfers report will list all incoming and outgoing transfers and their current status.
- The Transaction report will list the daily transactions and the object they were applied to.

3.5 [C17.4] Zone File Generation

> ? **C17.4.** Zone file generation. Procedures for changes, editing by registrars, updates. Address frequency, security, process, interface, user authentication, logging, data back-up.

These procedures may not be fully implemented until we have full control of authoritative nameservers for .org. For notes on compatibility with VeriSign's procedures, see below and [C17.5] Zone File Distribution and Publication. "Zone data" in this context can refer to the full set of zone data or to data offered as an incremental update, in accordance with documented DNS standards for each.

We intend to maintain a 5-minute update frequency for any given change 95% of the time. Additionally, at least once a week a full zone file will be generated and loaded onto our servers. At least once a day we will verify that the incremental changes and a full extract of zone data match.

A companion report will explicitly flag all changes as adds, drops, or modifications to aid systems support staff in spotting unusual patterns of activity.

The generated .org zone file will include the following resource records:

- A single SOA record.
- A number of NS and A records, up to a maximum of 13 each, for the authoritative, public DNS servers for .org.
- One NS record for each unique (domain, nameserver) tuple, for domains with associated status values of ACTIVE, LOCK, CLIENT-LOCK and PENDING-TRANSFER.
- One A record for each required glue record. We will implement, on a reasonable schedule, glue-generation and

pruning criteria specified by ICANN.

The incremental update to the zone will be generated by extracting from the database, at each zone update cycle, the zone data that has changed in the database since the last such cycle. The zone data thus generated from database changes will be checked against expected activity, with large changes in size or content (more than 2% change in total size or in the contents of more than 0.1% of the total delegations) to be flagged and the automatic process halted until review of the cause of the discrepancy can be performed by senior level systems staff.

Our expectations of normal activity in this zone are based upon previous experience with other critical DNS zones. During the prelaunch phase we expect that daily examination of the activity actually occurring in .org will allow us to considerably refine these expectations and our reporting thresholds.

Once the zone data has been generated, signed, and passed the automatic integrity checks, it will be loaded onto a non-public nameserver for a final verification pass. The availability of the zone for transfers and queries will be verified at this time.

When the test-load of the zone has been verified, it will be transferred to the published master. This system will not be a publicly known server and will not be used to resolve public queries against the .org zone. It will be a configuration usually described as a "hidden primary" or "distribution master", in which the only nameservers that can reach it are those configured as slaves for the .org zone and the only work it will do is the transfer of the zone to those appropriately configured slaves.

This configuration is operationally indifferent between the use of VeriSign's nameservers, the use of our nameservers, and the use of third parties for publication of the .org zone. All that is required is access control coordination between the operators so that all slaves have permission to gather the zone from the master (see note below on TSIG). However, our turnaround times are based on the ability to do DNS IXFR as the update mechanism; full zone transfer will be dramatically slower.

The NOTIFY extension to the DNS will be used to speed convergence between a new copy of the zone at the registry and that cached on the slaves.

It is extremely unlikely but not impossible that a seriously damaged version of the zone will pass the integrity checks and be loaded into publicly available slaves. Monitoring of both helpdesk activity and the operation of the slave nameservers, including regular automated tests of the availability and integrity of the zone on the slaves, will assist in identifying this should it ever occur. The recovery procedure includes:

1. Regenerate the previous, operationally acceptable version of the zone with a new serial number.
2. Force the normal update process with the newly revised zone, by manual intervention of a senior systems staff member.
3. Verify receipt of the recovered zone by the slaves as soon as practical.
4. Examine and resolve problems with the broken zone.

This would not allow for a perfect recovery because bad data may still be cached elsewhere among clients in the net. There is no way for the registry to prevent this owing to the way DNS works. However, it can be mitigated by fast detection of a flawed zone, fast action to back out the newest set of updates, and fast convergence among the slaves on the reversion to the old zone data under a new serial number.

3.5.1 A Note on TSIG and DNSSEC

A critical component of our strategy for operating .org is the ability to sign the zone in accordance with the protocol extensions documented in RFC 2535[2] and RFC 2845[33]. This commitment is undertaken both in the belief that this technology is critical to the future usefulness of the DNS and in accordance with our commitment to furthering the development of Internet technology through implementation and test. We have to date contributed heavily to the development of these protocol extensions, from protocol design to implementation and interoperability test activities.

The TSIG component of the DNS security standards has been stable for some time now and is beginning to see significant use among DNS operators. It is used to sign zone transfers between nameservers and we anticipate being able to use it to sign transfers of .org to slave servers at the launch of our service.

TSIG requires the use of a "shared secret" key and good time synchronization between servers, which in turn imposes a requirement for a basic level of coordination between separate operators for the same zone. We do not anticipate a problem in reaching an agreement with VeriSign, in accordance with their current practices and those of other registries, for the management of TSIG keys during the period in which their nameservers will be part of the authoritative server set for .org.

DNSSEC standardization for data signatures is incomplete, as the technology remains subject to the usual cycles of protocol refinement, implementation, test, and protocol tweaking. A critical phase of prelaunch will be to finalize our processes for signing the .org zone around the current state of standardization and implementation at that time. The process will include:

- A process for managing the relationship between the .org registry and its delegated zones regarding information exchange. A large remaining area of uncertainty in the final standardization of DNSSEC surrounds the specifics of a parent signing a delegation as unsecured or signing a reference to a child's zone key. We will in this area implement the current technology as consistent with other constraints, including interoperability with existing client DNS software and the performance limitations inherent in the current standard on the time it takes to sign a zone and the size of the resulting signed zone. We will also contribute code and developer time to the ongoing effort to implement, test, and refine the standard.
- Generation and propagation of keys for the .org zone.
- Cooperation with other registries and interested parties in developing Best Practices and operational documentation for registrars and ISPs on how to use zone signatures for delegations in .org. Such documentation is within the charter of the IETF DNSOP WG and will be offered accordingly.
- Development of key management procedures for the zone keys for .org, including publication, rollover, and access control. There is little available experience or guidance as yet in the community for balancing security, scalability, and operations concerns in such areas as determining the proper intervals for key rollover. We are uniquely positioned to contribute code, procedures, and experience in this area.

3.6 [C17.5] Zone File Distribution and Publication

? **C17.5.** Zone file distribution and publication. Locations of nameservers, procedures for and means of distributing zone files to them. If you propose to employ the VeriSign global resolution and distribution facilities described in subsection 5.1.5 of the current .org registry agreement, please provide details of this aspect of your proposal.

Transfers of zone data will be performed via a zone transfer from the "hidden primary" nameserver (see [C17.4] Zone File Generation) once the change report has been generated from the database, transformed into zone data format, and passed the required integrity checks. Transaction signatures (TSIG) will be supported as described in A Note on TSIG and DNSSEC.

As noted, our zone data generation and publication procedure as described in [C17.4] Zone File Generation is intended to be indifferent among slaves for the zone that are ISC's nameservers, VeriSign's nameservers, or some other third party's nameservers as long as they interoperate with DNS standards.

According to existing provisions in other ICANN registry contracts, including the one with VeriSign for .org, the registry is required to make the full zone file available under appropriate contractual restrictions to other parties. Such parties at this time are estimated to number in the hundreds. In order to meet this obligation without risking any impact to the operation of the authoritative nameservers for ORG, the complete zone file will be available by AXFR (as restricted by an access control list) or ftp (as restricted by a login and password) on a separate machine to any such parties who may wish to enter into an agreement with the registry for access to the data.

3.7 [C17.6] Billing and Collection Systems

? **C17.6.** Billing and collection systems. Technical characteristics, system security, accessibility.

Our billing and collection systems are fully automated and fully secured. We performed the first electronic commerce transaction on the Internet in 1994 and have extensive experience with these systems.

Communication with registrars is available through the use of secure electronic mail or secure sessions via the World Wide Web. Identity is established during the signing of the initial registry-registrar contract. Our systems use SSL to provide secure communication on the Web with identity established using the Thawte Certification Authority.

Registrars may make deposits into their accounts through all standard electronic funds transfer mechanisms, including bank drafts, ACH or SWIFT transfers, and using American Express, Discover, MasterCard, and Visa bank cards. Registrars may also send us a check payable in U.S. dollars, such amount being credited immediately upon clearance.

Once funds have cleared, a real-time system works with the core registry system to maintain a real-time account balance. Registrars will be able to use a secure web-based system to monitor the status of their account, including a variety of reports on registration and payment activity. Written statements will be dispatched by electronic mail at the option of the registrar.

SRS events that require financial transactions against a registrar account will be passed to a billing system as transactions to a General Ledger. The API of this software is the OMG's specification for a General Ledger Version 1.0.

Each registrar is required to provide funds as pre-payment for transactions such as registrations, renewals, and transfers. After each transaction the registrar's account is updated appropriately. If a registrar should fall below their balance and has no other credit instrument available, the registrar's account will be barred from processing billable RRP events.

Registrars may set a low water mark for their account. If their account reaches this threshold, email will be generated and sent to their billing contact warning them of their situation. If a registrar were to cross the low water mark for their account a phone call will be made to the registrar's billing contact to discuss their account. All attempts will be made to assist the registrar in understanding the situation and their accounts before a registrar is shut down for cause.

Under no circumstances will the registry extend credit to a registrar. No surety bond is required for registrars, but standard indemnification provisions and insurance requirements will apply.

3.8 [C17.7] Data Escrow and Backup

3.8.1 Requirements

? **C17.7.** Data escrow and backup. Frequency and procedures for backup of data. Describe hardware and systems used, data format, identity of escrow agents, procedures for retrieval of data/rebuild of database, etc.

3.8.2 Data Escrow Schedule, Content, Format and Procedure

3.8.2.1 Schedule

The Registry Operator will prepare:

1. Full data sets for one day of each week (the day to be designated by ICANN).
2. Incremental data sets for all seven days of each week.

Full and incremental data sets will be up-to-date and coherent as of 1200 UTC on the day to which they relate. Until a different day is designated by ICANN, the full data sets will be prepared on Sunday.

3.8.2.2 File Naming

Files will be prepared as XML documents adhering to Escrow Data Format. Each XML document will be placed in a file named according to the following convention:

Full data sets:

> "ORG-CCYYMMDD.full", where CCYYMMDD is constructed from the date (CC=century, YY=last two digits of year, MM=number of month, with January numbered 01, DD=day of month; in all cases a single-digit number should be left-padded with a zero).

Incremental data sets:

> "ORG-CCYYMMDD.inc", where CCYYMMDD is constructed as above.

3.8.2.3 Escrow Deposit Specification

The escrow data sets will contain Nameserver, Registrar, and Domain objects.

The domain object, which corresponds to a registered second-level domain under ORG, consists of the following elements:

- Domain ID (registry-assigned)
- Fully-qualified domain name
- Registrar ID (IANA-assigned)
- Domain status

- Nameservers
- Registration date
- Expiration date
- Last updated date
- Last transfer date

The nameserver object, which corresponds to a single registered nameserver, consists of the following elements:

- Nameserver ID (registry-assigned)
- Fully-qualified domain name of the nameserver
- Nameserver status
- Association status
- List of IP addresses associated with the nameserver
- Last updated date

The registrar object, which corresponds to a single registrar, consists of the following elements:

- Registrar ID (IANA-assigned)
- Registrar user ID (registry-assigned)
- Registrar name
- Registrar address
- Administrative contact IDs
- Technical contact IDs
- Billing contact IDs
- Registrar URL
- Registrar Whois server
- Created date
- Last updated date

The contact object is only used internally to manage contacts associated with registrars. The contact object consists of the following elements:

- Contact ID (registry-assigned)
- Name
- Status
- Linked
- Organization
- Address
- Phone, Fax
- E-mail address
- Registrar ID (IANA-assigned)
- Created date
- Modified date

Objects that have been deleted will have a status of DELETED.

3.8.2.4 Dump Format

The full and Incremental dumps will be in text format using RFC 822[3] like name value pairs with records separated by a CRLF (\r\n) pair. I18N domains will be expressed in their RACE format until such a time that an RFC on the internationalization of domain names is published by the IETF.

3.8.2.5 Deposit and Transfer

The registry operator will prepare and transfer the escrow data files in the following manner:

1. The files making up the deposit will be created according to File Naming, Escrow Deposit Specification, and Dump Format.
2. The registry operator may compress and split files into parts no larger than 1 Gigabyte each, named <original>.NNNN, where <original> denotes the name of the file before splitting, and NNNN is a monotonically increasing integer starting at 0, left-padded with zeros as appropriate. If the deposit file is split then a file will be created containing the result of applying the MD5 message-digest algorithm[4] to each split and complete file. The MD5 file will be named <split file>.md5, where <split file> is the name of the split file.
3. Files will then be encrypted and signed using a method mutually agreed by the registry and the escrow data recipient.
4. The data sets will be transferred to the escrow data recipient using a secure transport mechanism that will be defined by mutual agreement between the escrow data recipient and the registry operator. Transmission may be over the global Internet, VPN, private leased line or expedited delivery service.

3.8.2.6 Verification Procedures

The escrow agent will verify the format and completeness of each deposit by the following steps:

1. The deposit files will be decrypted using the mutually agreed upon method.
2. If the original deposit file was split, its component split files will be checked for accuracy by comparing the result of performing the MD5 algorithm over the split with the file's associated MD5 file.
3. The escrow agent will run a program to verify that the contents of the deposit and check the results against the registrar generated report transmitted with the escrow deposit. The program will generate a deposit completeness report for forwarding to ICANN.
4. The encrypted deposit files will be decrypted using the method mutually agreed upon by the registry operator and the escrow agent.
5. The decrypted deposit files will be destroyed.
6. If a MD5 check fails or description fails a report detailing the failure will be returned to the registry via a mutually agreed upon mechanism.

3.8.3 Backup Provisions

We recognize the risk posed to the stability of the DNS by failure of critical systems. We have extensive backup systems ensuring near zero data loss even in the event of multi-point infrastructure failures.

The need for conventional backups to tape has been largely eliminated in this infrastructure design by the use of RAID5, checkpointing of dynamic data, the deployment of identical pairs of machines allowing for the use of disk cloning to recover lost system functionality, etc. However, some data remains both dynamic and difficult to reconstruct, such as transaction data, some application data, trouble tickets, and the central database. These dynamic and less recoverable portions of the system environment will be backed up over the net to the central registry location regularly. This includes the equivalent data as described in the escrow provisions, including UTF-8 database dumps to be used in the event that online databases and checkpoints in database format are somehow corrupted.

We expect that the normal means of restoring a damaged server to operation will be to build operating system and initial configuration from original media, add applications as documented, and configure as per established, change-controlled configuration data. There will not be traditional full backups of servers because all that will be backed up for any server is the particular "personality" or state specific to its function.

Software development materials, including source code, tools, and test data, will be among the data committed to backup.

Periodically the archived configuration data, development snapshots, and other dynamic content will be sent offsite to secure storage for retrieval if needed.

Escrow data is deposited daily as incremental deposits, and weekly as full deposits, as described in Data Escrow Schedule, Content, Format and Procedure.

3.9 [C17.8] Whois Services

? **C17.8.** Publicly accessible look up/Whois service. Address software and hardware, connection speed, search capabilities, coordination with other Whois systems, etc.

The .org registry will provide a public Whois service as described in [C17.12] Compliance with Specifications. Example output is included in Initial Whois Output Format.

Facilities for alternative, additional output formats more suitable for machine parsing will be made available if .org registrars indicate they would be useful.

Future changes in the registry model (e.g. any transition to a thick registry which involved the storage of additional fields in the registry database) may require changes to the output of the Whois service. Any changes which are not backwards compatible with the initial planned Whois service will only be introduced following extensive consultation with .org registrars and ICANN.

Bulk access to the Whois data may be made available to registrars after signing a Whois Data Access Agreement designed in the same vein as TLD Zone File Access. Bulk Whois data would not contain any personally identifying information. Should the .org registry contain Contacts, personally identifying information would be withheld from bulk access.

A Whois Privacy policy will be developed and mutually agreed upon with ICANN.

3.10 [C17.9] System Security

? **C17.9.** System security. Technical and physical capabilities and procedures to prevent system hacks, break-ins, data tampering, and other disruptions to operations. Physical security.

Our general approach to security implements the following basic assumptions:

- Good security policy includes several layers, from dropping unwanted traffic at the router to extensive logging of system activity.
- Servers dedicated to firewall functions are neither necessary nor sufficient to support good security policy and can become bandwidth bottlenecks under some conditions. Thus the filtering and monitoring functionality of dedicated firewalls is distributed among configuration and logging on routers, switches, and hosts.
- In keeping with our support for open source solutions, we are relying to the maximum extent possible on available open source software and on our own tools for implementing our security policy.

3.10.1 Types of Services

Three types of services are run. These are fully public, restricted, and fully private. DNS and Whois fall into the first, and SRS protocols fall into the second. Bulk access to data and access to statistical information are restricted. Internal only services, such as database and shell access to server machines, are fully private, and may use on non-publicly routed addresses.

3.10.1.1 Public Services

Many of the services are fully public. Using multiple layers of firewalls, access to machines will be limited to only what is necessary to provide a service. These services are subject to denial of service attacks (both malicious and unintentional) and are probed for possible intrusion points.

These services are not password protected or otherwise authenticated before being queried:

- Whois does not need to run with any high level of system privileges. It will run in a restricted directory with the minimum privileges necessary. Rate-limiting of Whois services is used to prevent DOS attacks.
- DNS services will use well-tested software and will be kept up to date with all security fixes. Additionally, it will be configured to have minimal system privileges and will run in a restricted directory.

3.10.1.2 Restricted services

Supported SRS protocols are not public services, and can be protected from the general public. They are password and/or certificate authenticated. Encryption is used for these services.

3.10.1.3 Private services

Database services and shell access to server machines will be as tightly restricted as possible. Shell access will always be using well-established encrypted services such as SSH. Database services will be firewalled off to restrict access, and database access will be restricted.

3.10.2 Types of Attacks

3.10.2.1 Denial of Service

Denial of Service (DOS) attacks come in two types, those that are malicious and intentional, and those that are accidental. Intentional attacks are concerted efforts, while unintentional DOS situations arise from poorly configured client software, malfunctioning hardware, or attempts to circumvent restrictions on bulk access to data.

Prevention of DOS attacks. Some services can be protected against DOS attacks by limiting the number of queries an IP address can perform in a given amount of time. DOS attacks are the most prevalent and the hardest to defend against without human intervention.

Detection of DOS attacks. DOS attacks typically have easily detectable spikes in service load and server usage. Many tools exist to detect these situations.

Recovery from DOS attacks. Once a DOS attack is blocked, the machine and services return to normal. Other than analyzing and preventing such attacks, no other security work needs to be performed. We will put into place procedures to contact our network providers about any DOS situation. This will allow us to quickly recover from them, prevent new ones, and to trace the source of attacks.

3.10.2.2 Intrusion

Intrusion attacks attempt to run executable code provided by the attacker, or to obtain access to the server machine. These attacks are more severe than DOS attacks because, once successful, the machine itself cannot be trusted.

Prevention of Intrusions. All possible security measures will be used to prevent intrusions. Firewalls will limit access to services and machines, and all public services will run with limited privileges in restricted environments. Additionally, compromise of one machine will not allow compromise of other machines.

Detection of Intrusions and Attacks. Many tools are available to detect intrusions or other types of unusual system activity. Many of these are designed to detect the attacks before they are successful, while others detect changes to the machine's executables and data after the fact.

Network monitoring tools will be used to detect intrusions attempts by analyzing incorrectly formatted DNS and Whois queries, attempts to log into machines, and other network traffic. The data from this monitoring will aid in detecting unauthorized changes to data, and will help in developing and testing changes to services.

Tools like tripwire will be used to ensure system binaries are not modified. These tools compare the production server's environment with a known good image.

Recovery from Intrusions. The only sure way to recover from a system intrusion is to reinstall from operating system media and to install new security patches. Every machine runs a standardized operating system image and software set. Reconstructing a compromised server will happen very quickly. Additionally, due to our high service redundancy, removal of one machine will not cause a service interruption.

Compromises of more integral machines such as the database machine are more severe, but a strong backup and data mirroring will quickly allow a hot-spare to be configured, secured, and put into production.

3.10.2.3 General and Physical

Physical access to servers and networking components will be limited. Secure co-location services provide controlled access to equipment and network access points.

3.11 [C17.10] Peak Capacities

? **C17.10.** Peak capacities. Technical capability for handling a larger-than-projected demand for registration. Effects on load on servers, databases, back-up systems, support systems, escrow systems, maintenance, personnel.

Given the fact that .org has an established history and pattern of activity, we have little concern about a sudden, dramatic change in activity levels even with a change in management. Technical planning has, however, taken the possibility into account.

Peak capacities for the database, the servers, and the network have been planned such that one installation can easily handle the total expected load, which gives a built-in overprovisioning of a factor of 2 for total activity overall. Numbers used for planning normal load already use a base capacity required for servicing 5,000,000 names, approximately twice the number currently in use, so the total system is overprovisioned by a total factor of 4, with the option to grow network bandwidth essentially at will up to the total provisioned capacity of the 100Mb cross-connects.

Nameservers and Whois servers are overprovisioned by a factor of 10 or more and are limited by network bandwidth for presenting traffic to them rather than limited by CPU, memory, or disk. Database throughput for the primary installation is projected to be more than 10 times the expected loads of genuine updates, and can handle many times the same load of reads and unsuccessful writes.

Backup, data escrow, and other support systems are sensitive primarily to the size of the database and the latency of the network, so are subject to the same overprovisioning as those capabilities. Software is designed and built, and the network is engineered, to scale past an additional order of magnitude or more over currently projected use with minimal impact to support systems.

Customer support is 24x7 from launch, allowing unexpected support load to be spread out immediately, particularly for non-urgent issues. Additional less-skilled help, if needed, can be obtained temporarily, with minimal training time, while more advanced help with systems or software can be obtained from contractors with whom we already have relationships.

3.12 [C17.11] Customer Support

? **C17.11.** Technical and other support. Support for registrars and for Internet users and registrants. Describe technical help systems, personnel accessibility, web-based, telephone and other support, support services to be offered, time availability of support, and language-availability of support.

Customer support will benefit extensively from automation and experienced systems staff to keep the operation running smoothly, with minimal trouble. In addition we regard timely distribution of detailed information to registry customers as a critical component of support. Tools in support of this goal are expected to include industry-standard telecommunications facilities, trouble ticket and bug databases, and distribution of useful information to registrars and the public via email and the registry web site. However, the heart of any good support operation is always professional, skilled, available support staff.

The core of customer support for the .org registry is a dedicated customer support center, available 24x7 via telephone, email, and a website. The email and web portions of the support interface, along with certain notification facilities, will be maintained as part of the production service, including high reachability, reliability, fault tolerance, and graceful failover in the event of network or server issues at any one site.

The experience of the technical team in building customer support operations for Internet services suggests that the outsourced call center approach is not the most beneficial for a support operation required to provide a high degree of skilled support for specialized services to a small customer base, as is the case here. The customer support staff will be located with and work beside the systems and development staff. Internal processes will be closely coordinated between these two teams in order to provide minimal opportunity for delayed escalation, misunderstood problems, and the miscommunications that can otherwise limit the efficiency of support services when these teams are kept separate.

3.12.1 Incident Handling

Professional quality trouble ticket systems and telephone call management facilities will be used to track all incidents, whether internal or customer-driven. Industry standard metrics such as call hold times, call duration, and system availability will be used to track resource levels, including the need to increase staff or upgrade bandwidth or hardware.

Systems and software staff will be on-call 24x7 in the event that a problem is urgent and cannot be resolved by the customer support specialist receiving the incident report. Both customer support and the registrar, with appropriate authentication, will be able to view tickets in progress. A ticket will not be closed until the customer agrees the problem is resolved or a workaround is in place.

3.12.2 Notifications

It is anticipated that most incidents will involve a customer at a time, although a larger scale problem would affect many customers. In such an event, as well as in the case of routine maintenance that may have even limited customer impact, registrars will be notified by web and email.

3.12.3 Maintenance

Systems and software staff, in consultation with customer support, will establish a regular maintenance window. This will be used for non-outage maintenance such as phased software upgrades, minor routing policy adjustments, and other activity not expected to cause significant customer impact. There may be no separate notice to customers in advance of minor changes occurring within established maintenance windows and not anticipated to be affect the customers.

Maintenance activities will occasionally cause customer impact, from degraded performance or lower availability of SRS protocols to an outage of the database. Every effort will be made to choose times and methods for these activities that minimize impact to the customer and notification will be provided on the web and via email at a minimum of a week in advance.

3.12.4 Change Control

Software development and quality assurance activities will make use of a dedicated server facility, duplicating the fielded production systems, and professional software engineering tools and test practices.

Enhancement and new feature requests will be prioritized by the development team in terms of complexity and urgency, with a development road map published periodically to registrars and the public. Minor releases to propagate bug fixes will occur as they pass QA, in accordance with maintenance policy. Changes required to improve security, performance, or standards compliance will take precedence over such other changes as may be requested.

3.12.5 Questions/Help

Non-time-critical questions will be assigned a priority and a level of complexity by the support staff person who initially receives them, with a response within three business days either answering the question or stating that it has been escalated for further consideration by systems, software, or administrative staff.

FAQs, aggregate metrics of registry activity, the software bug database, and related material will be available via the registrar portal and, in many cases, to the public. We anticipate there may occasionally be a need to temporarily limit disclosure of some operational information, most likely for security or legal reasons. But we do find that one advantage of open source development and related processes is that they limit the overhead of customer contact authentication, confidentiality agreements, and other obstacles to quick sharing of information as needed.

3.12.6 Staffing

It is anticipated that a dedicated staff of six customer support specialists, including a manager, and five developers/system staff will be able to handle supporting registrars, public services, and initial software deployment as of the launch date. The registry may also require additional help in the form of part-time or consulting specialists as part of the launch phase or as special circumstances might dictate in the production phase.

3.13 [C17.12] Compliance with Specifications

? **C17.12.** Compliance with specifications. Describe the extent of proposed compliance with technical specifications, including compliance with at least the following RFCs: 954[5], 1034[6], 1035[7], 1101[8], 2181[9], 2182[10].

The Whois services described in [C17.8] Whois Services are implemented using the transport protocol specified in [5]. The query language and the format of the responses differ from RFC954, however, in favor of compatibility with the VeriSign Registry server whois.crsnic.net. The .org registry server will be known as whois.isc.org. Sample output can be found in Initial Whois Output Format and Thick Record Whois Output Format, for registry records which do not include and which do include contact objects, respectively.

DNS service will be sought from VeriSign initially. Our global deployment, which will replace the VeriSign secondary DNS service for .org, will run production releases of BIND, specific versions as performance and future needs require. Deployed authoritative nameservers will be operated as authoritative nameservers with no zone transfer or recursive lookup capabilities. Standards compliance of interest for this task includes the following DNS-specific RFCs:

- RFC 1034[6] (Domain Name Concepts): compliant.
- RFC 1035[7] (Domain Name Specification): compliant.
- RFC 1101[8] (DNS Encoding): compliant.
- RFC 1995[25] (IXFR): compliant.
- RFC 1996[25] (Notify): compliant.
- RFC 2136[26] (Dynamic Update): compliant.
- RFC 2535[2] (DNS data signatures): compliant.
- RFC 2671[28] (EDNS0): compliant.
- RFC 2874[29] (IPv6 AAAA records): compliant.
- RFC 2931[30] (TSIG): compliant.
- RFC 2182[10] (Clarifications to the DNS Specification): compliant.
- RFC 2182[10] (Recommended Distribution of Secondaries): compliant.

As a more general principle we build and buy software and equipment that support open, interoperable standards wherever possible. We also participate actively in the development and implementation of new protocols as the evolving Internet requires them.

3.14 [C17.13] System Reliability

? **C17.13.** System reliability. Define, analyze, and quantify quality of service.

Quality of Service for network services is expressed as a set of metrics that attempt to quantify how well the service is meeting expectations and requirements. Metrics we propose for the registry services are derived from those commonly used by ISPs, TLD registries and other DNS services, content delivery providers, and others providing widely used Internet infrastructure.

Questions to be addressed by defined metrics include:

- Service availability: what proportion of the time is the service available to its users? The system is considered unavailable if queries or attempts to initiate transactions get no response or fail.
- Service response times: how quickly is a query answered or a transaction completed? Expected responses times are based on both the time required to process a query or transaction once it reaches the server, and the expected round trip time through the server and the network from the initial query or connection attempt, through the return of the response or transaction commitment.
- Update frequency: what is the latency between an add/modify/delete operations on the database and visibility of that change?

An additional component of the quality of service is the nature, the duration, and the impact of outages, planned and unplanned.

3.14.1 Definitions

Deriving quality of service metrics for the .org registry uses the following definitions:

- 'Core Services': three core services provided by the registry - Shared Registration Service (SRS), Name Service, and Whois Service.
- 'Monthly Time-frame': a single calendar month
- 'Monthly Unplanned Outage Time': the sum of all minutes of all Unplanned Outage Time during a Monthly Time-frame. Each minute of unplanned outage time subtracts from the available Monthly Planned Outage for up to four (4) hours.
- 'Not Responding': means a service that has been identified as unavailable by internal measurements as described below.
- 'Planned Outage' is a pre-announced, controlled outage of one or more of the registry services for maintenance activity. Planned outage periods will generally be scheduled during the lowest activity periods of the registry, but this can be changed if there is compelling need.
- 'Service Unavailability' means that as a result of failure of systems under the registry's control in regards to provisioning services (SRS) that a registrar is unable to:
    - successfully initiate a TCP/IP session,
    - successfully complete a TLS authentication and,
    - successfully complete an SRS protocol login.

Permitted values for these parameters in the context of the .org registry operation can be found in the Performance Specification Summary table, below. Note the commitment that DNS will not be out of service.

Tools for monitoring availability and capacity of our registry services include:

- Internal instrumentation in BIND, including query rates and response latency.
- Well-known, freely available network monitoring tools for observing packet and query loads on a continuous basis, such as mrtg.
- Periodic instantaneous tests or probes of packet loss and latency such as those provided by NetSaint, from a variety of locations in the Internet.

Both daily reports and real-time displays on ongoing measurements will be made available to the technical staff for diagnostic and provisioning analysis.

3.14.2 Notification

Planned Outages will be scheduled well in advance. The registry will notify the registrars of any Planned Outage at least 3 days in advance.

The registry will notify all registrars of any Extended Planned Outage at least one month in advance. Extended outages are a serious matter for the registry and the registrars and will be avoided to the maximum extent possible.

3.14.3 Performance Metrics

Processing time is a critical component in a transaction based service like the SRS, and refers to the amount of time it takes to process a single request from when it is received at the server to when a response is emitted.

Processing time performance specifications for Add, Modify, and Delete, or Check operations in the SRS refer to the 95th percentile of the amount of time it takes to process transactions over a month.

Processing Time specification for a Whois query refers to the amount of time it takes from when the server receives the request until it emits a response.

Processing Time Specification for Domain Name Resolution refers to the amount of time from when the server receives a query until it emits a response.

Processing Time Specification for Domain Name Updates refers to the amount of time from when we receive a update request from a registrar until the DNS update is reflected in the public served by ISC DNS servers.

Summaries of the acceptable performance parameters for each of these metrics can be found in the table below.

3.14.4 Nameserver Availability and Performance Measurements

Our technical team, with experience of root nameservers, TLD DNS provisioning, and DNS service requirements for large ISPs, is well equipped to provide the critical elements of highly available service for nameservers. (The comments here apply to ISC's DNS service, which we will begin deploying within six months of the start of the registry contract and which will assume responsibility for DNS services from VeriSign at the end of the transition.)

There is a high degree of inherent redundancy in the DNS itself, in that only a subset of the authoritative nameservers for any zone needs to be functioning at any given time in order for satisfactory name resolution to occur. With geographic and network diversity of DNS servers (multiple physical sites, multiple major network carriers providing transit), plus this inherent fault tolerance that comes with maintaining a large set of well-provisioned servers, we anticipate essentially no likelihood of any downtime of the .org DNS service at all.

Each system, or cluster of systems in a load-balancing configuration, can be expected to meet a minimum 99.99% uptime on a monthly basis, with the ability to service at least 3 times the measured offered peak load on any single nameserver or cluster.

Availability of a nameserver within the provider's network is of course a less compelling measurement of its usefulness than availability from where the users are. The operator of any system has limited control over that system's availability from the perspective of an arbitrary user. However, our concentration on providing well-connected services through a variety of transit providers and peering partners allows us to maintain a very high degree of reachability to our servers from locations throughout the public Internet.

The .org registry DNS service will meet the Cross-Network Nameserver Performance Requirements as documented by ICANN at section 2.1. In addition, we expect to deploy our own monitoring to observe the performance of our services from outside of our own installations, and promptly correct any serious or persistent problems with reachability of our service from the public Internet.

3.14.5 Update Frequency

Two services, name service and Whois service, must be updated frequently. These services receive data from the database as updated by registrars and propagate them to the public Internet.

The committed update frequency metric for both the nameserver and Whois denotes the 95th percentile over a month for how long it takes an update to the registry database to applied to both DNS and Whois servers. This is measured from the time the registry confirms the registrar-initiated update to visibility on public services.

During the transition VeriSign will be initially responsible for serving the .org zone. We will commit to getting the updates to VeriSign within the specified update frequency, but it will be outside our control as to when VeriSign applies the updates to the published .ORG zone.

3.14.6 Performance Specification Summary

Category	Service	Metric
Service Availability	SRS	99.9% per calendar month.
	DNS	99.999% per calendar year.
	Whois	99.5% per calendar month.
Processing Time	SRS	Add, Modify, Delete: 3 seconds for 95%. Check: 1.5 seconds for 95%.
	Whois	1.5 seconds for 95%.
	DNS	150ms for 95%.
Update Frequency	DNS	5 minutes for 95%.
	Whois	5 minutes for 95%.
Planned Outage - Duration	SRS	8 hrs per calendar month.
	DNS	Never.
	Whois	8 hrs per calendar month.
Planned Outage - Notification	SRS	3 days.
	DNS	n/a
	Whois	3 days
Extended Planned Outage - Duration	SRS	18 hours per year.
	DNS	n/a
	Whois	18 hours per year.
Extended Planned Outage - Notification	SRS	1 month.
	DNS	n/a
	Whois	1 month

3.15 [C17.14] System Outage Prevention

> ? **C17.14.** System outage prevention. Procedures for problem detection, redundancy of all systems, back up power supply, facility security, technical security, availability of back up software, operating system, and hardware, system monitoring, technical maintenance staff, server locations.

All public registry services will be subject to automated, proactive monitoring (see Active Service Monitoring for a functional description of the monitoring infrastructure). The event handling facilities described in Event Monitoring include provision for real-time service monitoring, as well as an automated escalation component. Problems with production services, whether reported by customers or detected by automated monitoring, will be tracked in the registry's ticket system.

All registry systems will be housed in carrier-class co-location facilities, which will include fully redundant environmental control, and uninterruptible power supplies. Registry systems will be deployed in multiple sites, such that a complete failure of one site will not prevent registry systems from continuing to handle a full load of production services. The co-location facilities chosen will provide a very high level of physical security, and access to registry equipment will be strictly limited to registry technical staff. A full record of every physical visit to the equipment will be maintained.

The full-load, production operation of all registry services will not depend on any single network or server element.

Tru64 on Alpha systems has been developed over many years to the highest standards of performance and reliability, particularly in a configuration required to support high availability and high performance for web and database services. Our extensive previous experience on this platform has shown it to be fast, stable, reliable, and capable of handling the most intensive core Internet infrastructure functions.

All software changes applied to registry systems will be made first in an isolated test environment, and rolled out to a user-test environment once regression tests have been passed. Once successful user testing is complete, code will be migrated into production within maintenance windows, with full provision for rollback in the event that problems are discovered. Production deployment of software changes will not be made on two redundant servers simultaneously, unless the nature of the software change requires a consistent version of software to be running across the redundant pair.

All network changes will be subject to peer review, and will be made during published maintenance windows.

No changes will be made to any network element or registry system component without full documentation being included in the ticket system.

The registry has been designed to withstand single-point hardware failure at full system load. Failed hardware components will be replaced during published maintenance windows. Hardware maintenance will not be performed on both elements in a redundant pair during the same maintenance window.

If it is considered that the safe and stable operation of registry functions is seriously jeopardized, emergency software or hardware maintenance may be performed which does not follow the published maintenance policy. Such emergency maintenance will only be performed with the authorization of an .org Program Manager.

Backup services will run as described in [C17.7] Data Escrow and Backup.

System security is discussed in [C17.9] System Security.

Network diversity will be accomplished using multiple transit providers at each co-location facility. Additional route diversity will be obtained using an aggressive and open peering policy.

3.16 [C17.15] System Recovery Procedures

? **C17.15.** System recovery procedures. Procedures for restoring the system to operation in the event of a system outage, both expected and unexpected. Identify redundant/diverse systems for providing service in the event of an outage and describe the process for recovery from various types of failures, the training of technical staff who will perform these tasks, the availability and backup of software and operating systems needed to restore the system to operation, the availability of the hardware needed to restore and run the system, backup electrical power systems, the projected time for restoring the system, the procedures for testing the process of restoring the system to operation in the event of an outage, the documentation kept on system outages and on potential system problems that could result in outages.

As noted previously in [C17.14] System Outage Prevention, much of our architecture is designed around the architectural principle of avoiding single points of failure rather than having elaborate plans for recovering from faults involving such points. However, it is not realistic to assert all possible failures can be prevented.

In general, our response to major incidents is based on the multiple layers of redundant service available in our hardware and software configuration. As a matter of course we load-balance among multiple instances of the public Whois and DNS at all times, so the failure of a single instance of these services within one site or between sites should be literally unnoticeable.

The SRS services and database are slightly more complex to handle redundantly because of consistency issues between instances. Thus there will be a primary instance of the database (one per site) and a primary instance of the registrar portal for addressing it (two per site). Failover between servers at the same site, sharing a database instance, will occur within minutes, with some operations oversight, and will be transparent to the registry user owing to the redundancy features in the network equipment.

Transaction replication between the primary and secondary instances of the database will allow for transparent failover between sites in the event of a catastrophic failure at the primary site. Mechanisms contemplated to redirect traffic from the primary site to the secondary include https redirect, DNS changes, and network provisioning so as to support re-routing of traffic from one site to the other at the IP layer.

Procedures for failover between systems, failover between sites, and recovery from the fault or outage condition are the responsibility of the technical operations lead and the technical staff. The customer support technicians will have the ability to monitor automatic failover systems and processes, with escalation to on-call technical staff when any of the automatic failover processes are invoked. This ensures that the situation can be monitored, the initial problem corrected, and any additional failures diagnosed and repaired.

3.16.1 Recovery From Hardware Failure

As previously discussed in [C17.14] System Outage Prevention, fully redundant hardware and network connectivity allows us to minimize the impact of single hardware failures, whether routers, switches, or servers. It is to be expected that no noticeable outage will occur as a secondary router, switch, or server takes over the full load of a failed companion.

If such failures do occur, they will be fixed in a timely fashion in order to return to fully redundant operation. Support contracts with hardware vendors and with co-location providers will allow for on-site replacement of failed hardware as needed. In the event of a particularly complex failure, registry technical staff may be dispatched to the site to supervise diagnosis and repair.

Maximum impact of a single hardware failure: loss of a single site. In the event this is the primary production site, the second site will continue to function under the full expected load. Some outage or disruption may be notable to registrar clients as the database at the secondary site is validated and the server takes over as primary. In the event the development and management site is affected, software updates, customer service advisories, and some reporting functions may be impacted, but the production sites will continue to function.

3.16.2 Recovery From Software Failure

Software failures may be harder to isolate than hardware failures, requiring a more flexible response. Tools for diagnosis and mitigation of unexpected software problems include:

- The ability to take a production server offline for diagnosis and repair while a known-good version stored on read-only media continues in production service.
- Support contracts with vendors of any proprietary software, which we envision to be primarily limited to operating system issues.
- Relationships with experienced programmers and systems support people beyond full-time staff who can be called upon in an emergency to assist in efforts to diagnose and recover from any issues arising with our open source utilities and applications.

Software bugs will be classified and prioritized as reported, with resources assigned to fix them according to their severity. A bug, misconfiguration, or other anomaly that causes failure of production SRS services, public Whois, or DNS, will be assigned all possible resources until resolved.

Database anomalies or corruption are the most severe potential class of problems.

We expect that regular backups and maintenance of a "warm spare" copy at the secondary site will allow for recovery from a catastrophic failure of the database software or the corruption of the online contents. Database replication between a primary and a secondary is a well understood and widely used technology for fault tolerance.

However, periodic dumps of the database to plain text will be taken in order to support a "fix of last resort" in which the operations staff would load the text and table descriptions into a clean copy on some other database system, configured from scratch if necessary.

Maximum impact in the case of a switch to a new database system and reversion to archived database data would be some hours of downtime to bring up the new system online if checkpoint database logs are not available or are not compatible with the replacement database engine. Loss of the data will be limited to data committed between the text backup used for restoration and the failure event.

3.16.3 Recovery From Operational Failure

The primary value in having multiple production instances of the server farm is to eliminate the chance that a failure at a single facility or a single transit provider could destroy connectivity for the entire registry. Multiple transit providers at multiple sites mean that network connectivity is unlikely to be lost to even a single site for any significant length of time, much less all registry sites.

It is not impossible that for reasons of natural disaster or other causes a co-location or network services provider could experience an interruption in their ability to provide services to us. Failure of one site or one provider can be handled transparently. A more complete failure is unlikely to occur without affecting a far larger portion of the global public Internet than the .org registry.

The registry's later stage deployment plans involve "satellite installations" of servers to handle DNS and Whois queries at well-connected sites throughout the net. This will enhance the ability of the registry to support these critical services without interruption for .org registrants even during a period when the registry's ability to conduct other normal operations such as add/modify/delete might be impaired.

3.16.4 Customer Service

A critical component of fault recovery for the registry is the commitment of customer service to both supporting the recovery process and keeping customers informed throughout. The discussion of incident handling in [C17.11] Customer Support describes the responsibilities of Customer Service, but we emphasize here that the registry operations center is committed to disseminating information about outages in the following ways:

1. Email and web site advisories of service degradations and interruptions, with regular status updates for any incident of extended duration.
2. In the event of a catastrophic failure that would require any extended degradation of registry capabilities, or that would require action on the part of the registrar to maintain the ability to interact with the registry, registrars will be contacted by phone as well as email. This ensures that the registry has provided as much help as possible to the registrar in responding to the incident.

In the event of an outage affecting the customer service site itself, contingency plans for backup phone and network service at a nearby location are included in the registry operational plans. Thus even a major operational problem should not render the registry unable to carry out operations or maintain contact with its customers.

3.17 [C17.16] Registry Failure Provisions

? **C17.16.** Registry failure provisions. Please describe in detail your plans for dealing with the possibility of a registry failure due to insolvency or other factors that preclude restored operation.

3.17.1 Operational Failure

Previous portions of this discussion have described the redundancy, reliability, and failure recovery provisions of the operation we are proposing. These include valid, tested escrowed data or conventional backups for all data needed to take over operation of the registry:

- Operational database (source of Whois and zone file).
- Billing database (current OT&E and financial account standing of registrars).
- Whois, SRS when developed, and DNS server software.
- Scripts, management processes, and reports.

We find it unlikely that multiple production sites for the .org registry service, including both the primary production site and the backup site, along with all valid backups, would be destroyed. Please see the previous discussion for our reasons why we do not foresee any situation in which all of our production facilities would become unavailable, irrecoverably, all at once, barring the disruption or destruction of a substantial portion of the global public Internet. In all other cases the data escrow, backup, and software engineering processes we have described would allow us to recover operational capability.

However, the availability to ICANN or its designee of all the data required to run the registry will provide the ability to allow ICANN or its designee to run the registry in the event that we were no longer able to do so.

3.17.2 Business Failure

A business failure such as a judgment, insolvency, or Act of God, that only encompassed the registry operator would allow reconstruction of the technical ability to run the registry by any ICANN-designated party granted access to the escrowed material, just as above. In addition, the senior technical team would make a best effort attempt to assist the ICANN-named successor registry operator in a transition away from a business failure of the registry operator.

Whois and DNS services could be transitioned almost immediately to any entity with nameservers and other capable servers in geographically diverse locations. The ability to accept database changes and new registrations, and reconstruct relationships with registrars, could follow shortly thereafter, with the critical path determined by legal and regulatory concerns, not operational ones.

The open source and open standards orientation of the .org registry we are proposing has the particular advantage of no intellectual property encumbrances on the software required to run the registry. Succession for an operation based on open source and open standards software is significantly simpler than might be required for a registry based on proprietary solutions.

3.17.3 Regulatory Failure

A regulatory failure provides a less definitive scenario because of the difficulty in defining it. We are here envisioning the possibility of a radical change in either ICANN's composition or mission such that some other entity or group becomes responsible for some or all of the ICANN functions involved in concluding or maintaining a registry agreement, making the agreement with ICANN somehow unsustainable. It is impossible to predict how such changes might unfold, but we note that the organizations involved in the .org registry described here have a long history of commitment to a stable Internet, along with unmatched operational experience in assuring it.

In the event of a major change in ICANN's composition or mission that would impact its agreements with parties such as registries and registrars, the .org registry would continue to operate under the same terms as included in its ICANN contract as any regulatory changes and new contract negotiations went forward. The registry would continue to serve registrars and end-users with as little disruption as possible while regulatory issues were resolved such that a new contract became possible or a new operator was selected in accordance with evolving ICANN process.

3.18 [C18] Transition Plan

? **C18.** Transition Plan. This should present a detailed plan for the transition of the Registry Function from the current facilities and services provided by VeriSign, Inc., to the facilities and services you propose.

3.18.1 [C18.1] Steps of Proposed Transition

? **C18.1.** Steps of the proposed transition, including sequencing and scheduling.

We discuss here the high-level development and implementation roadmap for software and procedures up to registry function acceptance test and cutover from VeriSign management of the registry data to ISC.

We also discuss below in more detail RRP/EPP and Thin/Thick Transition, as well as DNS, IDN, Whois, and IPv6 issues.

The formal startup phase of the registry implementation begins with the bid award. We include a high-level description of the development and deployment plan for equipment, software, and technical support capabilities, based on a bid award in August 2002 and a production date of January 1, 2003.

3.18.1.1 August/September 2002

1. Initial deployment of the first instance of the server stack specified in Section 3.2 will be at the central registry site, to support development efforts.
2. Finalize co-location and bandwidth arrangements: initial space and bandwidth commits, contracts, pricing and terms for expansion as needed.
3. Technical staff hiring: system administrators and developers.
4. Second instance of the server stack specified above will arrive at the central registry site for assembly and test, followed by deployment in commercial co-location space for test and acceptance 30 days prior to go-live (12/1/02).
5. Third instance of the server stack is not critical path, as it's for redundancy and performance, but it should be in production as soon as feasible. Hardware delivery schedules permitting, this will also be assembled, delivered, and tested prior to launch.
6. Customer support manager hired, starts developing detail process, policy, training materials in consultation with project and technical management.

7. Technical assistance to the legal team on the registry/ICANN and registry/registrar contracts.
8. Design and procedures for OT&E process, offer registrars the opportunity to participate in early operational testing.
9. Facilities upgrades: detailed specification, place orders, schedule on-site work for power, phone system, and Heating, Ventilating, and Air-Condition (HVAC) systems.

3.18.1.2 September/November 2002

3.18.1.2.1 Implementation of RRP and EPP

1. Implementation of database services, including interface with registrar billing back-end.
2. Implementation of server-side RRP transaction interface to database, release as open source, manage feedback from external contributors and testers of the code.
3. Implementation of test client-side RRP transaction interface, release as open source, manage feedback from external contributors and testers of the code.
4. Implementation of server-side EPP transaction interface to database. Release date of this code base as open source will be decided pending the status of EPP in the IETF standardization process and determination of what version of the specification is to be supported by VeriSign and others at our launch date.

3.18.1.2.2 Whois Service

1. Implementation of database interface.
2. Implementation and test of public Whois server.

3.18.1.2.3 Zone File Generation

1. Implementation of database interface for generating zone files.
2. Implementation and test of verification tests and procedures.
3. Discussion with VeriSign of technical details of their provision of DNS resolution services to our .org zone after launch.

3.18.1.2.4 Operational Planning

- Finalize further transition details for zone file, Whois data, and any billing information to be included in the transition.
- Hire and train customer support staff.
- Facilities upgrades installed.
- Implement monitoring and management infrastructure, scripts, and processes.
- Final selection and initial configuration/test of trouble ticket system.
- Select registrars for beta test of RRP, billing, and public data services.

3.18.1.3 Final Cutover Preparation

1. Final integration tests:
    - Database and billing.
    - Database and zone files.
    - Database and Whois data.
    - Database failover between machines and locations.
    - Load-balancing and failover of Whois and RRP services.
2. Initial registrar OT&E:
    - Final beta registrars.
    - Open OT&E.
3. Final Test Outline. The high level operational cutover plan will be finalized no later than 15 days in advance of

the registry launch date, in the following general sequence:

- ❍ Plan and perform several test VeriSign registry .org snapshots and load into the registry database when all tests consistently succeed.
- ❍ Publish a maintenance window during which .org registrations will not be accepted by either VeriSign or by us.
- ❍ In window, take a snapshot of VeriSign registry data and load it into the registry database.
- ❍ If all tests confirm our registry is accurate and that interfaces to our registry (RRP, Whois, web) are functioning correctly, then the registry starts accepting registrar traffic for .org.
- ❍ If tests cannot be made to succeed within window, VeriSign starts accepting registrations for .org again, and we fall back to the next window. While we have confidence that we will not attempt final integration unless it will succeed, a contingency plan is always required.

3.18.1.4 Live Cutover Acceptance Criteria

The following characteristics will be used to determine readiness for operational cutover of the registry function from VeriSign to us:

- DNS resolution works.
- Registry changes (adds, changes, deletes) are propagated to the .org zone in an appropriate fashion.
- Whois queries work against our servers .
- Basic compatibility with registrars: our database can add/mod/delete and perform other SRS transactions.
- Billing systems integrity and reliability verified (beta test with registrars).
- Basic customer support: phone numbers, email support addresses, and website exist and work.
- Basic audit: we know how much traffic, database activity, and other work we're doing from day one.
- Backups and reliability plans in place and working.

Non-critical path items for initial launch, to be resolved within operational Q1:

- Performance tuning of database, network, other system characteristics.
- Fine-tuning of customer support for responsiveness and efficiency.
- OT&E for new registrars (not grandfathered).
- 2nd production instance of server node, if hardware delivery schedules did not permit pre-launch deployment.
- Data escrow.

3.18.1.5 RRP/EPP and Thin/Thick Transition

There are three phases to the .org transition from VeriSign Registry to the new .org Registry. Phase I will consist of serving registrars requests with an RRP protocol compliant Shared Registry Service (SRS) and providing the basic services for DNS and Whois. The goal of Phase I is rock solid stability for registrars and their customers and the DNS.

If VeriSign has initiated transition to thin-EPP we will accept any registrars passing of an OT&E testing criteria with the VeriSign Registry. We will also combine Phase I and Phase II for the launch of the .org Registry so that qualified registrars have the opportunity to use either EPP or RRP on day one.

Phase I will consist of serving registrar's requests with an RRP 1.1.0 protocol compliant Shared Registry Service (SRS) and providing the basic services for DNS and Whois. The goal of Phase I is rock solid stability for registrars and their customers and the DNS.

During Phase I of the transition we will take over the management of the .org registry. We will manage the .org zone file and provide a RRP based registry service. We will manage the data transfer from VeriSign and deploy services exactly replicating the current VeriSign service offering for .ORG. Phase I is all about staying consistent with current requirements thus providing for a stable transfer.

In Phase II, we propose to migrate from a pure RRP based registry to a thinly managed EPP based registry. During this migration phase the registry will support two similar protocols. We intend to run both EPP and RRP in parallel for at least 18 months. EPP can run in either a thick or thin model and in Phase III we propose to take the .org registry to a thick registry.

The main difference between thick and thin registry protocols is that thin registries do not maintain contact data. The use of thin registries has been a constant issue for all ICANN registrars and the recent launch of several thick gTLD registries has proven the viability of a thick EPP registry protocol.

During Phase III we propose that registrars migrate their contact data to the registry. As domains are migrated to maintain contacts the Whois for the domain will also migrate. We will work with ICANN and the registrars on the time line of the thin to thick registry migrations with the understanding that a thick EPP based registry is our goal for the .org registry.

It is our goal to provide this service to the registrar community with a smooth, low-cost transition from RRP to EPP. Not only will the server software become freely available, but our experience, software, and expertise will be open for all current and future name registries to use and inspect. We will create a platform for ICANN to create a more stable and robust Internet naming infrastructure.

3.18.1.6 Phase I - Stable Transition

The goals for Phase I is smooth transition and stability for registrars. Our focus will be on a complete and accurate implementation of RRP and its associated out of band communications such as using identical automated e-mail messages for transfer notifications. We will work to mirror the current registry operations for a seamless transition. If VeriSign has deployed a thin EPP implementation this phase will be combined with Phase II.

3.18.1.7 Phase I - Transfers

During Phase I of the migration transfers will operate just as they do now with VeriSign Registry. We will assume and implement duplicate policy regarding domain transfers.

3.18.1.8 Phase I - Deleted Domains

During Phase I of the migration we will implement processes, under the direction of ICANN, based on the outcome of the Redemption Grace Periods for Deleted Names (Technical Steering Group's Implementation Proposal)

3.18.1.9 Phase II - Dual Protocol Support (RRP and EPP)

Our first evolution will be to dual protocol support, meaning we will host RRP and thin-EPP on the same virtual front-end. Allowing the registrar the option to use either RRP or transition to thin-EPP. We believe that the improved robustness of EPP will allow registrars to compete more effectively than registrars using legacy RRP.

We will work with ICANN and registrars to determine a mutually agreed upon time frame for determining the end-of-life date for RRP support. Should ALL registrars complete the evolution to EPP before the agreed upon time-frame period we could accelerate to Phase III after appropriate consultations with ICANN and registrars.

3.18.1.10 Phase II - Transfers

While we are running both EPP and RRP transfers will continue to function for RRP as they did in Phase I, however there will be several enhanced features that we will take advantage of with EPP. When we place EPP into production every domain will be assigned a randomly generated AuthInfo token. These tokens will be available to the registrar of record through the EPP "info" command. Registrars must present this token to initiate and or acknowledge a transfer request over EPP.

We will work with ICANN and the registrar community to determine the most effective date to retire the RRP transfer functionality and only allow the more secure and clearly authorized EPP transfer functionality.

3.18.1.11 Phase III - From Thin to Thick

Thin registries only support referrals in their Whois, meaning that thin registries only manage relationships that describe the domain and which registrar it belongs to: thin registries do not maintain contact information and they cannot display any information about contacts from their Whois database.

Registrars that participate with thin registries must maintain their own Whois and must also implement parsers for some 100+ other registrar Whois formats. All efforts within the IETF and ICANN to further specify port 43 Whois into a common format have failed; However registries that provide thick Whois and use thick protocols such as EPP allow a registrar to implement a parser for the registry Whois format instead of parsers for 100+ registrar formats.

The .org EPP accreditation process will include a rigorous Operational Testing Criteria, which must be passed with 100% accuracy for a registrar to become operational with the additional EPP protocol. Registrars that have passed a Operational Testing Criteria from VeriSign will be grandfathered if VeriSign has launched an thinly managed EPP registry function before Jan 1, 2003.

At some point in Phase III of the protocol evolution phase, after all registrars are using EPP, the registry will allow registrars to start associating contacts with domains. Again we will work with the registrar community and ICANN to determine the best time frame for phasing out the thin EPP registry function.

EPP will become the primary method to manipulate registry objects. Once an object has contacts associated with the domain the Whois for that domain will include those objects in the Whois output. Once all domain objects have associated contacts the registry will no longer accept thinly manage domain objects. Meaning that the registry will require all addDomain commands to contain the required contact references. The date of this final thin to thick transition will be mutually agreed upon with the registrars and ICANN.

3.18.1.12 Phase IV - Complete Thick/Thin Transition

Phase IV will signify the complete transition from a thin EPP based registry to a thick EPP basted registry. In Phase IV all domains will have associated contacts and all Whois replies for domain requests will contain contact information.

3.18.2 DNS Server Service Assimilation

VeriSign will initially run the DNS for the .org registry on the currently deployed GTLD-SERVERS.NET cluster. During this time we will abide by VeriSign DNS server update policy, which will be mutually agreed upon with VeriSign and ICANN. During the transition we will abide by this policy until ALL nameservers are under our direct control.

We will selectively deploy the .org zone on additional servers and in coordination with ICANN roll the new delegations into the root-zone and off individual VeriSign .org Domain Servers. The assimilation is expected to take 6 months for the full and complete replacement of VeriSign nameservers with our DNS infrastructure.

3.18.3 IDN Transmigration

VeriSign Registry has sold a significant number of domains described as Internationalized domain names. These domain names are encoded using a encoding described in the expired Internet-Draft draft-ietf-idn-race-03.txt. The encoding was called RACE or Row-based ASCII Compatible Encoding for IDN. This obsolete encoding is still supported by VeriSign and the IETF has abandoned it as a viable solution for Domain internationalization. These domains, encoded in the RACE format starting with the four-character prefix 'bq--', will be call the RACE domains.

We will maintain the RACE domains until such a time that the IETF IDN working group creates a Proposed Standard for creating and manipulating Internationalized Domain Names(IDN). We will allow domains to be manipulated but not renewed. RACE domain may be deleted but not added to the registry.

The current registrars of RACE encoded domains will not be charged for RACE encoded domains until the registry has a production solution in operation. No new RACE domains may be created via EPP or RRP, but no registrar, and hopefully registrant, will be charged for a domain that cannot be resolved from the .org DNS Servers.

We will only support internationalized domains once the IETF has created a Proposed Standards for such encodings and consultation with ICANN has produced a mutually agreed upon action plan for the deployment of I18N functionality in the .org registry.

RACE encoded domains will only be delegated under the domain "mltbd.org" until ICANN has approved the use of an IETF-designated Proposed Standard on the use of Internationalized Domain Names.

3.18.4 Whois Redirection from VeriSign

We propose that the VeriSign Registry serve a single referral to the .org registry for any .org domain or nameserver that is sent to any of the port 43 Whois servers the VeriSign Registry operates.

A sample request/reply for the domain 'example.org' to whois.internet.net:

```
C: example.org\r\n
S: Domain names in the .com, .net, and .org domains can now be registered
S: with many different competing registrars. Go to http://www.internic.net
S: for detailed information.
S:
S: .org Domains are now handled by the .org registry administered by
S: the Internet Software Consortium. See http://nic.isc.org for more
S: information.
```

```
S:
S:   Domain Name: EXAMPLE.ORG
S:   Whois Server: whois.isc.org
S:\r\n
```

3.18.5 IP Version 6 Support

The major components of .org registry support for IPv6 are as follows:

1. Submission of IPv6 records (AAAA) as nameservers via SRS services. We will support IPv6 nameservers and any other additions to the SRS protocols VeriSign discloses when the contract for the .org registry is signed with ICANN.
2. Publication of IPv6 hosts as nameservers in the .org zone. We will allow for the inclusion of nameservers with IPv6 addresses in the .ORG zone at initial launch, including necessary AAAA records .
3. Query response over IPv6 transport for .org nameservers. We are testing various aspects of IPv6 use on the Internet, including the use of IPv6 transport for DNS queries and responses. We will follow the lead of the root nameserver operators in production deployment of this enhancement to .org registry support.

3.18.6 Community Notification and Outreach

We will post notifications to various operational mailing lists of the stage and progress of the .org transition. We will attend and present status and progress reports to ICANN and at various operator conferences.

3.19 [C18.2] Interruption of the Registry Function

? **C18.2.** The duration and extent of any interruption of any part of the Registry Function.

We anticipate some interruption in the registry function for a few hours as we synchronize databases with VeriSign, validate the data, and make sure VeriSign has stopped accepting add/mod/deletes for the .org domain before we start to accept them. This will require some assistance from VeriSign and some effort by registrars to reconfigure their SRS clients. Support requirements more than the operational requirements dictate we be prepared for the handoff to take several hours to finalize and verify.

3.20 [C18.3] Contingency Plans

? **C18.3.** Contingency plans in the event any part of the proposed transition does not proceed as planned.

Contingency plans for some failure of the proposed changeover address three possible situations:

1. Tests for acceptance of the transition as ready to go are included in the [C18] Transition Plan. Should any of these tests fail, the cutover will be suspended until the problem can be identified and resolved. The result would be some amount of schedule slippage if the problem turned out to be time-consuming.
2. The cutover phase itself includes a final database synchronization event between VeriSign and us, with a final set of tests to validate. Should any inconsistency be found between the databases, or any other anomaly be observed, the cutover will be postponed from the current window while the problem is found and corrected. The cutover will be rescheduled as soon as feasible, but will allow no less than three days from the date of the initial failed attempt, in the interests of insuring stability for registrars and end users.
3. In the event that a problem or anomaly occurs within the first month after the cutover, consideration will be given to invoking a back-out plan. Such a plan will be finalized before the cutover is allowed to go forward. Details will depend on operational considerations to be determined between VeriSign and us, but the result of invoking the plan will be to return responsibility to VeriSign for .org operations, along with our data for any add/modify/delete operations to the database during the interim. We do not anticipate needing to resort to backing out the change once made and would only do so under the most serious unforeseen conditions. The cutover would be initiated again once the problem was found and solved, no less than one week from the date when control was reverted to VeriSign, again in the interests of promoting stability for registrars and end users.

3.21 [C18.4] Effect on .org Registrants and Internet Users

? **C18.4.** The effect of the transition on (a) .org registrants and (b) Internet users seeking to resolve .org domain names.

Effects of the transition on .org registrants are expected to be limited to the need to change their Whois clients to point to a different registry Whois. As new versions of commonly used clients appear, this will rapidly become unnoticeable to the average user.

Registrants will as time goes on notice decreased latency in getting registry add/modify/deletes they commit through their registrars into the public DNS and Whois infrastructure. Initial service levels commitments are to maintain the current 12-hour cycle for Whois and zone file changes, but it is also expected that significant progress will be made within the first six months in reducing that latency.

Internet users seeking resolution for .org names will see literally no change at first, as VeriSign's nameservers will continue to serve the .org zone. As our servers are added and zone data refresh cycles accelerate beyond the initial commitment of 12-hour latency, changes to domain name information will be reflected in the global DNS and Whois services much faster.

3.22 [C18.5] Specific Cooperation Required from VeriSign

? **C18.5.** The specifics of cooperation required from VeriSign, Inc.

We will require VeriSign Registry cooperation in the following areas.

- .org zone file transmission for service on VeriSign GTLD-SERVERS.NET.
- Registry Cut-Over Coordination.
- .org Registry Data Dump.
- Update VeriSign Whois to produces an .org referral.
- Transfer mltbd.org to new registry operator.
- Provide SRS Server Software Specifications.
- Provide SRS Server Software Source Code.
- Provide DNS Update Mechanism.

We will generate a zone file at least once every 12 hours. This zone must be transferred to the GTLD-SERVERS.NET cluster of name servers. As we transition our own nameservers to replace the individual machines in the cluster. ICANN and VeriSign will need to coordinate the update of the ROOT zone with the newly deployed .org nameservers.

During the process where by VeriSign stops accepting SRS transactions for .org and we start accepting the transactions, VeriSign will need to discontinue service for the .org registry. Also, should there be a massive failure during the transition and the transition needs to be reversed in favor of another transition date, VeriSign will need to be able to cause their systems to resume accepting SRS transactions for .org.

VeriSign will need to compile an .org Registry Data Dump on several occasions. The dump must contain all relevant data so that we can properly populate the registry for seamless transition. The Dump should contain, but not be limited to, the following data sets: Registrar to Domain associations, domain status and domain to name server associations with any appropriate glue records.

VeriSign will have to create these data sets and make them available to our registry over the Internet via secure methods such as SFTP or SCP on several occasions.

VeriSign will also have to update their Whois so that it emits a referral for any .org name queried. A sample of an appropriate referral would be as follows:

```
C: example.org\r\n
S: Domain names in the .com, .net, and .org domains can now be registered
S: with many different competing registrars. Go to http://www.internic.net
S: for detailed information.
S:
S: .org Domains are no handled by the .org registry administered by
S: the Internet Software Consortium. See http://nic.isc.org for more
S: information.
S:
S:   Domain Name: EXAMPLE.ORG
```

```
 S:   Whois Server: whois.isc.org
 S:\r\n
```

For complete management of the currently registered .org namespace We will require VeriSign Registry to transfer the domain mltbd.org to us so we can continue to manage the Multilingual RACE Encoded domain registrations currently registered in the .org namespace. For a complete overview on IDN transition refer to section on IDN Transmigration of this proposal.

VeriSign must provide complete specifications for the SRS (RRP and, if in production, EPP) server software implementations, including but not limited to, business logic for grace periods and billing, email templates for notifications, and any functional implementation used in the registry but not documented in RFC 2832[1] or one of the EPP Internet-Drafts

VeriSign will need to provide complete sources of the Server software, scripts and associated documentation and build tools for SRS protocol implementations.

Provide mutually agreed upon standard protocol mechanism or functional equivalent to transmit DNS additions, deletions, and modifications to the .org zone while some .org Nameservers are managed by VeriSign. The standard protocol mechanism must be at least more robust than that stated in [13].

3.23 [C18.6] Relevant Prior Transition Experience

? **C18.6.** Any relevant experience of the applicant and the entities identified in item C13 in performing similar transitions.

We have extensive experience performing similar transitions and deep familiarity with the current operating environment. Our team members have:

- Worked at ICANN during the initial incubation period.
- Built some of the first test bed registrars and first 3rd level registrars.
- Built some of the key Exchange Points and integrated them into the Internet infrastructure.
- Extensive experience building new databases and transitioning legacy databases.
- Extensive program management experience dealing with large MIS operations during transitions.
- Extensive experience working with policy makers and the public during transitions.
- Extensive experience in re-provisioning core Internet services.

3.24 [C18.7] Proposed Criteria for the Evaluation of Transition

? **C18.7.** Any proposed criteria for the evaluation of the success of the transition.

For the transition period, the goal is to complete the transition within the schedule allotted with minimal downtime and no after-effects. In the plan we've put forward, questions could include in the short term:

1. Has the transition completed in a timely fashion with minimal disruption?
2. Are registrars able to successfully switch from VeriSign's SRS to ours?
3. Are users getting fast, accurate answers from Whois and DNS servers?
4. Is SRS service performance within the service commitments made to, and relied on by, the registrar population?

After the transition period, the goal is to run a stable .org registry that meets the performance and functionality criteria specified in this proposal and in a subsequent agreement with ICANN. Specific criteria could include:

1. Has the publication of new data for DNS and Whois services occurred more rapidly?
2. Has customer service improved?
3. Have performance standards and QoS targets been met?

TOC

4. [C19] Compliance with ICANN-Developed Policies and the Registry Agreement

? **C19.** Please describe in detail mechanisms that you propose to implement to ensure compliance with ICANN-developed policies and the requirements of the registry agreement.

We will regularly publish many of the operational statistics to the general public. We will designate various members of staff to participate in the gTLD Registries constituency and work within the DNSO on Consensus Policy Development. A Policy Compliance Officer staff person will be designated to work directly with ICANN management on issues of compliance and best industry practice.

We will generate and submit to the ICANN Office of Policy Compliance the following reports:

- Accredited Registrar Status - the status of operational registrars, registrars in the ramp up period, and registrars in the pre-ramp-up period.
- Service Level Agreement Performance - compare SLA with actual performance.
- TLD Zone File Access Activity Report - lists number of zone file accounts, accesses and new account approvals.
- Completed SRS/System Software Releases - release, features, target date, completed date.
- Domain Names Under Sponsorship - Per Registrar.
- Nameservers Under Management - Per Registrar.
- Domain Names Registered by Registry.
- Whois Service Activity - number of queries, downloads.
- Monthly Growth Trends - Read, Write, Query transaction counts.
- Total Number of Transactions by Subcategory by Month for each of the appropriate commands in either EPP or RPP, depending on the Phase of transition.
- Total Number of Failed Transactions by Subcategory by Month - for each of the appropriate commands in either EPP or RPP, depending on the Phase of transition.
- Daily Transaction Range - daily volume report.
- TLD Geographical Registrations Distribution - geographic distribution of domains.

---

5. [C20] Provisions for Equivalent Access by Accredited Registrars

TOC

? **C20.** The selected successor operator for the .org registry will be required to provide all ICANN-accredited registrars having registry-registrar agreements in effect with equivalent access to registry services through a shared registry system, under which those registrars will provide services (either directly or through resellers) to registrants. This section of the .org Proposal covers the applicant's proposed arrangements for interacting with registrars in a manner that provides equivalent access.

5.1 [C21] Equivalent Access Policies

? **C21.** Describe in detail your proposed methods of providing registry services on an equivalent basis to all accredited registrars having registry-registrar agreements in effect. Your description should include any measures intended to make registration, technical assistance, and other services available to ICANN-accredited registrars in different time zones and relevant languages. In addition, describe the Registry Code of Conduct and other commitments you propose to make to ensure that all such registrars receive equivalent access to registry services. In preparing your response to this item, you may wish to refer to Appendices H and I of the registry agreements ICANN has entered for unsponsored TLDs (e.g., .biz, .com, .info, .name, and .pro).

Neither ISC nor IMS will be a registrar. We will not compete with our customers. Our first priority is to provide stable, responsive, and fair service to our customers and to the registrants in the .org TLD.

5.1.1 Equivalent Access Policy

It is the goal of this policy to ensure that:

- All ICANN-Accredited registrars connect to the System using the same protocols and with the same limitations and security measures.
- All ICANN-Accredited registrars have the same access to customer support, administrative and business services.
- All ICANN-Accredited registrars have the same access to the tools required to access their data through the System including billing, account management, and other similar services.
- With the exception of systems designed to enforce our or ICANN's terms of service, contract or policy, the System does not include any features or systems designed to perform prejudicially or favorably towards any specific ICANN-Accredited registrar[s].

5.1.2 Registry Code of Conduct

We will at all times operate as a trusted neutral third-party provider of DNS Registry Services. We recognize that domain names are the means by which businesses, consumers, and individuals gain access to, navigate, and reap the benefits of the global Internet. These benefits cannot be fully realized, however, unless DNS resources are administered in a fair, efficient, and neutral manner that makes them available to all parties desiring to provide DNS services. To ensure the provision of neutral Registry Services, We will comply with the following Code of Conduct.

Neither us nor any of our subcontractors will, directly or indirectly, show any preference or provide any special consideration to any company, person or entity that is a DNS registry provider or registrar services provider, as those terms are defined by ICANN.

All registrars accredited by ICANN who are authorized to register domain names in the .org registry shall have equal access to Registry Services provided by us.

We and our subcontractors shall not in any way attempt to register domain names in their own right, except for names designated for operational purposes. In its monthly report to ICANN, we shall include a list of all names designated for operational purposes.

Any subcontractor, affiliate, or other related entity that also operates as a provider of registrar services shall maintain separate books of account with respect to its registrar operations.

Neither us, nor our directors, subsidiaries, affiliates, or other related entities shall have access to user data or proprietary information of a registrar served by us, except as necessary for registry management and operations.

We will ensure that no user data or proprietary information from any registrar are disclosed to its affiliates, subsidiaries, or other related entities, except as necessary for registry management and operations.

Confidential information about our business services will not be shared with employees of any DNS services provider, except as necessary for registry management and operations.

We will conduct internal neutrality reviews on a regular basis. In addition, we may mutually agree with ICANN on an independent party that ICANN may hire, at ICANN's expense, to conduct a neutrality review of our operations, ensuring that we comply with all the provisions of this Registry Operator Code of Conduct. The neutrality review may be conducted as often as once per year. We will provide the analyst with reasonable access to information and records appropriate to complete the review. The results of the review will be provided to ICANN.

5.2 [C22] EPP Support

? **C22.** VeriSign, Inc., the current operator of the .org registry uses a registry-registrar protocol (RRP) documented in RFC 2832[1]. At the time of the transition, the selected successor operator will be required to continue to support the RRP (unless a migration of registrars in .org to another protocol has already been completed by that time). In addition, the selected successor operator will be required to implement support for the IETF provreg working group's protocol specification for an Extensible Provisioning Protocol (EPP) no later than 135 days after it is adopted as a Proposed Standard RFC 2026[11], section 4.1.1]. Provide a detailed description of your plan for supporting RRP at the time of transition, for supporting EPP within the required time frame, and for providing registrars with a smooth, low-cost migration path from RRP to EPP.

5.2.1 EPP Transition

We plan a complete transition to a Thick EPP based Registry. Our plan will be carried out through three Phases. The first, Phase I, involves seamless migration to our RRP based .org registry. Phase II involves dual concurrent support of EPP and RRP. During this phase registrars migrate from RRP to EPP. Since our current database schema supports all the requirements for implementing EPP and RRP, we are confidant that an EPP implementation can be developed and installed within the 135-day time frame after the EPP documents make it to Proposed Standard. During Phase II, we will announce the end-of-life date for RRP Registry support after consulting the registrar community and ICANN. In Phase III, we will assist registrars in migrating to a thick EPP based registry. Phase III consists of registrars populating the registry with contact information and associating the contacts with the appropriate domain names.

for a complete discussion of how Transfers, Deletes and Grace periods work during the transition please see [C18.1] Steps of Proposed Transition.

C23. and **C24.** Intentionally omitted.

---

6. Proposed Registry Services

TOC

6.1 [C25] Registry Services for Fee

? **C25.** Describe each Registry Service (as defined in subsection 1.16 of the model .org Registry Agreement) that you propose to provide for a fee. For an example of a description of this type, see http://www.icann.org/tlds/agreements/name/registry-agmt-appc-1-03jul01.htm.

The following services will be offered for fee:

- Registrations of new domain names. When a registrar creates a new Domain by using the addDomain command, the registrar's account will be debited the Registration fee times the multiple of years that the domain is registered for. Domains May be registered in increments of one (1) to ten (10) years in one (1) year increments.
- Renewal of domain names. Existing domains may be renewed for up to a maximum of 10 years. domains may be renewed in increments of one (1) year to ten (10) years in one (1) year increments.
- Transfers will require a Renewal of the domain, per industry practice, for at least one (1) year when the transfer completes, the renewal is automatic; however the act of the transfer incurs no charge, it is the required renewal that will incur a fee.

6.2 [C26] Maximum Price

? **C26.** State the maximum price you propose for each Registry Service identified in item C25.

We believe the price to register or transfer a name in the .org registry should not be lower than the lowest price charged for other TLDs, as that simply encourages speculation. However, the price should not be higher: noncommercial organizations should not pay more than other types of registrants. We will monitor the market and on a quarterly basis will adjust our prices accordingly.

Our planning assumptions are that the wholesale price for domain names will go down 10% per year over the 5-year period. Based on our analysis of market conditions:

- We propose a maximum price of $6 for add, or renew operations.
- If we qualify for the VeriSign Endowment as discussed in [C40] The VeriSign Endowment we propose a maximum price of $5.50 for add, or renew operations.

The difference in price is based on our costs for debt financing of the initial startup phase of the .org registry. We're perfectly happy to accept a lower startup price if the other TLD registries have similar price adjustments.

Stability of the .org registry function is our first priority. As detailed in the accompanying Consolidated Pro Forma Financial Statements, we believe that stability can be achieved even if the wholesale price of registering a domain name goes down significantly faster than 10% per year.

6.3 [C27] Registry Services Without Fee

? **C27.** Describe each Registry Service (as defined in subsection 1.16 of the model .org Registry Agreement) that you propose to provide without charging a fee.

The following services will be offered without fee:

- Creation and maintenance of nameservers. Domains that have an associated nameserver may create or update their relative or associated Nameservers.
- Creation and maintenance of contact information. Contacts that are associated with domain names may be created or modified for no charge.
- Deletion of domains, contacts, and nameservers. All objects may be deleted for no charge.
- Status information of domains, contacts, and nameservers. Domains, Contacts, and Nameservers may be inspected by the Registrar of Record at no charge.
- Distribution of zone files. We will make available for no charge the .org zone files for any entity that signs a Zone File Access Agreement.
- Operation of the registry TLD zone servers. We will operate at no charge the .org zone servers.
- Operation of the Registry Whois servers. We will operate at no charge the servers that provide the port 43 Whois Service. We will operate a web server using the HTTP and HTTPS protocols that will have a web interface to the Whois service.
- Distribution of bulk Whois. We may make bulk Whois data available to the registrars that sign a Whois File Access Agreement. The Whois data would not contain any personally identifying information, such as contacts or their respective e-mail addresses.
- Distribution of software used to run the registry. We will not charge a fee to distribute the very software that the registry uses in its day-to-day operation.
- Distribution of software for registrars. We will not charge for any software developed for registrars to access or use the registry or additional tools developed for registrars.
- Technical support. We will not charge for providing technical support to ICANN accredited registrars via phone, email or fax.
- Publication of statistic information about .org zones. We will not charge for any statistical analysis that is performed and published on or about the .org zone, including aggregate information about the operations.

6.4 [C28] Technical Performance Specifications

? **C28.** Describe the technical performance (including quality-of-service commitments) you propose to make. See http://www.icann.org/tlds/agreements/name/registry-agmt-appd-29jun01.htm for an example. The successor operator will be expected to meet the Cross-Network Nameserver Performance Requirements set forth in section 2.1 of the document at the above URL.

Please see Performance Specification Summary for a summary of our service level targets for production DNS, Whois, and SRS services. We regard these proposed metrics, based on common practice in the Internet services industry, as a starting point for quantifying the performance and capabilities of the registry. Other appropriate metrics will be developed in consultation with ICANN and the registrar community.

The initial set of metrics is described in more detail below.

In addition we will strive to develop and maintain the strictest performance specification for Servicing SRS transactions in either RRP or EPP and for servicing the public's DNS or Whois queries. Furthermore we will regularly publish the statistics and raw data for full disclosure of our operational performance.

Definitions of terms included below shall be as described in [C17.13] System Reliability.

6.4.1 Performance Specifications

Processing time is a critical component in a transaction-based service like the SRS. Processing Time measures the quality of service while the registry is Available. Processing time refers to the amount of time it takes to process a single request.

Processing Time specification for Add, Modify and Delete is three (3) seconds for 95% of the transactions processed for a Monthly Time-frame. That is 95% of the Add, Modify and Delete commands will take three (3) seconds or less from the time the SRS received the request until the SRS emits a response.

Processing Time Specification for a Check command is 1.5 seconds for 95% of the transactions processed in a Monthly Time-frame. That is, 95% of the Checks will take 1.5 seconds or less from the time the SRS received the request until the SRS emits a response.

Processing Time Specification for a Whois query is 1.5 seconds for 95% of transactions. That is, 95% of Whois queries will take less than 1.5 seconds from the time the Whois server receives the request until it emits a response.

Processing Time Specification for Domain Name Resolution is 150 milliseconds for 95% of transactions. That is, 95% of nameserver resolutions will take less than 150 milliseconds from the time the server receives a query until it emits a response.

Processing Time Specification for DNS Updates is 5 minutes for 95% of transactions. That is, 95% of all updates applied to data to be reflected in the published .org zone will be published in less than 5 minutes from receipt of the successful SRS transaction from a registrar.

Processing Time Specification for Whois Updates is 5 minutes for 95% of transactions. That is, 95% of all updates applied to data to be reflected in the published port 43 Whois service will be published in less than 5 minutes.

6.4.2 Update Frequency

As previously discussed another critical parameter of service availability for the registry is the update frequency of the publicly available information provided by the Whois and DNS services. Our DNS architecture will operate at a normal update latency of 5 minutes for 95% of updates on a monthly basis, with a service goal of 3 minutes for the great majority of updates and 99.9% of updates in 15 minutes or less. The Whois service will be held to a similar standard, as described in Performance Specification Summary.

6.4.3 Cross-Network Nameserver Performance Requirements

As noted above in Performance Metrics, we are fully prepared to meet the Cross-Network Nameserver Performance Requirements as described by ICANN, which are based on an expectation of less than 10% packet loss and less than 300ms round trip time between query and response for DNS queries sent from diverse locations in the public Internet.

C29. Intentionally omitted.

---

7. [C30] Enhancement of Competition

TOC

? **C30.** One of ICANN's core principles is the encouragement of competition in the provision of registration services at both the registry and registrar levels. Promotion of that principle will be a criterion. As one illustration of this criterion, a major purpose of the reassignment of the .org registry is to diversify the provision of registry services by placing the .org registry under different operation than the .com and .net registries. Consideration will be given to the extent to which proposed arrangements are consistent with this purpose. As another illustration, applicants are encouraged to refrain from prohibiting non-affiliated providers of backend services from offering their services in connection with other applications. This section of the .org Proposal concerns the effect on competition of the selection of a successor registry operator.

? **C31.** Give your analysis of how selecting your application would affect competition in the provision of registration services at both the registry and registrar level.

Our proposal would provide ICANN and the public with the first registry operator operating solely for the public benefit. We have years of experience operating this type of infrastructure and have provided many of the core functions on which registry operators and registrars depend.

Selection of our team to operate the .org registry will have a strong ripple effect. We will enhance competition at the registry level because of our strong commitment to keep prices as low as possible as detailed in [C26] Maximum Price. Our commitment to provide freely available software in binary and source format for both registrar and registry solutions will have a strong impact on competition, particularly at the registry level. Our team is well known for production-quality solutions and our software will enable new registries to quickly enter the market, operating in either the public or some private interest.

We provide public solutions and operate public services. Our team views our role as policy neutral. For example, if ICANN wished to greatly enlarge the number of TLDs available, our freely available software would allow other organizations to operate registries or to have those registries quickly and easily hosted on our own operating environment. In summary, we can help facilitate and support an environment with more registry operators, more TLD policy bodies, and more choice for consumers. We can do so by setting a Best Current Practices standard of how to operate a rock-solid registry for the .org TLD.

? **C32.** State whether the applicant or any entity identified in item C13 operates a DNS registry having more than 500,000 registered names and, if so, provide details.

Neither the applicant nor any entity identified in item C13 operates a DNS registry having more than 500,000 registered names. On the other hand, we've helped operate some of the largest databases (the EDGAR and Patent database involved tens of millions of documents) and busiest services (e.g., the "F" root server) on the Internet.

? **C33.** Describe in detail all affiliations, including direct or indirect ownership and contractual arrangements (including letters of intent) for the past, present, or future provision of registry services, between (a) the applicant or any entity identified in item C13 and (b) any operator of a DNS registry having more than 500,000 registered names.

We have no such affiliations.

C34. Intentionally omitted.

---

8. [C35] Responsiveness to the Noncommercial Internet User Community

TOC

? **C35.** Describe in detail the mechanisms you propose for ensuring that the policies and practices followed in your operation of the .org registry are responsive to and supportive of the noncommercial Internet user community, and reflect as much of its diversity as possible. Your description should include any affiliation you propose with representative noncommercial organizations and details (including proposed bylaws or other chartering documents) regarding any governing or advisory groups that you propose.

Our team has worked the vast majority of our careers in the noncommercial Internet user community. Our program managers and board have over 250 years of collective public service to the Internet between them. Our program managers will have direct and immediate involvement in the day-to-day operations of the registry, and our staff and volunteers usually provide a response time to incoming e-mail that rivals the response times we promise for core .org services in Performance Specifications.

Because we operate production services in the public eye, we have a very direct and immediate communications pipeline with our users. If something isn't working or could be working better, we get immediate feedback.

We will operate the .org registry as a fully public process. Our code will be public from very early releases, all enhancements to our service will be fully vetted by open public forums and IETF review, and our support functions will have the direct involvement and supervision of our program managers.

We will operate a variety of web sites and email services that are aimed at our various constituencies. In addition to the extensive support infrastructure for registrars, we will build a web portal for registrants in the .org TLD that will provide our end users with a direct communication channel with the .org registry and a public forum for discussions of our operations.

One of our primary goals is responsiveness to noncommercial organizations around the world. We believe that our constituencies range from formal organizations, such as charted NGOs and 501(c)(3) non-profits, to loose collectives and unincorporated groups, such as open source developers and many other active communities on the Internet. We participate extensively in public forums, both Internet-specific and general-purpose, and we intend to make the .org TLD a dynamic, responsive home to these groups.

In terms of formal advisory bodies, we spent a great deal of time in the bid preparation process attempting to formulate charters for a variety of advisory bodies. We felt it important that any advisory body have real teeth and not simply serve in a token figurehead role. After a great deal of deliberation, we determined that the best way to keep operational stability for the .org registry and still maintain responsiveness is a four-part strategy:

1. Run a fully open .org TLD registry, disclosing all of our work product and all of our plans.
2. Provide extensive mechanisms for the general public and our various constituencies to make their views known.
3. Have the staff of the .org TLD develop full proposals on a variety of measures and make those plans public early.
4. Entrust our board of directors with fiduciary responsibility for the stability of the .org registry and decisions on which strategies will best meet our goals of differentiation of the .org TLD, responsiveness to our constituencies, and enhancing the general Internet infrastructure. Our board of directors is thus our advisory body with full responsibility for our operations in a fully public process.
5. Provide full accountability through audited financial reports and extensive reporting on our operations.

In addition, we intend to seek formal partnerships with a variety of noncommercial organizations. We have already signaled our Intent to Donate to the Internet Society. We will work with a wide variety of organizations, both within Internet infrastructure and in the rest of society, to make the .org public utility serve the needs of the public.

9. [C36] Support for Proposal

TOC

? **C36.** Submit any evidence that demonstrates support for your proposal among registrants in the .org TLD, particularly those actually using .org domain names for noncommercial purposes. Support from diverse noncommercial entities from across the global Internet community will be considered in the selection.

While we must commend and compliment ICANN for the clear and complete proposal process in the competition for the privilege of running the .org registry, we respectfully submit that with multiple bids contending for this opportunity, the global Internet community will want to make a choice based on an examination of the options that are available to them.

We would thus encourage ICANN and the Internet community to examine all the bids and make a decision after a careful assessment of the relative merits of all the options. We have made available a page on the World Wide Web where supporters of our bid, after they've examined all the facts, to signal their support for the IMS/ISC bid to make .org a public trust at <http://trusted.resource.org/> We would encourage ICANN to watch this and other URLs for evidence of public support.

While we do feel that it is premature to summarize public support for our bid before it is public, initial indications are that noncommercial organizations and the general Internet community view the service we are offering to provide very positively. A large number of organizations have asked for briefings, and we begin the briefing process for those organizations immediately after our bid is public. Early evidence of community support in public forums such as The New York Times, Slashdot, and ICANN Watch has been quite positive.

C37. Intentionally omitted.

10. [C38] Differentiation of the .org TLD

TOC

? **C38.** Describe any measures you propose to make to differentiate the .org TLD from TLDs intended for commercial purposes. Your proposal should describe in detail any planned marketing practices designed to differentiate the .org TLD, promote and attract registrations from the global noncommercial community, and minimize defensive and duplicative registrations.

A series of steps will be taken that will substantially differentiate the .org TLD from gTLDs and ccTLDs:

- Because we a non-profit service, we are able to publish the source code for components that we write, as well as fine-grained implementation details of the infrastructure we deploy. The .org TLD will be extremely well documented as we are not under the constraint of commercial registry operators to maintain this information as proprietary.

- We will publish extensive data relating to the measurement of the services we provide and work with our colleagues in the Internet research community. The .org statistics and measurements will make our TLD run better, but will also enable operators of other TLDs to learn from the real-time data we provide.
- We will provide a strong web presence as the home for information about the .org TLD. Our experience building production web sites that involve large communities will quickly differentiate the .org TLD. Because our intended audience is the noncommercial organizations of the world, our site will be tailored towards their needs, as well as to the needs of the broader Internet community.
- We will aggressively market .org as a home for noncommercial organizations using our skills in building awareness around new Internet services. We will work extensively with the media, policy makers, and noncommercial organizations around the world to explain to them why .org is differerent and what that means to them.
- Our boards of directors have established priorities for use of funds in .org to be differentiation and service to the .org registrants and general benefit to Internet infrastructure. All of our advanced development programs will be oriented around these goals, providing a substantial stream of new ideas that will be made targeted to our registrants, registrars, and other constituencies.

Four aspects of our work will be particularly important in differentiating the .org TLD:

1. Our core operation will be producing new tools for people to use, with particular emphasis on use in the .org TLD and by other registry and registrar operators.
2. Our advanced development program will provide a steady stream of new ideas for the IETF to consider.
3. Our outreach efforts will bring new organizations into the .org TLD and will teach existing registrants how they can use their presence on the Internet in a more effective fashion.
4. We will develop, and we will encourage others to develop, "deep domains."

Our core operation includes intensive work on tools such as registry software and registrar software. We will be constantly improving our tools as standards evolve and as our customers teach us better ways to do things. The .org TLD will receive a series of improvements in performance, stability, and functionality over time by a team of experienced service operators and software developers.

Our advanced development program, which is under the direction of Carl Malamud, Rebecca Malamud, and Marshall T. Rose will provide a long horizon, developing ways to substantially improve core functions. It is important to note that we do not view the .org TLD as a guinea pig: all new innovations are published first as prototypes, then submitted to an internal reality check, then submitted to the IETF as Internet-Drafts with working code. Only after consensus is reached and operational experience achieved will changes be proposed to the community on how a registry might operate.

An example of our advanced development program can be found in a recently submitted Internet-Draft on Assigned Names and Number Allocation (ANANA[47]). In this work and in the software we have written to implement the ANANA protocols, we demonstrate how a series of specifications and protocols can be used to automate namespace management and to provide a clean separation between the policy aspects of allocating names and the technical aspects of access control, validation of incoming requests for allocation, and distribution of results. Our work is based on some extensions to the XML protocols to add access control capability to logical namespaces and has service specifications that allow batch and interactive modes of accessing the service.

As a proof of concept of the ANANA concepts, we have applied them to a variety of core Internet namespaces, including the IANA registries. It is our hope to begin applying these same concepts to the concept of personal and organizational namespaces. If our research and implementation proves successful, we will attempt to apply the work to the modernization of existing personal and organizational registry solutions, such as Whois.

Again, it is important to note that the advanced development aspect of our work is separated from the core operations functions. A "5 nines," rock-solid operational service is the goal for our operation of the .org TLD. Our advanced development is but one of many sources of improvements to how registries operate, and when it comes to modifications in the core service we look to our customers, other registries, standards bodies, and ICANN for guidance.

The marketing of .org is the third method by which we differentiate this TLD. We have strong roots in the noncommercial world, our team has several prolific writers and public speakers, and we have very strong experience using the Internet to reach out to new communities. As the operators of the .org TLD, we intend to apply those skills with vengeance to make .org a dynamic, useful home for the noncommercial organizations of the world.

Deep domains were the original intention of the DNS architects. They thought most users of the Internet would occupy 3rd and 4th levels of the domain hierarchy. For example, Marshall T. Rose registered his domain name under dbc.mtview.ca.us, for the Mt. View subdomain of the California subdomain of the U.S. TLD. Over time, it was thus with some surprise that the DNS architects saw their system evolve from a tree into a bush.

Our deep domains program will attempt to develop well-known resources in the .org TLD. For example, our own resource.org domain includes three well-developed branches: public.resource.org, bulk.resource.org, and xml.resource.org. We intend to develop media.org, phone.org, fax.org, and resource.org into utilities for the general public. We will also work with other .org registrants to encourage them to develop their domains to include broad communities of users or to become general-purpose public utilities.

In sum, a well-run public utility responsive to the needs of users and able to achieve both stability and innovation is the differentiation we propose for the .org TLD.

C39. Intentionally omitted.

---

11. [C40] The VeriSign Endowment

TOC

?

C40. The current .org registry agreement between ICANN and VeriSign, Inc., states:

> 5.1.4 No later than 90 days prior to the Expiration Date, [VeriSign] will pay to ICANN or ICANN's designee the sum of US $5 million, to be used by ICANN in it sole discretion to establish an endowment to be used to fund future operating costs of the non-profit entity designated by ICANN as successor operator of the .org registry. [VeriSign] agrees that such funds, once paid to ICANN, will become the property of ICANN and/or ICANN's designee, and that [VeriSign] will have no ownership or other rights or interests in such funds or in the manner in which they are used or disbursed.

C41. Do you propose to seek to qualify to receive any funds from this endowment?

Yes.

?

C41.1. If so, describe in detail how you propose to use this endowment. Include the commitments you propose to make about the uses to which the endowment would be put. Explain why those uses are consistent with the smooth, stable transition and operation of the .org TLD for the benefit of current and future .org registrants.

Our financial analysis in the attached Consolidated Pro Forma Financial Analysis details our revenue and expense projections under various market conditions. Our primary goal is stability of the .org TLD service. As such we have set a minimum of US$500,000 in operating capital for each month of operation. Our startup costs our financed by our own capital, supplemented by a US$2.5 million line of credit of which we anticipate drawing US$1.5 million for startup costs, leaving a substantial cushion for changes in market conditions.

We would use the VeriSign endowment to more quickly achieve our goals for stability. As detailed in [C25] Registry Services for Fee, this would result in lower costs to consumers as well as increased stability of the .org TLD.

We would also use the VeriSign endowment to accelerate deployment of our core deliverables, including the production of freely available software for registrars and registries, and to more quickly productize innovations such as namespace management from our advanced development program.

We would use also use the VeriSign endowment to accelerate our Internet Public Works Program, which is used to fund programs that differentiate the .org registry and produce solutions for core Internet infrastructure. For example, use of the endowment would accelerate the deployment of BIND 9 and secure DNS.

Finally, we would use the VeriSign endowment to work with other organizations on the net to provide services that benefit the .org registrants and core Internet infrastructure. An example of such cooperation is detailed in the accompanying Intent to Donate in which we certify our intention to use 8% of gross revenues to fund IETF and IAB activities in the Internet Society. Program Managers, in close cooperation with .org registrants, registrars, and registries, will develop proposals for other such programs to be reviewed in a public comment period and then decided by our board of directors.

? **C41.2.** If you propose to seek to qualify to receive the endowment funds, explain why you believe that your proposed use is consistent with the terms of the endowment.

We are a non-profit entity and our operation of the .org registry as a public service with benefit to .org registrants, the marketplace, and the broader Internet community at large, is entirely consistent, indeed is the essence of, the terms of the endowment.

We are fully prepared and capable of operating the .org registry without the VeriSign endowment, but we believe that our use of those funds will provide greater public benefit to current .org registrants and to other registry operators, including future operators of the .org TLD.

12. [C50] Supporting Documentation

TOC

? **C50.** The following documentation should be provided in support of your .org Proposal:

? **C50.1.** Organizational documents of applicant. A copy of the organizational documents (articles of association, bylaws, enabling legislation, etc.) of the applicant.

Attached are the following documents for the Internet Multicasting Service.

- Delaware - Articles of Incorporation
- Delaware - Restated Articles of Incorporation
- Delaware - Certificate of Good Standing
- IRS - Preliminary 501(c)(3) Ruling
- IRS - Final 501(c)(3) Ruling
- California - Certificate of Qualification
- California - Tax Exempt Status Ruling

Attached are the following documents for the Internet Software Consortium:

- California - Articles of Incorporation
- California - Bylaws

? **C50.2.** Organizational documents of certain other entities. A copy of the organizational documents of each non-profit entity identified in item C13.

Please see previous section C50.1.

? **C50.3.** Business references. A list of significant trade and credit references of the applicant and each entity identified in item C13.

For the Internet Multicasting Service:

- Perkins Coie, LLP
  1201 Third Avenue, 40th Floor
  Seattle, Washington 98101-3099
  +1.206.583.8888

- UUNET/Worldcom
  22001 Loudoun County Parkway
  Ashburn, VA 20147
  +1.877.709.8901

- Oracle Corporation
  500 Oracle Parkway
  Redwood Shores, CA 94065

+1.650.506.7000

For the Internet Software Consortium:

- Acme Byte & Wire
  5802 Linder Lane
  Bethesda, MD 20817
  +1.301.571.0444

- McKenna & Cuneo, LLP
  1900 K Street NW
  Washington, D.C. 20008
  +1.202.498.7500

- Telnet Systems Solutions Inc
  2480 Kruse Drive
  San Jose, CA 95131
  +1.408.383.0334

For account numbers and contact names, please contact us.

C50.4. Annual reports. A copy of the most recent annual financial report (or similar document), if any, of the applicant and each entity identified in item C13.

Attached are the following documents:

- Tax Returns for IMS for 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, and 2001.
- Audited Financials for IMS for 1999-2001.
- Compiled Financials for IMS for Q1/2002.
- Tax Returns for ISC for 2001.
- Audited Financials for ISC for 2000.

A full on-line due diligence area is maintained by the Internet Multicasting Service. Please contact us for login information.

C50.5. Evidence of commitment. Any documentation requested by item C14.

Please see the attached Joint Statement of Authority.

C50.6. Evidence of community support. Any documentation requested by item C36.

Please see [C36] Support for Proposal and http://trusted.resource.org/.

13. Signature and Certification

TOC

By signing this .org Proposal, the undersigned certifies (a) that he or she has authority to do so on behalf of the applicant and, (b) on his or her own behalf and on behalf of the applicant, that all information contained in this proposal, and all documents attached to this proposal, is true and accurate to the best of his/her/its knowledge and information. The undersigned and the applicant understand that any material misstatement or misrepresentation will reflect negatively on the application of which this proposal is a part and may cause cancellation of any delegation of a top-level domain based on that application.

/Carl Malamud/
Signed

Carl Malamud

Normative References

TOC

[1] Hollenbeck, S. and M. Srivastava, "NSI Registry Registrar Protocol (RRP) Version 1.1.0", RFC 2832, May 2000.
[2] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.
[3] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.
[4] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.
[5] Harrenstien, K., Stahl, M. and E. Feinler, "NICNAME/WHOIS", RFC 954, October 1985.
[6] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.
[7] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
[8] Mockapetris, P., "DNS encoding of network names and other types", RFC 1101, April 1989.
[9] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.
[10] Elz, R., Bush, R., Bradner, S. and M. Patton, "Selection and Operation of Secondary DNS Servers", BCP 16, RFC 2182, July 1997.
[11] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.
[12] Eidnes, H., de Groot, G. and P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, March 1998.
[13] Waitzman, D., "IP over Avian Carriers with Quality of Service", RFC 2549, April 1999.
[14] Hollenbeck, S., "Extensible Provisioning Protocol", draft-ietf-provreg-epp-06 (work in progress), January 2002.
[15] Hollenbeck, S., "Extensible Provisioning Protocol Domain Name Mapping", draft-ietf-provreg-epp-domain-04 (work in progress), January 2002.
[16] Hollenbeck, S., "Extensible Provisioning Protocol Host Mapping", draft-ietf-provreg-epp-host-04 (work in progress), January 2002.
[17] Hollenbeck, S., "Extensible Provisioning Protocol Contact Mapping", draft-ietf-provreg-epp-contact-04 (work in progress), January 2002.
[18] Hollenbeck, S., "Extensible Provisioning Protocol Transport Over TCP", draft-ietf-provreg-epp-tcp-04 (work in progress), January 2002.

Select RFCs By Team Members

TOC

[19] Horton, M. and R. Adams, "Standard for interchange of USENET messages", RFC 1036, December 1987.
[20] Malamud, C. and M. Rose, "Principles of Operation for the TPC.INT Subdomain: Remote Printing -- Technical Procedures", RFC 1528, October 1993.
[21] Malamud, C. and M. Rose, "Principles of Operation for the TPC.INT Subdomain: Remote Printing -- Administrative Policies", RFC 1529, October 1993.
[22] Malamud, C. and M. Rose, "Principles of Operation for the TPC.INT Subdomain: General Principles and Policy", RFC 1530, October 1993.
[23] Rose, M., "Principles of Operation for the TPC.INT Subdomain: Radio Paging -- Technical Procedures", RFC 1703, October 1994.
[24] Davis, C., Vixie, P., Goodwin, T. and I. Dickinson, "A Means for Expressing Location Information in the Domain Name System", RFC 1876, January 1996.

[25] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, August 1996.

[26] Rekhter, Y., Thomson, S., Bound, J. and P. Vixie, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[27] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[28] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[29] Crawford, M. and C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", RFC 2874, July 2000.

[30] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[31] Vixie, P. and D. Wessels, "Hyper Text Caching Protocol (HTCP/0.0)", RFC 2756, January 2000.

[32] Gulbrandsen, A., Vixie, P. and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[33] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[34] Rose, M., "The Blocks Extensible Exchange Protocol Core", RFC 3080, March 2001.

[35] Rose, M., "Mapping the BEEP Core onto TCP", RFC 3081, March 2001.

[36] Rose, M., "On the Design of Application Protocols", RFC 3117, November 2001.

[37] New, D. and M. Rose, "Reliable Delivery for syslog", RFC 3195, November 2001.

Current Internet-Drafts by Team Members

TOC

[38] Abley, J., "Edge Policy Propagation Control", draft-jabley-eppc-00 (work in progress), February 2002.

[39] Manning, B., Vixie, P. and E. Guttman, "The DISCOVER opcode", draft-dnsext-opcode-discover-00 (work in progress), April 2002.

[40] Rose, M., "A Transient Prefix for Identifying Profiles under Development by the Working Groups of the IETF", draft-mrose-beep-transientid-02 (work in progress), March 2002.

[41] Rose, M., Crocker, D. and G. Klyne, "The APEX Presence Service", draft-ietf-apex-presence-06 (work in progress), January 2002.

[42] Rose, M., Masinter, L. and S. Hollenbeck, "Guidelines for The Use of XML within IETF Protocols", draft-hollenbeck-ietf-xml-guidelines-04 (work in progress), June 2002.

[43] Rose, M., Crocker, D. and G. Klyne, "The Application Exchange Core", draft-ietf-apex-core-06 (work in progress), January 2002.

[44] Rose, M., "IM Simple Exchange (IMSX)", draft-mrose-simple-exchange-01 (work in progress), January 2002.

[45] Rose, M., Crocker, D. and G. Klyne, "The APEX Access Service", draft-ietf-apex-access-08 (work in progress), January 2002.

[46] Rose, M. and D. Crocker, "Toward a Quantitative Analysis of IETF Productivity", draft-etal-ietf-analysis-00 (work in progress), March 2002.

[47] Rose, M., "The ANANA Datastore", draft-anana-datastore (work in progress), June 2002.

Books by Team Members

TOC

[48] Malamud, C., "DEC Networks and Architectures", February 1989.

[49] Malamud, C., "Ingres", July 1989.

[50] Malamud, C., "Stacks : Interoperability in Today's Computer Networks", October 1991.

[51] Malamud, C., "Exploring the Internet: A Technical Travelogue", October 1992.

[52] Malamud, C., "Analyzing Sun Networks", June 1991.

[53] Malamud, C., "Analyzing DECnet/OSI Phase V", August 1991.

[54] Malamud, C., "Analyzing Novell Networks", July 1992.

[55] Malamud, C., "A World's Fair for the Global Village", September 1997.

[56] Rose, M., "The Open Book: A Practical Perspective on OSI", January 1990.

[57] Rose, M., "The Internet Message : Closing the Book With Electronic Mail (Prentice Hall Series in Innovative Technology)", October 1992.

[58] Rose, M. and D. Lynch, "The Internet Handbook", January 1993.

[59] Rose, M. and K. McCloghrie, "How to Manage Your Network Using SNMP", January 1995.

[60] Rose, M., "The Simple Book: An Introduction to Internet Management, Revised Second Edition", March 1996.

[61] Rose, M. and D. Strom, "The Simple Book", July 1998.

[62] Rose, M., "BEEP: The Definitive Guide", March 2002.

[63] Vixie, P. and F. Avolio, "Sendmail: Theory and Practice", December 2001.

Web Sites by Team Members

TOC

[64] Malamud, C., "http://town.hall.org/", April 1993.

[65] Rose, M. and C. Malamud, "http://www.tpc.int/", August 1993.

[66] Malamud, R. and C. Malamud, "http://mappa.mundi.net/", June 1999.

[72] Internet Software Consortium, "http://f.root-servers.org/", August 1999.

[73] Rose, M., "http://www.beepcore.org/", July 2000.

[74] Malamud, R. and C. Malamud, "http://betterdogfood.com/", July 2000.

[75] Malamud, R., "http://undesign.org/", April 2001.

[76] Malamud, R. and C. Malamud, "http://nate.malamud.com/", April 2001.

[77] Rose, M., "http://xml.resource.org/", July 2001.

[78] Malamud, R. and C. Malamud, "http://bulk.resource.org/", December 2001.

[79] Vixie, P. and F. Avolio, "http://smtp.al.org/", December 2001.

[80] Malamud, R. and C. Malamud, "http://not.invisible.net/", December 2001.

Authors' Addresses

TOC

Internet Multicasting Service
P.O. Box 217
Stewarts Point, CA 95450
US
Phone: +1.707.847.3720
Fax: +1.415.680.1556
URI: http://not.invisible.net/

Internet Software Consortium
950 Charter Street
Redwood City, CA 94063
US
Phone: +1.650.779.7000
Fax: +1.650.779.7055
URI: http://www.isc.org/

TOC

Appendix A. Escrow Data Format

A.1 Domain Format

- Domain:
- Nameserver:
- Updated Date:
- Updated By:
- Created Date:
- Created By:
- Last Transferred:
- Registrar:

A.2 Nameserver Format

- Nameserver:
- IPv4:
- IPv6:
- Updated Date:
- Updated By:
- Created Date:
- Created By:
- Registrar:

A.3 Registrar Format

- Registrar Name:
- Address:
- Phone Number:
- Email:
- Whois Server:
- Referral URL:
- Billing Contact:
- Phone Number:
- Email:
- Technical Contact:
- Phone Number:
- Email:

A.4 Contact Format

Contact-ID:

Name:

Status:

Association status:

Organization:

Address:

Phone :

Fax:

Email Address:

Associated Registrar:

Created Date:

Modified Date:

A.5 Escrow Format Example

- Domain: example.org
- Nameserver: ns1.example.org
- Nameserver: ns2.example.org
- Updated Date: 10-Jun-2002 17:18:07 EDT
- Updated By: REGISTRAR-A
- Created Date: 11-Apr-2001 13:02:05 EDT
- Created By: REGISTRAR-A
- Last Transferred:
- Registrar: REGISTRAR-A
- Nameserver: ns1.example.org
- IPv4: 10.10.10.1
- Updated Date:
- Updated By:
- Created Date: 10-Jun-2002 17:18:27 EDT
- Created By: REGISTRAR-A
- Registrar: REGISTRAR-A
- Nameserver: ns2.example.org
- IPv4: 10.10.11.1
- Updated Date:
- Updated By:
- Created Date: 10-Jun-2002 17:18:17 EDT
- Created By: REGISTRAR-A
- Registrar: REGISTRAR-A
- Registrar Name: Example Registrar, Inc.
- Address: 512 Main St
- Phone Number: +1.800.555.1212
- Email: support@example.org
- Whois Server: whois.example.org
- Referral URL: http://www.example.org
- Billing Contact: Sarah Foo Bar
- Phone Number: +1.800.555.1212
- Email: accounting@example.org
- Technical Contact: Support
- Phone Number: +1.800.555.1213
- Email: support@example.org

Appendix B. Registry/Registrar E-Mail Templates

TOC

On occasion the registry may send e-mail notifications to registrars, as described in Message Passing to Registrars. The machine-readable portions of these e-mails will be formatted as follows.

B.1 Receipt of Transfer Request

Message subject: "Receipt of Transfer Request: <domain>.ORG"

Message body as follows:

```
------------------------------------------------------------
Transfer Request for:

Domain Name: <domain>.ORG
Requesting Registrar: <textual registrar name>
Current Registrar: <textual registrar name>

<multi-line human-readable descriptive text>
------------------------------------------------------------
```

B.2 Completion of Transfer Request

Message subject: "Completion of Transfer Request: <domain>.ORG"

Message body as follows:

```
------------------------------------------------------------
Notification of Completion of Transfer Request

Domain Name: <domain>.ORG
Requesting Registrar: <textual registrar name>
Current Registrar: <textual registrar name>

<multi-line human-readable descriptive text>
------------------------------------------------------------
```

B.3 Auto-Acknowledgement of Transfer Request

Message subject: "Auto-Acknowledgement of Transfer Request: <domain>.ORG"

Message body as follows:

```
------------------------------------------------------------
Notification of Auto-Acknowledgement of Transfer Request:

Domain Name: <domain>.ORG
New Registrar: <textual registrar name>
Previous Registrar: <textual registrar name>

<multi-line human-readable descriptive text>
------------------------------------------------------------
```

B.4 Non-Completion of Transfer Request

Message subject: "Non-Completion of Transfer Request: <domain>.ORG"

Message body as follows:

```
------------------------------------------------------------
Notification of Decline of Transfer Request

Domain Name: <domain>.ORG
Requesting Registrar: <textual registrar name>
Current Registrar: <textual registrar name>

<multi-line human-readable descriptive text>
------------------------------------------------------------
```

Appendix C. Initial Whois Output Format

TOC

The following template describes the machine-parsable portions of the output from whois.isc.org for queries corresponding to domains with no associated contact objects.

```
------------------------------------------------------------
Whois Server Version <version>

<multi-line human-readable descriptive text>

   Domain Name: <domain>.ORG
   Registrar: <textual registrar name>
   Whois Server: <referral (registrar) Whois server name>
   Referral URL: <referral (registrar) URL>
   Nameserver: <hostname>
   Nameserver: <hostname>
   <0 to 11 additional Nameserver records>
   Updated Date: <DD-MMM-YYYY>


>>> Last update of Whois database: <date in common UNIX format> <<<

<multi-line human-readable descriptive text>
------------------------------------------------------------
```

Appendix D. Thick Record Whois Output Format

TOC

The following template describes the machine-parsable portions of the output from whois.isc.org for queries corresponding to domains with associated contact objects.

```
------------------------------------------------------------
Whois Server Version <version>

<multi-line human-readable descriptive text>

   Domain Name: <domain>.ORG
   Registrar: <textual registrar name>
   Referral URL: <referral (registrar) URL>
   Nameserver: <hostname>
   Nameserver: <hostname>
   <0 to 11 additional Nameserver records>
   Updated Date: <DD-MMM-YYYY>

   Registrant name: <textual registrant name>
   Registrant street 1: <address information>
   Registrant street 2: <address information>
   Registrant city: <address information>
   Registrant region: <address information>
   Registrant code: <address information>
   Registrant country: <address information>

   Admin name: <textual registrant name>
   Admin e-mail: <e-mail address>
   Admin phone: <phone number>
   Admin fax: <phone number>
   Admin street 1: <address information>
   Admin street 2: <address information>
   Admin city: <address information>
   Admin region: <address information>
   Admin code: <address information>
   Admin country: <address information>

   Technical name: <textual registrant name>
   Technical e-mail: <e-mail address>
   Technical phone: <phone number>
   Technical fax: <phone number>
   Technical street 1: <address information>
   Technical street 2: <address information>
   Technical city: <address information>
   Technical region: <address information>
   Technical code: <address information>
   Technical country: <address information>


>>> Last update of Whois database: <date in common UNIX format> <<<
------------------------------------------------------------
```

Appendix E. Biographies of Key Personnel

TOC

E.1 Program Managers

E.1.1 Carl Malamud

Carl Malamud created the first Internet radio station and put the SEC's EDGAR database on-line. A serial social entrepreneur, he's helped establish and lead a number of non-profit organizations, including the Internet Multicasting Service and the Internet Software Consortium. He was founding CEO of two Silicon Valley startups which he led through several rounds of financing, was a visiting professor at the MIT Media Lab and Keio University, and has 20 years experience leading large-scale computer networking projects in the public and private sectors. Carl is the author of 8 books, numerous articles, and a few RFCs.

E.1.2 Rebecca Malamud

Rebecca Malamud's interface design and creative work has been profiled by numerous organizations, including The Art Directors Club of New York, Communication Arts, USA Today, CNN, The New York Times, The Wall Street Journal, and ABC News. A career creative hell-bent on true community, Rebecca has led the creative and community efforts of the Internet Multicasting Service since 1995 including primary operating responsibility for projects such as the Internet 1996 World Exposition, Mappa.Mundi Magazine, north.pole.org, and many others. She has worked in executive and creative direction positions in numerous organizations ranging from Silicon Valley startups to traditional print shops and is responsible for a large number of community-based Internet projects.

Becky's latest creation is IMS Signals, the first glimpse of an architecture for conversational applications that will form the form the foundation for the IMS NetTopBox and Core Technologies Programs.

E.1.3 Paul Vixie

Paul Vixie has been contributing to Internet protocols and UNIX systems as a protocol designer and software architect since 1980. Early in his career, he developed and introduced sends, proxynet, rtty, cron and other lesser-known tools. Today, Paul is considered the primary modern author and technical architect of BINDv8 the Berkeley Internet Name Domain Version 8, the open source reference implementation of the Domain Name System (DNS). He formed the Internet Software Consortium (ISC) in 1994, and now acts as Chairman of its Board of Directors. The ISC reflects Paul's commitment to developing and maintaining production quality open source reference implementations of core Internet protocols.

More recently, Paul co-founded MAPS LLC (Mail Abuse Prevention System), a California non-profit company established in 1998 with the goal of hosting the RBL (Realtime Blackhole List) and stopping the Internet's email system from being abused by spammers. Vixie was also the Chief Technology Officer of Metromedia Fiber Network Inc (MFNX.O).

Along with Frederick Avolio, Paul co-wrote "Sendmail: Theory and Practice" (Digital Press, 1995:2001). He has authored or co-authored several RFCs, including a Best Current Practice document on Classless IN-ADDR.ARPA Delegation.[12] He is also responsible for overseeing the operation of F.root-servers.net, one of the thirteen Internet root domain nameservers.

E.1.4 Suzanne Woolf

Suzanne Woolf worked from 1989-2000 at the Information Sciences Institute, where she worked in the Network Division. Her assignments included automation of record keeping for the IANA, operations of the RWhois service for the .US domain, and technical support to a variety of government- and privately-funded projects in network technology development. She served as the Technical Operations Manager for ICANN during its first year of operation. Before joining the Internet Software Consortium as Program Manager, she was Manager of Operations Systems and Support for a large ISP.

E.2 Additional Personnel

E.2.1 Joe Abley

Joe Abley has worked in numerous positions as a lead engineer including backbone architecture, design, deployment, and maintenance for the AboveNet/MFN global IP network and technical lead in the early design work which led to the roll-out of Telstra Saturn's (now TelstraClear's) broadband packet VPN infrastructure in New Zealand. He led the design and and deployment of nameserver infrastructure for the AQ, TK and PN country-code top-level domains. Joe was the architect and deployment prime for a high-capacity international network between NZ and the USA for Internet access, using unidirectional satellite broadcast in conjunction with bi-directional under-sea cable, with appropriate latency-sensitive traffic prioritization over the satellite and terrestrial paths.

Joe participates actively in NANOG, NZNOG and the IETF and is author or co-author of publications on Edge Policy Propagation Control[38], and IPv4 multi-homing and IPv6 multihoming. He is a contributor to OpenBSD, FreeBSD, and ISC BIND.

E.2.2 Luther Brown

Luther Brown began his career at CBS, then moved on to NBC News where he produced political and campaign coverage for ten years. He has worked in such diverse areas as speechwriting for the U.S. Secretary of Health and Human Services, developing training material for the Environmental Protection Agency, representing the Wilderness Society, and producing and consulting on broadcast issues for the City of Atlanta. Luther received his law degree from Georgetown University Law Center and pursued doctoral coursework in English at Rutgers.

E.2.3 Brad Burdick

Brad Burdick has run systems for IMS since 1993. He personally oversaw the operation of the first 24-hour/day streaming audio and video feeds on the Internet, turned EDGAR and Patents into the world's largest WAIS database and then converted most of the U.S. government into XML, and in 1996 helped activate the first Internet DS3 over the Pacific ocean, part of a network that included a 2-terabyte disk farm distributed in 8 countries.

E.2.4 Michael Graff

Michael Graff is a lead contributor to BIND 8, BIND 9, and NetBSD. He is the author of loadable device modules for file systems under NetBSD and he has done device driver programming for DS3, HSSI, and T1 interface cards for NetBSD, FreeBSD, BSDI, and linux. In addition to his work on BIND at ISC, Michael coordinated over 1200 individuals for the RSA-129 project, which factored a large cryptographically secure number. Prior to working for ISC, Michael was the author of the first generation of PGP Key Servers, which were in use at over 50 sites in 10 countries. He was also the coordinator of the PGP Network, the collection of PGP Key Servers.

E.2.5 Lynda McGinley

Lynda McGinley is the Executive Director of the Internet Software Consortium. Lynda has been active in system and network administration for the past 16 years, working at the University of Colorado, Qwest Advanced Technologies, and Network Daemon Associates. She has been managing the USENIX terminal room for the past 5 years. Lynda has been President of the Board of Directors of the Colorado Internet Cooperative, and a member of the Board of Directors of XOR Networking Engineering, Inc.

Lynda is a contributing author of the third edition of the UNIX System Administration Handbook. She is professionally active in SAGE, USENIX, and FRUUG.

E.2.6 Rick H. Wesson

Rick H. Wesson is a technical expert in the areas of DNS & Registry Registrar Protocols; Automation of Provisioning Systems; and, Online Fraud Detection. He has the following affiliations:

- CEO, Alice's Registry, Inc.
- CTO, ICANN/DNSO Registrars Constituency
- Director, Santa Cruz Community Credit Union
- Member, ICANN Security and Stability Advisory Committee
- Member, ICANN Technical Steering Group on Redemption Grace Periods for Deleted Names

Rick has consulted in the San Francisco Bay Area since 1993 working for a variety of technology companies. In 1999, he was the technical lead for CORE, one of the first testbed registrars. In 2000-2002, he helped build the technical infrastructure of many ICANN accredited registrars, including Name Secure, Domain Bank, PSI-Japan, TuCows, Catalog.com, and other DNS related companies like Nominum and Name Zero. He continues to provide protocol implementations for registrars for RRP, EPP, and Whois.

E.3 Board Members

E.3.1 Rick Adams

Rick Adams is the founder of UUNET Technologies and the author of RFC 1036.[19] He serves on the board of the Internet Multicasting Service.

E.3.2 Dave Farber

Dave Farber is the Alfred Fitler Moore Professor of Telecommunication Systems in the School of Engineering and Applied Sciences at the University of Pennsylvania and Professor of Business and Public Policy at the Wharton School. A former Chief Technologist for the FCC, he is the creator of the interesting-people list.

E.3.3 Teus Hagen

Teus Hagen has been involved in many aspects of the Internet and has been a key participant in the growth of the net in Europe. He was the principal founder of the Dutch UNIX users group NLUUG and the European UNIX Users Group (EUUG), the umbrella organization for 26 national UNIX users groups and the European sister organization of USENIX.

In 1994, he joined the NLnet Foundation as President. NLnet was reorganized as a corporation with the Foundation as sole shareholder. Currently, he is the general director and president for the NLnet Foundation. In 1997 the NLnet ISP Corporation was sold to UUnet/Worldcom, at which time the Foundation began leading and sponsoring Internet technology research and development projects in Holland, Europe and the world, including funding for the Internet Software Consortium.

E.3.4 Carl Malamud

Carl Malamud

E.3.5 Rebecca Malamud

Rebecca Malamud

E.3.6 Evi Nemeth

Evi Nemeth is retired from the Department of Computer Science at the University of Colorado and is a part-time researcher at CAIDA, the Cooperative Association for Internet Data Analysis at the University of California's San Diego Supercomputer Center. She has coordinated MBONE broadcasts from the IETF, INET, and USENIX since 1993. She has served on the boards of directors of the Internet Software Consortium and the Colorado Internet Cooperative. Evi's current research focuses on DNS behavior and performance at the root nameserver level, including recent publications on DNS Root/gTLD Performance Measurements and DNS Measurements at a Root Server.

E.3.7 Marshall T. Rose

A member of the IMS Board of Directors since 1993, Marshall lives with internetworking technologies as a theorist, implementer, and agent provocateur. He is held accountable for the design, specification, and implementation of several Internet-standard technologies, and is an author of over 60 of the Internet's Request for Comment (RFC) Series. He is the author of several professional texts on network management, electronic mail, directory services, and application framing protocols. His latest book is The Beep Book. Marshall chairs the Protocol Advisory Board, which provides a technical reality check to work products before they are submitted as Internet-Drafts and participates actively in the Core Technologies Program. His most recent work for IMS has been definition of the ANANA Datastore.

E.3.8 Paul Vixie

Paul Vixie

E.3.9 Stephen Wolff

Stephen Wolff taught Electrical Engineering in The Johns Hopkins University for ten years and subsequently spent fifteen years leading a computing- and network-related research group at the U.S. Army Research Laboratory. In 1983 he took a sabbatical half-year as a Program Director in the Mathematics Division of the U.S. Army Research Office.

From 1986 to 1995 he was Director of the Division of Networking and Communications Research and Infrastructure (NCRI, now ANIR) at the U.S. National Science Foundation, responsible for the NSFNET, the NSF participation in the National Research and Education Network element of the HPCC program, and NSF's support programs for basic research in networking and communications. While at NSF, he was among the founders of the inter-agency and international research networking management and advisory structure whose descendants today include the Large-Scale Networking (LSN) working group and the President's Information Technology Advisory Committee (PITAC).

He left Federal service and joined Cisco Systems in 1995, where he currently directs the Advanced Internet Initiatives Division with responsibility for Cisco's participation in Internet2, the U.S. government's Next Generation Internet and IT2 programs, and similar and related projects both domestically and abroad. Dr. Wolff holds two patents and is the author of several dozen technical reports and articles; he a member of AAAS and ACM, a Pioneer Member of the Internet Society, and a Life Member of IEEE.

E.3.10 Pindar Wong

Pindar Wong (pindar@hk.super.net) is the immediate past Chairman of the Asia and Pacific Internet Association, the Executive Committee Chairman of the Asia Pacific Regional Internet Conference on Operational Technologies, Advisor to the Asia Pacific Networking Group, and Member of the Editorial Advisory Board of Cisco Systems' Internet Protocol Journal. He is also the Chairman of VeriFi (Hong Kong) Ltd., a discrete Internet infrastructure consultancy. Previously he co-founded Hong Kong's first licensed ISP in 1993, was the alternate chair of Asia Pacific Network Information Centre, and was appointed by the Internet Architecture Board to the Policy Oversight Committee. He served as Vice Chairman of ICANN's Board of Directors from 1999-2000 and Vice-Chairman of the At Large Study Committee 2001-2002. Prior to his involvement in commercial Internet services, he was a doctoral candidate and Sir Edward

Youde research fellow at the Hong Kong University of Science and Technology.

Appendix F. Document Formats

TOC

This document is available in the following formats:

- [html] This document.
- [htm] ICANN original form.
- [xml] XML[27] format.
- [txt] ASCII
- [nroff] NROFF
- [word] Word
- [pdf] PDF

TOP THE .ORG TLD IS A PUBLIC TRUST »