New gTLD Application Submitted to ICANN by: Medistry LLC

String: MED

Originally Posted: 13 June 2012

Application ID: 1-907-38758

Applicant Information

1. Full legal name

Medistry LLC

2. Address of the principal place of business

3029 Prospect Avenue
Cleveland Ohio 44115
US

3. Phone number

1 216 361 1000

4. Fax number

5. If applicable, website or URL

Primary Contact

6(a). Name

Mr. Brian David Johnson

6(b). Title

Secretary and General Counsel

6(c). Address

6(d). Phone Number

1 216 361 1000

6(e). Fax Number

1 216 426 1400

6(f). Email Address

bdj@secondgen.com

Secondary Contact

7(a). Name

Mr. Scott Curtis Finerman

7(b). Title

Chief Financial Officer

7(c). Address

7(d). Phone Number

1 216 361 1000

7(e). Fax Number

1 216 426 1400

7(f). Email Address

scf@partnerss.com

Proof of Legal Establishment

8(a). Legal form of the Applicant

Delaware Limited Liability Company

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

Delaware LLC law

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

11(b). Name(s) and position(s) of all officers and partners

Brian D. Johnson	Secretary & General Counsel
Dr. C. Martin Harris	Executive Advisor
Dr. Delos M. Cosgrove	Executive Advisor
F. Matthew Embrescia	President
Ray W. Fassett	Executive Vice President
Scott C. Finerman	Chief Financial Officer
Thomas J. Embrescia	Chairman

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

CC Web Solutions, Inc.	Not Applicable
Second Genistry LLC	Not Applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

MED

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

Medistry LLC is unaware of any known operational or rendering problems related to the .MED gTLD.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

Question 18 (a)

The Cleveland Clinic (“Cleveland Clinic”), founded in 1921 and headquartered in Cleveland Ohio, today is a $5 billion international medical center with almost 1,000 doctors, offering world-class hospital and outpatient care in virtually every medical specialty. Ranked each year as one of the top five hospital systems in the United States, the Cleveland Clinic is recognized for its achievements in demonstrating unusually high expertise across multiple medical and healthcare related specialties.

The Cleveland Clinic is currently ranked in numerous areas of medical specialty, including rankings of number 1 in Cardiology and Heart Surgery; number 2 in Nephrology; number 2 in Urology; number 2 in Gastroenterology; number 3 in Rheumatology; number 3 in Pulmonology; number 4 in Orthopedics; number 4 in Cardiology; number 5 in Diabetes and Endocrinology; number 6 in Neurology and Neurosurgery; number 7 in Geriatrics; number 7 in Pediatrics: Neurology and Neurosurgery; and number 9 in Cancer. The Cleveland Clinic has received such high rankings on a consistent basis.

Cleveland Clinic’s executive management team includes Dr. Toby Cosgrove (Chief Executive Officer and President of the Cleveland Clinic) and Dr. C. Martin Harris (Chief Information Officer of the Cleveland Clinic).

Dr. Cosgrove presides over a $5 billion healthcare system comprised of the Cleveland Clinic, nine community hospitals, 15 family health and ambulatory surgery centers, Cleveland Clinic Florida, the Lou Ruvo Center for Brain Health in Las Vegas, Nevada, Cleveland Clinic Toronto, and Cleveland Clinic Abu Dhabi. His leadership has emphasized patient care and patient experience, including the re-organization of clinical services into patient-centered, organ and disease-based institutes. He has launched major wellness initiatives for patients, employees and communities.

Dr. Harris, a frequent presenter at national meetings on health care and technology, is on the advisory board of the Association of American Medical Colleges' Better Health 2010 committee and is a judge for the case studies in medicine for The Computerworld Smithsonian Honors Program. He is also a member of the American Medical Informatics Association and the Healthcare Information and Management Systems Society.

The Cleveland Clinic firmly believes that establishment of a .MED top-level domain, imbued with the principles established by the Cleveland Clinic, will promote competition, consumer trust and consumer choice. Towards this end, the Cleveland Clinic has engaged Medistry LLC (“Medistry”) to apply for, obtain and operate the .MED gTLD under guidance and direction from the Cleveland Clinic. Medistry is owned and operated by CC Web Solutions, Inc., a wholly owned subsidiary of the Cleveland Clinic, and Second Genistry LLC, which includes the same management team which owns and operates the .JOBS sponsored gTLD. Both Drs. Cosgrove and Harris serve in the formal capacity of Executive Advisors to Medistry.

The mission⁄purpose of .MED is to perform as a new gTLD consistently with the mission and purpose of the Cleveland Clinic. The mission of the Cleveland Clinic, a nonprofit multispecialty academic medical center, is to integrate clinical and hospital care with research and education. Under the stewardship of the Cleveland Clinic, the .MED gTLD will aim to serve as a source identifier that accomplishes integrating clinical and hospital care with research and education in a digital world, providing a trusted name space wherein users can come to find trusted sources for medical information.

Towards fulfilling this mission⁄purpose, domain registrations in .MED will not be real-time, but instead will be allocated by Requests for Proposals (RFPs) only. RFP applicants will at minimum be required to set forth their qualifications to integrate clinical and hospital care with research and education, and any registration and⁄or use of domain names in .MED will be under terms, policies and guidelines as the Cleveland Clinic so determines in its sole discretion, consistent with the above-stated mission⁄purpose of the .MED gTLD, any applicable ICANN Consensus Policies, ICANN’s registry agreement, any applicable rules of law and Cleveland Clinic-approved guidelines.

The Cleveland Clinic firmly believes that the .MED gTLD, as used to promote the above-stated mission⁄purpose, would provide benefit to Internet users in general. In fulfilling .MED’s mission⁄purpose, the Cleveland Clinic, upon allocation of .MED, intends to explore ways of promoting adoption and use of .MED to fulfill the mission⁄purpose set forth above, and will likely obtain input from a broad range of medical service providers towards investigating many such ways.

One exemplary way the Cleveland Clinic intends to explore is providing geographic, clinical and⁄or other medical-related terms not otherwise reserved from registration and⁄or use for use at the second-level to provide medically-related information in the area associated with the geographic term or the field associated with the clinical⁄medical term. In conjunction with allocation via RFPs, consumer choice is thus promoted by providing an easily accessible and intuitive source for providing medical-related information.

The Cleveland Clinic believes that medical professionals, educators, patients and, generally, consumers associate the Cleveland Clinic with integrating clinical and hospital care with research and education. People have come to trust the care, research and education provided by the Cleveland Clinic. The Cleveland Clinic believes that its stewardship of the .MED gTLD will extend that trust into the DNS namespace for the .MED gTLD, and that such trust would be created in no small part by the Cleveland Clinic’s ability and willingness to protect .MED both through the registration limitations set forth above and compliance with the Cleveland Clinic’s mission. When a consumer visits a .MED domain, she can be assured that the registrant has been reviewed and approved by the Cleveland Clinic, and that any content is consistent with the stated mission⁄purpose of the gTLD.

Medistry will be managed in a highly professional and commercially reasonable manner, consistent with any applicable ICANN Consensus Policies, ICANN’s registry agreement and any applicable rules of law, providing a level of comfort to registrants and Internet users alike as being a gTLD powered by the industry’s leading back end provider (Verisign, Inc.) and backed by a management team already experienced in the operation of a gTLD and with the executive advice of Drs. Cosgrove and Harris.

Medistry pledges to assist ICANN in reviewing the New gTLD Program as specified in section 9.3 of ICANN’s Affirmation of Commitments as such relates to .MED and the materials set forth in this application, including consideration of the extent to which the .MED gTLD has promoted competition, consumer trust and consumer choice, as well as effectiveness of the application and evaluation process for .MED, and all safeguards put in place for .MED to mitigate issues involved in running .MED.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

Question 18(b)

The proposed .MED gTLD will benefit registrants, Internet users and others by, among other reasons, providing a trusted name space wherein users can come to find trusted sources for medical information, consistent with the Cleveland Clinic’s mission of integrating clinical and hospital care with research and education in a digital world. The proposed .MED gTLD will further benefit registrants, Internet users and others by promoting consumer trust by providing a gTLD operated in a professional and commercially reasonable manner by an experienced management team, powered by a world-class back end registry provider (Verisign, Inc.) and backed by the Cleveland Clinic. Use of the .MED gTLD under the Cleveland Clinic’s stewardship will provide new on-line opportunities for medical practitioners, educators, providers, patients, vendors and users alike.

Awareness of the existence of the .MED gTLD will also benefit Internet users -- such awareness will create new choice within the DNS for how to access and locate medically-related information.

Users will also benefit from the trusted, valued nature of the .MED space. Users can be confident that a domain in the .MED gTLD has as its registrant an entity which has been reviewed and approved by the Cleveland Clinic, and any content is consistent with the stated mission⁄purpose of the gTLD.

1. The goals of the .MED gTLD in terms of areas of specialty, service levels and reputation.

A goal of the .MED gTLD is to serve as a trusted source on the Internet for medical-related information, providing people greater choice for obtaining such information. The Cleveland Clinic believes that multiple sectors of the healthcare industry would be implicated in the sharing of trusted information within the .MED gTLD, including:

* eHealthServices, including Telehealth, Remote Services and Non-Acute Services including Home Health, LTAC, Skilled, and Semi-Skilled Providers

* Pharma, including Pharmaceutical Providers and Consumers, Pharmacy and Mail-Order Pharmacy

* Pharmacy Benefits Manager

* Research, both Basic and Clinical

* Chronic Disease Patient Management, including Patient Monitoring

* Personal Health Record

* Medical Devices, including Medical Device Manufacturers

* Durable Medical Equipment, including Medical Device Manufacturers

* Health Exchange

* Medical Education, including health-related educational materials and continuing Medical Education

* Commercial Lab, accommodates both For-Profit and Non-Profit Labs

* Imaging, including Imaging Services

* Genomics, including educators and researchers

While it is not anticipated that all sectors identified above will become registrants of, or even provide content for, domain names within the .MED gTLD, the Cleveland Clinic anticipates that most, if not all of the above sectors involved in the Healthcare ecosystem would likely be interested in participating in some use of trusted information and⁄or services provided via the .MED gTLD.

A further goal of the .MED gTLD is to foster collaboration, in the public interest, for the purpose of a new online experience and environment for producers and users of medical-related information. Such collaboration will be fostered by the selected nature of allocation within the gTLD, and by adherence to the policies, rules and guidelines promulgated by the Cleveland Clinic and implemented by Medistry.

The Cleveland Clinic is associated with trust and professionalism in the provision of care, research and education in the medical field. It is the Cleveland Clinic’s goal to extend such trust and professionalism to operation and use of the .MED gTLD. In this regard, Cleveland Clinic anticipates that the same level of medical specialty, service and reputation associated with the Clinic’s mission⁄purpose in the non-digital world will cross-over to the .MED gTLD.

In terms of service level goals, it is Medistry’s goal for users to experience robust DNS industry standards for technical back-end operations, including but not limited to near 100% uptime; timely zone file dissemination; searchable WHOIS capabilities; and additional security measures such as for DNS Security Extensions (DNSSEC).

In terms of reputation, it is the Cleveland Clinic’s goal to provide a gTLD that upholds the Clinic’s reputation in the medical industry, and it is Medistry’s goal to provide a gTLD operated (and recognized as being operated by users) in a professional and commercially reasonable manner by an experienced management team and powered by a world-class back end registry provider.

2. What the .MED gTLD will add to the current space in terms of competition, differentiation and innovation.

Creation of .MED will provide competition to existing TLD’s in the form of a trusted new name space for provision of medical-related information.

The stewardship of the Cleveland Clinic, along with Medistry’s intended allocation method, both inherently bring differentiation and innovation to the .MED gTLD. As previously noted, domain name registrations in .MED will not be “real-time”. All domain name registrations will take place by Request for Proposal only. Applicants for a .MED domain name will at minimum be required to state their qualifications to integrate clinical and hospital care with research and education. The Cleveland Clinic, through its interest in operating Medistry, is expertly situated to evaluate such applicants and proposals specific to .MED’s mission and purpose.

Applications for a .MED domain name registration will be accepted or rejected at the sole discretion of the Cleveland Clinic. The Cleveland Clinic has the depth, reach, and expertise to foster a collaborative environment for participants to work together for the common good, which will both differentiate .MED from its gTLD brethren and foster innovation in the .MED namespace. The .MED gTLD will evolve to become known as a source destination for medical information which users are able to trust.

The Cleveland Clinic anticipates that proposals will be received from many of the Healthcare sectors mentioned above. Consistent with its stated mission/purpose, the Cleveland Clinic intends to evaluate all such proposals towards creating a trusted, differentiated namespace for the exchange of medical-related information, and further for the promulgation of any use/registration/RFP policies, rules and/or guidelines, as the Cleveland Clinic sees fit in its sole discretion as the steward of the .MED gTLD, to foster user awareness, adoption, growth and use of the gTLD, all within the confines of the stated mission/purpose.

Over time, the Cleveland Clinic anticipates a single dedicated name space under the unique .MED gTLD, in combination with the reputation and professionalism users associate with the Cleveland Clinic, will resonate with users to create differentiation that otherwise could not exist in current gTLD’s. Further, provision of the .MED gTLD as a trusted, valued space will differentiate .MED from other, untrusted TLD’s.

While it is difficult to predict in exact terms what future innovation may occur as a result of the existence of the .MED gTLD, we expect the Cleveland Clinic to demonstrate the same capacity to innovate and adapt as they have shown over nearly one hundred years of operation. One possible example of this innovation which the Cleveland Clinic intends to explore is the option of providing a hierarchical and intuitive framework for the .MED namespace by using geographical identifiers as second-level domain names, as described further in the answer to Question 22.

3. User experience goals of the .MED gTLD.

A goal of .MED is for users to experience robust DNS industry standards for technical back-end operations, including but not limited to near 100% uptime; timely zone file dissemination; searchable WHOIS capabilities; and additional security measures such as for DNS Security Extensions (DNSSEC).

Over time, an additional goal is for users to experience .MED websites as trusted, valued sources for professional clinical information, and particularly medical and care related information. One goal the Cleveland Clinic intends to explore is to provide professional information at domains which are associated with geographic and/or subject matter terms. Over time, users desiring to locate medical and care related information in a specific area, or services in a particular type, will be conditioned to navigate to “geographic.MED” or “subjectmatter.MED”. Consistent with the Cleveland Clinic’s mission/purpose for the .MED gTLD, the Cleveland Clinic will determine, in its sole discretion, who may register domains in .MED.

4. Intended registration policies in the .MED gTLD in support of the goals listed above.

Consistent with the stated mission/purpose for the .MED gTLD, the Cleveland Clinic will determine, in its sole discretion, who may register domains in .MED, and how such domains may be used. The Cleveland Clinic will set forth policies and practices relating to registration and use of domains in .MED which are reasonably necessary for the management, operations and purpose of the gTLD in light of its stated mission/purpose, and which are consistent with such mission/purpose. As set forth above, allocation will be by RFP under guidelines, rules and criteria as set forth by the Cleveland Clinic in its sole discretion.

Additional restrictions, policies or practices may be set forth by the Cleveland Clinic during initial operations of the .MED gTLD so that the .MED gTLD can be launched and initially operated in a controlled manner, granting the gTLD the opportunity to fulfill its stated mission(s)/purpose(s), and allowing the Cleveland Clinic the opportunity to study use of the gTLD and user adoption of the gTLD. Any such restrictions, policies or practices will also allow the Cleveland Clinic the ability to explore and implement user experience goals noted above and to find additional ways of achieving the missions/purposes identified above.

Cleveland Clinic will periodically review progress and adoption of the .MED gTLD with an eye towards maintaining consistency with the gTLD’s stated mission/purpose and achieving the goals set forth above. The Cleveland Clinic – in its sole discretion – may add, delete, amend or otherwise modify registration restrictions, policies and practices in support of the goals listed above. The Cleveland Clinic may also adopt use policies consistent with the principles set forth herein.

5. Measures for protecting the privacy and confidentiality of registrants and users.

Applicant does not at this time propose any measures for protecting the privacy of confidential information of registrants or users of .MED domain names, outside of what is required under applicable statute, contract or law.

6. Outreach and communications which will help achieve projected benefits.

The primary outreach and communications that will occur for .MED will be through the Cleveland Clinic and its related entities through existing channels of communication. Over time, Medistry expects these existing channels of communication to produce widespread awareness for .MED.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

Question 18(c)

It is Medistry’s intent to operate .MED as a restricted gTLD, at least as compared to open, unrestricted TLD’s such as .com and .net, consistent with its stated mission/purpose and employing the registration and use restrictions set forth herein and as promulgated by the Cleveland Clinic from time to time. The restricted nature of the gTLD, along with allocation via RFP, will help eliminate or minimize social costs, as registrants will be limited to individuals or entities which have been vetted by the Cleveland Clinic. Further, the .MED gTLD implicates Cleveland Clinic’s reputation, further minimizing or eliminating social costs as compared to users/operators of unrestricted gTLD’s, which have no such reputations to protect.

To further help eliminate or minimize social costs, Medistry will implement all abuse mitigation and rights protection mechanisms set forth in applicable ICANN Consensus Policies, ICANN’s registry agreement, any applicable rules of law and any policies implicated for compliance with Medistry’s response to Questions 28 and 29 related to mitigation of abusive registrations and rights protection mechanisms.

Medistry and the Cleveland Clinic are both committed to operating the .MED gTLD in a professional and commercially reasonable manner. Medistry does not believe that operating a gTLD in a manner that unreasonably facilitates undue and unreasonable (at Medistry’s sole determination) social costs is professional or commercially reasonable. In that regard, Medistry will reserve the right to adopt registration and use policies as commercially reasonably necessary, in Medistry’s and the Cleveland Clinic’s sole discretion, to mitigate any such undue and unreasonable social costs towards fulfillment of the mission/purpose of the .MED gTLD and the goals set forth in Medistry’s answer to Question 18(b).

1. Resolving multiple applications for a particular domain name.

All domains in the .MED gTLD will be allocated by RFP at the sole discretion of the Cleveland Clinic pursuant to the mission/purpose of the gTLD as set forth herein. Resolution of any contention over a .MED domain name must be consistent with the Cleveland Clinic’s mission and the mission/purpose of the .MED gTLD. In the event multiple applicants are not distinguishable in light of Cleveland Clinic’s mission and the mission/purpose of the gTLD, the Cleveland Clinic will seek to resolve any such contention by encouraging the applicants to work together for the common good and in pursuit of the mission/purpose of the .MED gTLD. In the event the multiple applicants are still not distinguishable, Medistry and the Cleveland Clinic will evaluate industry-practiced and commercially reasonable ways to distinguish the applicants. While the Cleveland Clinic does not intend to use an auction process to resolve any such situations, Medistry and the Cleveland Clinic reserve the right to explore resolving the contention via an auction process. Any such auction, in the event one should take place, would be performed by an experienced domain auction provider under best auction practices. In any event, the Cleveland Clinic reserves the right to make final determinations in all multiple applicant/contention situations.

2. Cost benefits for registrants in the .MED gTLD.

Medistry, in consultation with the Cleveland Clinic, intends to investigate the provision of one or more introductory discounts, advantageous pricing and/or bulk registration discounts during initial operations of the .MED gTLD, and will review the results of any such discount(s) or pricing to determine if further discounts or other advantageous pricing should be implemented at any further time during operations of the .MED gTLD. Medistry, in consultation with the Cleveland Clinic, will receive pricing proposals, including any proposed cost benefits for applicant/registrants, at the discretion of the RFP applicant, and will review any such pricing proposals with the Cleveland Clinic towards final determination regarding any proposal submitted under the RFP.

3. Price escalation.

Medistry does not intend to make contractual commitments to registrants regarding the magnitude of price escalation.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

In responding to the issues indicated in Question 22, Medistry LLC ("Medistry") has considered GAC advice set forth at https://gacweb.icann.org/display/gacweb/New+gTLDs and https://gacweb.icann.org/download/attachments/1540128/gTLD_principles_0.pdf?version=1&modificationDate=1312358178000. Medistry has also considered the methodology developed for the reservation and release of country names in the .INFO tld, and specifically the information relating to .INFO at Resolution 01-92 at http://www.icann.org/en/minutes/minutes-10sep01.htm and ICANN's proposed action plan at http://www.icann.org/en/meetings/montevideo/action-plan-country-names-09oct01.htm . Medistry has also reviewed the Second WIPO Internet Domain Name Process – The Recognition and Rights and the Use of Names in the Internet Domain Name System, Section 6, Geographical Identifiers, at http://www.wipo.int/amc/en/processes/process2/report/html/report.html and ICANN's Generic Names Supporting Organization Reserved Names Working Group – Final Report at http://gnso.icann.org/issues/new-gtlds/final-report-rn-wg-23may07.htm.

Initial Reservation of Country and Territory Names

Medistry is committed to initially reserving, at no cost to governments, public authorities or inter-governmental organizations, the country and territory names contained in the internationally recognized lists described in Article 5 of Specification 5 attached to the New gTLD Applicant Guidebook Draft New gTLD Registry Agreement at the second level and at all other levels within the .MED generic top-level domain (gTLD) at which Medistry will provide for registrations. Specifically, Medistry will reserve:

1. The short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union, http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166- 1_decoding_table.htm - EU;

2. The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and

3. The list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

To the extent Article 5 of Specification 5 of the final version of the New gTLD Registry Agreement is amended to include additional country, territory or other geographic identifiers, Medistry will similarly initially reserve all such names.

It is Medistry's intent to initially reserve the names mentioned above by blocking them from registration at the registry level (for example, Medistry's back end provider, Verisign, would block the names from registration), but Medistry may use any other method for initially reserving the names as not prohibited by the final version of the New gTLD Registry Agreement, such as, for example, registering such names in its own name in order to withhold them from delegation or use.

Use of Non-Reserved Geographical Identifiers

Medistry believes that it is important to be able to register and/or use non-reserved geographical identifiers to promote competition in the DNS, competition among TLD operators, and to promote user acceptance and registrant interest in .MED. However, Medistry recognizes that such registration and/or use should be in a fair and non-misleading manner.

Because of the importance in geographical identification in helping consumers locate medical information, Medistry and the Cleveland Clinic (CC) intend to explore the option of providing a hierarchical and intuitive framework for the .MED namespace by using geographical identifiers as second-level domain names. Medistry and CC believe the use of geographical identifiers to the left of the gTLD and as part of the domain name itself will have a direct and material impact on consumer adoption and search engine algorithms, along with corresponding query results. In addition, such naming conventions are intuitive and practiced by direct navigation Internet users. Medistry and CC believe that .MED may provide an online, single-source identifying function, allowing consumers to locate medical information relating to domain-specified geographic areas. As ICANN has largely premised this new gTLD round on promoting innovation, Medistry and CC would like to determine if this type of hierarchical and intuitive use of second-level domain names within a gTLD provides increased consumer functionality.

Medistry and CC recognize that there is concern regarding misuse of geographical identifiers in the international, regional and national levels. Medistry and CC, acting as responsible global businesses, seek to avoid business practices that could potentially mislead consumers and misuse geographical identifiers. Medistry and CC believe that it is important to be able to use geographical identifiers in a fair and non-misleading manner, as such use can benefit Internet users and consumers.

Medistry’s and CC’s intent is to consider using non-reserved geographic identifiers as part of a hierarchical and intuitive framework in a fair and non-misleading manner to help consumers navigate the .MED namespace. One option that may be considered is creation of GeographicLocation.MED website(s) which include listings of medical information at such “GeographicLocation.” Medistry and CC are committed to operating the .MED namespace in a manner that minimizes potential consumer confusion, and will actively work with others in the ICANN community regarding any future policy development in this area.

As set forth in the answer to Question 29, an additional registry service which Medistry will offer, commonly used in the marketplace today, is the use of RFPs (Request for Proposals) in the first three years of operation to determine string allocation in appropriate circumstances. Medistry and CC intend to explore allocating some non-reserved geographical identifiers as set forth herein.

Alleged Abuses of Geographic Names

Medistry does not anticipate any disputes with governments or public authorities arising in connection with the registration and use of geographic names within the .MED gTLD based upon its proposed use set forth in Answer 18 of this application and the statements made herein. Nevertheless, Medistry and CC are committed to working with governments, public authorities, or IGOs to quickly resolve any such potential disputes, and as such ensure that such governments, public authorities and IGO’s will at minimum have access to .MED’s abuse prevention procedure(s) and rights protection mechanisms set forth in answers to Questions 28 and 29 of this Application in order to ensure an ability to address alleged abuses of names with national or geographic significance at the second level of .MED.

Potential Future Release of Initially Reserved Names

Medistry looks forward to collaborating with other new gTLD Registry Operators in potentially working with the GAC and ICANN to explore processes that could permit the release of initially reserved country names, such as Registry Service Evaluation Processes (RSEP) requests that have been filed by existing gTLD Registry Operators in releasing previously reserved domain names.

Creation and Updating the Policies

Should the need arise in the future for the creation or updating of the policies regarding this class of domain names, Medistry will act in an open and transparent manner to develop such a policy and⁄or recommendation.

Medistry is also committed to the ongoing review and updating of these lists to prevent the misleading use of geographical identifiers. Consistent with this commitment, Medistry intends to participate in any ongoing ICANN policy discussion regarding the protection of geographic names within the DNS.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

1 CUSTOMARY REGISTRY SERVICES

As Medistry LLC’s (“Medistry”) selected provider of backend registry services, Verisign provides a comprehensive system and physical security solution that is designed to ensure a TLD is protected from unauthorized disclosure, alteration, insertion, or destruction of registry data. Verisign’s system addresses all areas of security including information and policies, security procedures, the systems development lifecycle, physical security, system hacks, break-ins, data tampering, and other disruptions to operations. Verisign’s operational environments not only meet the security criteria specified in its customer contractual agreements, thereby preventing unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with applicable standards, but also are subject to multiple independent assessments as detailed in the response to Question 30, Security Policy. Verisign’s physical and system security methodology follows a mature, ongoing lifecycle that was developed and implemented many years before the development of the industry standards with which Verisign currently complies. Please see the response to Question 30, Security Policy, for details of the security features of Verisign’s registry services.

Verisign’s registry services fully comply with relevant standards and best current practice RFCs published by the Internet Engineering Task Force (IETF), including all successor standards, modifications, or additions relating to the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472. Moreover, Verisign’s Shared Registration System (SRS) supports the following IETF Extensible Provisioning Protocol (EPP) specifications, where the Extensible Markup Language (XML) templates and XML schemas are defined in RFC 3915, 5730, 5731, 5732, 5733, and 5734. By strictly adhering to these RFCs, Verisign helps to ensure its registry services do not create a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems. Besides its leadership in authoring RFCs for EPP, Domain Name System Security Extensions (DNSSEC), and other DNS services, Verisign has created and contributed to several now well-established IETF standards and is a regular and long-standing participant in key Internet standards forums.

Figure 23-1 summarizes the technical and business components of those registry services, customarily offered by a registry operator (i.e., Verisign), that support this application. These services are currently operational and support both large and small Verisign-managed registries. Customary registry services are provided in the same manner as Verisign provides these services for its existing gTLDs.

Through these established registry services, Verisign has proven its ability to operate a reliable and low-risk registry that supports millions of transactions per day. Verisign is unaware of any potential security or stability concern related to any of these services.

Registry services defined in the Figures below are not intended to be offered in a manner unique to the new generic top-level domain (gTLD) nor are such services unique to this application’s registry. An additional registry service which Medistry will offer, commonly used in the marketplace today, is the use of RFPs (Request for Proposals) in the first three years of operation to determine string allocation in appropriate circumstances. Yet another service which Medistry may offer is the use of Auctions and First Come, First Serve (potentially at a higher annual fee) to determine string allocation in appropriate circumstances, such as in allocation of any premium names.

Figure 23-1: See Medistry LLC_Q23_registry services

As further evidence of Verisign’s compliance with ICANN mandated security and stability requirements, Verisign allocates the applicable RFCs to each of the five customary registry services (items A – E above). For each registry service, Verisign also provides evidence in Figure 23-2 of Verisign’s RFC compliance and includes relevant ICANN prior-service approval actions.

Figure 23-2: See attached

Critical Operations of the Registry

i. Receipt of Data from Registrars Concerning Registration of Domain Names and Name Servers

See Item A in Figure 23-1 and Figure 23-2.

ii. Provision to Registrars Status Information Relating to the Zone Servers

Verisign is Medistry’s selected provider of backend registry services. Verisign registry services provisions to registrars status information relating to zone servers for the TLD. The services also allow a domain name to be updated with clientHold, serverHold status, which removes the domain name server details from zone files. This ensures that DNS queries of the domain name are not resolved temporarily. When these hold statuses are removed, the name server details are written back to zone files and DNS queries are again resolved. Figure 23-3 describes the domain name status information and zone insertion indicator provided to registrars. The zone insertion indicator determines whether the name server details of the domain name exist in the zone file for a given domain name status. Verisign also has the capability to withdraw domain names from the zone file in near-real time by changing the domain name statuses upon request by customers, courts, or legal authorities as required.

Figure 23-3: See attached

iii. Dissemination of TLD Zone Files

See Item B in Figure 23-1 and Figure 23-2.

iv. Operation of the Registry Zone Servers

Verisign is Medistry’s selected provider of backend registry services. Verisign, as a company, operates zone servers and serves DNS resolution from 76 geographically distributed resolution sites located in North America, South America, Africa, Europe, Asia, and Australia. Currently, 17 DNS locations are designated primary sites, offering greater capacity than smaller sites comprising the remainder of the Verisign constellation. Verisign also uses Anycast techniques and regional Internet resolution sites to expand coverage, accommodate emergency or surge capacity, and support system availability during maintenance procedures. Verisign operates Medistry’s gTLD from a minimum of eight of its primary sites (two on the East Coast of the United States, two on the West Coast of the United States, two in Europe, and two in Asia) and expands resolution sites based on traffic volume and patterns. Further details of the geographic diversity of Verisign’s zone servers are provided in the response to Question 34, Geographic Diversity. Moreover, additional details of Verisign’s zone servers are provided in the response to Question 32, Architecture and the response to Question 35, DNS Service.

v. Dissemination of Contact and Other Information Concerning Domain Name Server Registrations

See Item C in Figure 23-1 and Figure 23-2.

2 OTHER PRODUCTS OR SERVICES THE REGISTRY OPERATOR IS REQUIRED TO PROVIDE BECAUSE OF THE ESTABLISHMENT OF A CONSENSUS POLICY

Verisign, Medistry’s selected provider of backend registry services, is a proven supporter of ICANN’s consensus-driven, bottom-up policy development process whereby community members identify a problem, initiate policy discussions, and generate a solution that produces effective and sustained results. Verisign currently provides all of the products or services (collectively referred to as services) that the registry operator is required to provide because of the establishment of a Consensus Policy. For the .MED gTLD, Verisign implements these services using the same proven processes and procedures currently in-place for all registries under Verisign’s management. Furthermore, Verisign executes these services on computing platforms comparable to those of other registries under Verisign’s management. Verisign’s extensive experience with consensus policy required services and its proven processes to implement these services greatly minimize any potential risk to Internet security or stability. Details of these services are provided in the following subsections. It shall be noted that consensus policy services required of registrars (e.g., Whois Reminder, Expired Domain) are not included in this response. This exclusion is in accordance with the direction provided in the question’s Notes column to address registry operator services.

2.1 Inter-Registrar Transfer Policy (IRTP)

Technical Component: In compliance with the IRTP consensus policy, Verisign, Medistry’s selected provider of backend registry services, has designed its registration systems to systematically restrict the transfer of domain names within 60 days of the initial create date. In addition, Verisign has implemented EPP and “AuthInfo” code functionality, which is used to further authenticate transfer requests. The registration system has been designed to enable compliance with the five-day Transfer grace period and includes the following functionality:

* Allows the losing registrar to proactively ‘ACK’ or acknowledge a transfer prior to the expiration of the five-day Transfer grace period

* Allows the losing registrar to proactively ‘NACK’ or not acknowledge a transfer prior to the expiration of the five-day Transfer grace period

* Allows the system to automatically ACK the transfer request once the five-day Transfer grace period has passed if the losing registrar has not proactively ACK’d or NACK’d the transfer request.

Business Component: All requests to transfer a domain name to a new registrar are handled according to the procedures detailed in the IRTP. Dispute proceedings arising from a registrar's alleged failure to abide by this policy may be initiated by any ICANN-accredited registrar under the Transfer Dispute Resolution Policy. Medistry’s compliance office serves as the first-level dispute resolution provider pursuant to the associated Transfer Dispute Resolution Policy. As needed Verisign is available to offer policy guidance as issues arise.

Security and Stability Concerns: Verisign is unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. By implementing the IRTP in accordance with ICANN policy, security is enhanced as all transfer commands are authenticated using the AuthInfo code prior to processing.

ICANN Prior Approval: Verisign has been in compliance with the IRTP since November 2004 and is available to support Medistry in a consulting capacity as needed.

Unique to the TLD: This service is not provided in a manner unique to the .MED TLD.

2.2 Add Grace Period (AGP) Limits Policy

Technical Component: Verisign’s registry system monitors registrars’ Add grace period deletion activity and provides reporting that permits Medistry to assess registration fees upon registrars that have exceeded the AGP thresholds stipulated in the AGP Limits Policy. Further, Medistry accepts and evaluates all exemption requests received from registrars and determines whether the exemption request meets the exemption criteria. Medistry maintains all AGP Limits Policy exemption request activity so that this material may be included within Medistry’s Monthly Registry Operator Report to ICANN.

Registrars that exceed the limits established by the policy may submit exemption requests to Medistry for consideration. Medistry’s compliance office reviews these exemption requests in accordance with the AGP Limits Policy and renders a decision. Upon request, Medistry submits associated reporting on exemption request activity to support reporting in accordance with established ICANN requirements.

Business Component: The Add grace period (AGP) is restricted for any gTLD operator that has implemented an AGP. Specifically, for each operator:

* During any given month, an operator may not offer any refund to an ICANN-accredited registrar for any domain names deleted during the AGP that exceed (i) 10% of that registrar's net new registrations (calculated as the total number of net adds of one-year through ten-year registrations as defined in the monthly reporting requirement of Operator Agreements) in that month, or (ii) fifty (50) domain names, whichever is greater, unless an exemption has been granted by an operator.

* Upon the documented demonstration of extraordinary circumstances, a registrar may seek from an operator an exemption from such restrictions in a specific month. The registrar must confirm in writing to the operator how, at the time the names were deleted, these extraordinary circumstances were not known, reasonably could not have been known, and were outside the registrar's control. Acceptance of any exemption will be at the sole and reasonable discretion of the operator; however "extraordinary circumstances" that reoccur regularly for the same registrar will not be deemed extraordinary.

In addition to all other reporting requirements to ICANN, Medistry identifies each registrar that has sought an exemption, along with a brief description of the type of extraordinary circumstance and the action, approval, or denial that the operator took.

Security and Stability Concerns: Verisign is unaware of any impact, caused by the policy, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems.

ICANN Prior Approval: Verisign, Medistry’s backend registry services provider, has had experience with this policy since its implementation in April 2009 and is available to support Medistry in a consulting capacity as needed.

Unique to the TLD: This service is not provided in a manner unique to the .MED TLD.

2.3 Registry Services Evaluation Policy (RSEP)

Technical Component: Verisign, Medistry’s selected provider of backend registry services, adheres to all RSEP submission requirements. Verisign has followed the process many times and is fully aware of the submission procedures, the type of documentation required, and the evaluation process that ICANN adheres to.

Business Component: In accordance with ICANN procedures detailed on the ICANN RSEP website (http://www.icann.org/en/registries/rsep/), all gTLD registry operators are required to follow this policy when submitting a request for new registry services.

Security and Stability Concerns: As part of the RSEP submission process, Verisign, Medistry’s backend registry services provider, identifies any potential security and stability concerns in accordance with RSEP stability and security requirements. Verisign never launches services without satisfactory completion of the RSEP process and resulting approval.

ICANN Prior Approval: Not applicable.

Unique to the TLD: gTLD RSEP procedures are not implemented in a manner unique to the .MED TLD.

3 PRODUCTS OR SERVICES ONLY A REGISTRY OPERATOR IS CAPABLE OF PROVIDING BY REASON OF ITS DESIGNATION AS THE REGISTRY OPERATOR

Verisign, Medistry’s selected backend registry services provider, has developed a Registry-Registrar Two-Factor Authentication Service that complements traditional registration and resolution registry services. In accordance with direction provided in Question 23, Verisign details below the technical and business components of the service, identifies any potential threat to registry security or stability, and lists previous interactions with ICANN to approve the operation of the service. The Two-Factor Authentication Service is currently operational, supporting multiple registries under ICANN’s purview.

Medistry is unaware of any competition issue that may require the registry service(s) listed in this response to be referred to the appropriate governmental competition authority or authorities with applicable jurisdiction. ICANN previously approved the service(s), at which time it was determined that either the service(s) raised no competitive concerns or any applicable concerns related to competition were satisfactorily addressed.

3.1 Two-Factor Authentication Service

Technical Component: The Registry-Registrar Two-Factor Authentication Service is designed to improve domain name security and assist registrars in protecting the accounts they manage. As part of the service, dynamic one-time passwords augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by “what users know” (i.e., their user name and password) and “what users have” (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the one-time-password when communicating directly with Verisign’s Customer Service department as well as when using the registrar portal to make manual updates, transfers, and⁄or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement.

Business Component: There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

Security and Stability Concerns: Verisign is unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. The service is intended to enhance domain name security, resulting in increased confidence and trust by registrants.

ICANN Prior Approval: ICANN approved the same Two-Factor Authentication Service for Verisign's use on .com and .net on 10 July 2009 (RSEP Proposal 2009004) and for .name on 16 February 2011 (RSEP Proposal 2011001).

Unique to the TLD: This service is not provided in a manner unique to the .MED TLD.

3.2 Other allocation methods

As set forth above, an additional registry service which Medistry will offer, commonly used in the marketplace today, is the use of RFPs (Request for Proposals) in the first three years of operation to determine string allocation in appropriate circumstances. Yet another service which Medistry may offer is the use of Auctions and First Come, First Serve (potentially at a higher annual fee) to determine string allocation in appropriate circumstances, such as in allocation of any premium names.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

1 ROBUST PLAN FOR OPERATING A RELIABLE SRS

1.1 High-Level Shared Registration System (SRS) System Description

Verisign, Medistry LLC's ("Medistry") selected provider of backend registry services, provides and operates a robust and reliable SRS that enables multiple registrars to provide domain name registration services in the top-level domain (TLD). Verisign's proven reliable SRS serves approximately 915 registrars, and Verisign, as a company, has averaged more than 140 million registration transactions per day. The SRS provides a scalable, fault-tolerant platform for the delivery of gTLDs through the use of a central customer database, a web interface, a standard provisioning protocol (i.e., Extensible Provisioning Protocol, EPP), and a transport protocol (i.e., Secure Sockets Layer, SSL).

The SRS components include:

* Web Interface: Allows customers to access the authoritative database for accounts, contacts, users, authorization groups, product catalog, product subscriptions, and customer notification messages.

* EPP Interface: Provides an interface to the SRS that enables registrars to use EPP to register and manage domains, hosts, and contacts.

* Authentication Provider: A Verisign developed application, specific to the SRS, that authenticates a user based on a login name, password, and the SSL certificate common name and client IP address.

The SRS is designed to be scalable and fault tolerant by incorporating clustering in multiple tiers of the platform. New nodes can be added to a cluster within a single tier to scale a specific tier, and if one node fails within a single tier, the services will still be available. The SRS allows registrars to manage the .MED gTLD domain names in a single architecture.

To flexibly accommodate the scale of its transaction volumes, as well as new technologies, Verisign employs the following design practices:

* Scale for Growth: Scale to handle current volumes and projected growth.

* Scale for Peaks: Scale to twice base capacity to withstand "registration add attacks" from a compromised registrar system.

* Limit Database CPU Utilization: Limit utilization to no more than 50 percent during peak loads.

* Limit Database Memory Utilization: Each user’s login process that connects to the database allocates a small segment of memory to perform connection overhead, sorting, and data caching. Verisign’s standards mandate that no more than 40 percent of the total available physical memory on the database server will be allocated for these functions.

Verisign’s SRS is built upon a three-tier architecture as illustrated in Figure 24-1 and detailed here:

* Gateway Layer: The first tier, the gateway servers, uses EPP to communicate with registrars. These gateway servers then interact with application servers, which comprise the second tier.

* Application Layer: The application servers contain business logic for managing and maintaining the registry business. The business logic is particular to each TLD’s business rules and requirements. The flexible internal design of the application servers allows Verisign to easily leverage existing business rules to apply to the .MED gTLD. The application servers store Medistry’s data in the registry database, which comprises the third and final tier. This simple, industry-standard design has been highly effective with other customers for whom Verisign provides backend registry services.

* Database Layer: The database is the heart of this architecture. It stores all the essential information provisioned from registrars through the gateway servers. Separate servers query the database, extract updated zone and Whois information, validate that information, and distribute it around the clock to Verisign’s worldwide domain name resolution sites.

Figure 24-1: See Medistry LLC_Q24_shared registration system performance

Scalability and Performance. Verisign, Medistry’s selected backend registry services provider, implements its scalable SRS on a supportable infrastructure that achieves the availability requirements in Specification 10. Verisign employs the design patterns of simplicity and parallelism in both its software and systems, based on its experience that these factors contribute most significantly to scalability and reliable performance. Going counter to feature-rich development patterns, Verisign intentionally minimizes the number of lines of code between the end user and the data delivered. The result is a network of restorable components that provide rapid, accurate updates. Figure 24-2 depicts EPP traffic flows and local redundancy in Verisign’s SRS provisioning architecture. As detailed in the figure, local redundancy is maintained for each layer as well as each piece of equipment. This built-in redundancy enhances operational performance while enabling the future system scaling necessary to meet additional demand created by this or future registry applications.

Figure 24-2: See attached

Besides improving scalability and reliability, local SRS redundancy enables Verisign to take down individual system components for maintenance and upgrades, with little to no performance impact. With Verisign’s redundant design, Verisign can perform routine maintenance while the remainder of the system remains online and unaffected. For the .MED gTLD registry, this flexibility minimizes unplanned downtime and provides a more consistent end-user experience.

1.2 Representative Network Diagrams

Figure 24-3 provides a summary network diagram of Medistry’s selected backend registry services provider’s (Verisign’s) SRS. This configuration at both the primary and alternate-primary Verisign data centers provides a highly reliable backup capability. Data is continuously replicated between both sites to ensure failover to the alternate-primary site can be implemented expeditiously to support both planned and unplanned outages.

Figure 24-3: See attached

1.3 Number of Servers

As Medistry’s selected provider of backend registry services, Verisign continually reviews its server deployments for all aspects of its registry service. Verisign evaluates usage based on peak performance objectives as well as current transaction volumes, which drive the quantity of servers in its implementations. Verisign’s scaling is based on the following factors:

* Server configuration is based on CPU, memory, disk IO, total disk, and network throughput projections.

* Server quantity is determined through statistical modeling to fulfill overall performance objectives as defined by both the service availability and the server configuration.

* To ensure continuity of operations for the .MED gTLD, Verisign uses a minimum of 100 dedicated servers per SRS site. These servers are virtualized to meet demand.

1.4 Description of Interconnectivity with Other Registry Systems

Figure 24-4 provides a technical overview of the Medistry’s selected backend registry services provider’s (Verisign’s) SRS, showing how the SRS component fits into this larger system and interconnects with other system components.

Figure 24-4: See attached

1.5 Frequency of Synchronization Between Servers

As Medistry’s selected provider of backend registry services, Verisign uses synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. This synchronization is performed in near-real time, thereby supporting rapid failover should a failure occur or a planned maintenance outage be required.

1.6 Synchronization Scheme

Verisign uses synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. Because the alternate-primary site is continuously up, and built using an identical design to the primary data center, it is classified as a “hot standby.”

2 SCALABILITY AND PERFORMANCE ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign’s infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign’s scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .MED gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign’s pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, the Medistry’s selected provider of backend registry services, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD’s initial implementation and ongoing maintenance. Verisign’s pricing for the backend registry services provided to Medistry fully accounts for this personnel-related cost, which is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign’s quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign’s ability to align personnel resource growth to the scale increases of Verisign’s TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support SRS performance:

* Application Engineers: 19
* Database Administrators: 8
* Database Engineers: 3
* Network Administrators: 11
* Network Architects: 4
* Project Managers: 25
* Quality Assurance Engineers: 11
* SRS System Administrators: 13
* Storage Administrators: 4
* Systems Architects: 9

To implement and manage the .MED gTLD as described in this application, Verisign, Medistry’s selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign’s internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 EVIDENCE OF COMPLIANCE WITH SPECIFICATION 6 AND 10 TO THE REGISTRY AGREEMENT

Section 1.2 (EPP) of Specification 6, Registry Interoperability and Continuity Specifications. Verisign, Medistry's selected backend registry services provider, provides these services using its SRS, which complies fully with Specification 6, Section 1.2 of the Registry Agreement. In using its SRS to provide backend registry services, Verisign implements and complies with relevant existing RFCs (i.e., 5730, 5731, 5732, 5733, 5734, and 5910) and intends to comply with RFCs that may be published in the future by the Internet Engineering Task Force (IETF), including successor standards, modifications, or additions thereto relating to the provisioning and management of domain names that use EPP. In addition, Verisign's SRS includes a Registry Grace Period (RGP) and thus complies with RFC 3915 and its successors. Details of the Verisign SRS' compliance with RFC SRS⁄EPP are provided in the response to Question 25, Extensible Provisioning Protocol. Verisign does not use functionality outside the base EPP RFCs, although proprietary EPP extensions are documented in Internet-Draft format following the guidelines described in RFC 3735 within the response to Question 25. Moreover, prior to deployment, Medistry will provide to ICANN updated documentation of all the EPP objects and extensions supported in accordance with Specification 6, Section 1.2.

Specification 10, EPP Registry Performance Specifications. Verisign's SRS meets all EPP Registry Performance Specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports, which Verisign files with ICANN. These reports detail Verisign's operational status of the .com and .net registries, which use an SRS design and approach comparable to the one proposed for the .MED gTLD. These reports provide evidence of Verisign's ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http:⁄⁄www.icann.org⁄en⁄tlds⁄monthly-reports⁄.

In accordance with EPP Registry Performance Specifications detailed in Specification 10, Verisign's SRS meets the following performance attributes:

* EPP service availability: < or = 864 minutes of downtime (approx. 98%)

* EPP session-command round trip time (RTT): < or = 4000 milliseconds (ms), for at least 90 percent of the commands

* EPP query-command RTT: < or = 2000 ms, for at least 90 percent of the commands

* EPP transform-command RTT: < or = 4000 ms, for at least 90 percent of the commands

25. Extensible Provisioning Protocol (EPP)

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Verisign, Medistry LLC's ("Medistry") selected backend registry services provider, has used Extensible Provisioning Protocol (EPP) since its inception and possesses complete knowledge and understanding of EPP registry systems. Its first EPP implementation— for a thick registry for the .name generic top-level domain (gTLD)—was in 2002. Since then Verisign has continued its RFC-compliant use of EPP in multiple TLDs, as detailed in Figure 25-1.

Figure 25-1: See Medistry LLC_Q25_extensible provisioning protocol_F25-1

Verisign's understanding of EPP and its ability to implement code that complies with the applicable RFCs is unparalleled. Mr. Scott Hollenbeck, Verisign's director of software development, authored the Extensible Provisioning Protocol and continues to be fully engaged in its refinement and enhancement (U.S. Patent Number 7299299 – Shared registration system for registering domain names). Verisign has also developed numerous new object mappings and object extensions following the guidelines in RFC 3735 (Guidelines for Extending the Extensible Provisioning Protocol). Mr. James Gould, a principal engineer at Verisign, led and co-authored the most recent EPP Domain Name System Security Extensions (DNSSEC) RFC effort (RFC 5910).

All registry systems for which Verisign is the registry operator or provides backend registry services use EPP. Upon approval of this application, Verisign will use EPP to provide the backend registry services for this gTLD. The .com, .net, and .name registries for which Verisign is the registry operator use an SRS design and approach comparable to the one proposed for this gTLD. Approximately 915 registrars use the Verisign EPP service, and the registry system performs more than 140 million EPP transactions daily without performance issues or restrictive maintenance windows. The processing time service level agreement (SLA) requirements for the Verisign-operated .net gTLD are the strictest of the current Verisign managed gTLDs. All processing times for

Verisign-operated gTLDs can be found in ICANN's Registry Operator's Monthly Reports at http://www.icann.org/en/tlds/monthly-reports/.

Verisign has also been active on the Internet Engineering Task Force (IETF) Provisioning Registry Protocol (provreg) working group and mailing list since work started on the EPP protocol in 2000. This working group provided a forum for members of the Internet community to comment on Mr. Scott Hollenbeck's initial EPP drafts, which Mr. Hollenbeck refined based on input and discussions with representatives from registries, registrars, and other interested parties. The working group has since concluded, but the mailing list is still active to enable discussion of different aspects of EPP.

1.1 EPP Interface with Registrars

Verisign, Medistry's selected backend registry services provider, fully supports the features defined in the EPP specifications and provides a set of software development kits (SDK) and tools to help registrars build secure and stable interfaces. Verisign's SDKs give registrars the option of either fully writing their own EPP client software to integrate with the Shared Registration System (SRS), or using the Verisign-provided SDKs to aid them in the integration effort. Registrars can download the Verisign EPP SDKs and tools from the registrar website (http://www.Verisign.com/domain-name-services/current-registrars/epp-sdk/index.html).

The EPP SDKs provide a host of features including connection pooling, Secure Sockets Layer (SSL), and a test server (stub server) to run EPP tests against. One tool—the EPP tool—provides a web interface for creating EPP Extensible Markup Language (XML) commands and sending them to a configurable set of target servers. This helps registrars in creating the template XML and testing a variety of test cases against the EPP servers. An Operational Test and Evaluation (OT&E) environment, which runs the same software as the production system so approved registrars can integrate and test their software before moving into a live production environment, is also available.

2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Medistry's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .MED gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Medistry's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the provisioning of EPP services:

* Application Engineers: 19
* Database Engineers: 3
* Quality Assurance Engineers: 11

To implement and manage the .MED gTLD as described in this application, Verisign, Medistry's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed TLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 ABILITY TO COMPLY WITH RELEVANT RFCS

Verisign, Medistry's selected backend registry services provider, incorporates design reviews, code reviews, and peer reviews into its software development lifecycle (SDLC) to ensure compliance with the relevant RFCs. Verisign's dedicated QA team creates extensive test plans and issues internal certifications when it has confirmed the accuracy of the code in relation to the RFC requirements. Verisign's QA organization is independent from the development team within engineering. This separation helps Verisign ensure adopted processes and procedures are followed, further ensuring that all software releases fully consider the security and stability of the TLD.

For the .MED gTLD, the Shared Registration System (SRS) complies with the following IETF EPP specifications, where the XML templates and XML schemas are defined in the following specifications:

* EPP RGP 3915 (http://www.apps.ietf.org/rfc/rfc3915.html): EPP Redemption Grace Period (RGP) Mapping specification for support of RGP statuses and support of Restore Request and Restore Report (authored by Verisign's Scott Hollenbeck)

* EPP 5730 (http://tools.ietf.org/html/rfc5730): Base EPP specification (authored by Verisign's Scott Hollenbeck)

* EPP Domain 5731 (http://tools.ietf.org/html/rfc5731): EPP Domain Name Mapping specification (authored by Verisign's Scott Hollenbeck)

* EPP Host 5732 (http://tools.ietf.org/html/rfc5732): EPP Host Mapping specification (authored by Verisign's Scott Hollenbeck)

* EPP Contact 5733 (http://tools.ietf.org/html/rfc5733): EPP Contact Mapping specification (authored by Verisign's Scott Hollenbeck)

* EPP TCP 5734 (http://tools.ietf.org/html/rfc5734): EPP Transport over Transmission Control Protocol (TCP) specification (authored by Verisign's Scott Hollenbeck)

* EPP DNSSEC 5910 (http://tools.ietf.org/html/rfc5910): EPP Domain Name System Security Extensions (DNSSEC) Mapping specification (authored by Verisign's James Gould and Scott Hollenbeck)

5 PROPRIETARY EPP EXTENSIONS

Verisign, Medistry's selected backend registry services provider, uses its SRS to provide registry services. The SRS supports the following EPP specifications, which Verisign developed following the guidelines in RFC 3735, where the XML templates and XML schemas are defined in the specifications:

* IDN Language Tag (http://www.verisigninc.com/assets/idn-language-tag.pdf): EPP internationalized domain names (IDN) language tag extension used for IDN domain name registrations

* RGP Poll Mapping (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP mapping for an EPP poll message in support of Restore Request and Restore Report

* Whois Info Extension (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP extension for returning additional information needed for transfers

* EPP ConsoliDate Mapping (http://www.verisigninc.com/assets/consolidate-mapping.txt): EPP mapping to support a Domain Sync operation for synchronizing domain name expiration dates

* NameStore Extension (http://www.verisigninc.com/assets/namestore-extension.pdf): EPP extension for routing with an EPP intelligent gateway to a pluggable set of backend products and services

* Low Balance Mapping (http://www.verisigninc.com/assets/low-balance-mapping.pdf): EPP mapping to support low balance poll messages that proactively notify registrars of a low balance (available credit) condition

As part of the 2006 implementation report to bring the EPP RFC documents from Proposed Standard status to Draft Standard status, an implementation test matrix was completed. Two independently developed EPP client implementations based on the RFCs were tested against the Verisign EPP server for the domain, host, and contact transactions. No compliance-related issues were identified during this test, providing evidence that these extensions comply with RFC 3735 guidelines and further demonstrating Verisign's ability to design, test, and deploy an RFC-compliant EPP implementation.

5.1 EPP Templates and Schemas

The EPP XML schemas are formal descriptions of the EPP XML templates. They are used to express the set of rules to which the EPP templates must conform in order to be considered valid by the schema. The EPP schemas define the building blocks of the EPP templates, describing the format of the data and the different EPP commands' request and response formats. The current EPP implementations managed by Verisign, Medistry's selected backend registry services provider, use these EPP templates and schemas, as will the proposed TLD. For each proprietary XML template⁄schema Verisign provides a reference to the applicable template and includes the schema.

XML templates⁄schema for idnLang-1.0: See Medistry LLC_Q25_extensible provisioning protocol_xml

XML templates⁄schema for rgp-poll-1.0: See Medistry LLC_Q25_extensible provisioning protocol_xml

XML templates⁄schema for whoisInf-1.0: See Medistry LLC_Q25_extensible provisioning protocol_xml

XML templates⁄schema for sync-1.0 (consoliDate) : See Medistry LLC_Q25_extensible provisioning protocol_xml

XML templates⁄schema for namestoreExt-1.1: See Medistry LLC_Q25_extensible provisioning protocol_xml

XML templates⁄schema for lowbalance-poll-1.0: See Medistry LLC_Q25_extensible provisioning protocol_xml

6 PROPRIETARY EPP EXTENSION CONSISTENCY WITH REGISTRATION LIFECYCLE

Medistry's selected backend registry services provider's (Verisign's) proprietary EPP extensions, defined in Section 5 above, are consistent with the registration lifecycle documented in the response to Question 27, Registration Lifecycle. Details of the registration lifecycle are presented in that response. As new registry features are required, Verisign develops proprietary EPP extensions to address new operational requirements. Consistent with ICANN procedures Verisign adheres to all applicable Registry Services Evaluation Process (RSEP) procedures.

26. Whois

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Verisign, Medistry LLC's ("Medistry") selected backend registry services provider, has operated the Whois lookup service for the gTLDs and ccTLDs it manages since 1991, and will provide these proven services for the .MED gTLD registry. In addition, it continues to work with the Internet community to improve the utility of Whois data, while thwarting its application for abusive uses.

1.1 High-Level Whois System Description

Like all other components of Medistry's selected backend registry services provider's (Verisign's) registry service, Verisign's Whois system is designed and built for both reliability and performance in full compliance with applicable RFCs. Verisign's current Whois implementation has answered more than five billion Whois queries per month for the TLDs it manages, and has experienced more than 250,000 queries per minute in peak conditions. The proposed gTLD uses a Whois system design and approach that is comparable to the current implementation. Independent quality control testing ensures Verisign's Whois service is RFC-compliant through all phases of its lifecycle.

Verisign's redundant Whois databases further contribute to overall system availability and reliability. The hardware and software for its Whois service is architected to scale both horizontally (by adding more servers) and vertically (by adding more CPUs and memory to existing servers) to meet future need.

Verisign can fine-tune access to its Whois database on an individual Internet Protocol (IP) address basis, and it works with registrars to help ensure their services are not limited by any restriction placed on Whois. Verisign provides near real-time updates for Whois services for the TLDs under its management. As information is updated in the registration database, it is propagated to the Whois servers for quick publication. These updates align with the near real-time publication of Domain Name System (DNS) information as it is updated in the registration database. This capability is important for the .MED gTLD registry as it is Verisign's experience that when DNS data is updated in near real time, so should Whois data be updated to reflect the registration specifics of those domain names.

Verisign's Whois response time has been less than 500 milliseconds for 95 percent of all Whois queries in .com, .net, .tv, and .cc. The response time in these TLDs, combined with Verisign's capacity, enables the Whois system to respond to up to 30,000 searches (or queries) per second for a total capacity of 2.6 billion queries per day.

The Whois software written by Verisign complies with RFC 3912. Verisign uses an advanced in-memory database technology to provide exceptional overall system performance and security. In accordance with RFC 3912, Verisign provides a website at whois.nic.<TLD> that provides free public query-based access to the registration data.

Verisign currently operates both thin and thick Whois systems.

Verisign commits to implementing a RESTful Whois service upon finalization of agreements with the IETF (Internet Engineering Task Force).

Provided Functionalities for User Interface

To use the Whois service via port 43, the user enters the applicable parameter on the command line as illustrated here:

* For domain name: whois EXAMPLE.TLD
* For registrar: whois "registrar Example Registrar, Inc."
* For name server: whois "NS1.EXAMPLE.TLD" or whois "name server (IP address)"

To use the Whois service via the web-based directory service search interface:

* Go to http://whois.nic.<TLD>
* Click on the appropriate button (Domain, Registrar, or Name Server)
* Enter the applicable parameter:
o Domain name, including the TLD (e.g., EXAMPLE.TLD)
o Full name of the registrar, including punctuation (e.g., Example Registrar, Inc.)
o Full host name or the IP address (e.g., NS1.EXAMPLE.TLD or 198.41.3.39)
* Click on the Submit button.

Provisions to Ensure That Access Is Limited to Legitimate Authorized Users and Is in Compliance with Applicable Privacy Laws or Policies

To further promote reliable and secure Whois operations, Verisign, Medistry's selected backend registry services provider, has implemented rate-limiting characteristics within the Whois service software. For example, to prevent data mining or other abusive behavior, the service can throttle a specific requestor if the query rate exceeds a configurable threshold. In addition, QoS technology enables rate limiting of queries before they reach the servers, which helps protect against denial of service (DoS) and distributed denial of service (DDoS) attacks.

Verisign's software also permits restrictions on search capabilities. For example, wild card searches can be disabled. If needed, it is possible to temporarily restrict and/or block requests coming from specific IP addresses for a configurable amount of time. Additional features that are configurable in the Whois software include help files, headers and footers for Whois query responses, statistics, and methods to memory map the database. Furthermore, Verisign is European Union (EU) Safe Harbor certified and has worked with European data protection authorities to address applicable privacy laws by developing a tiered Whois access structure that requires users who require access to more extensive data to (i) identify themselves, (ii) confirm that their use is for a specified purpose and (iii) enter into an agreement governing their use of the more extensive Whois data.

1.2 Relevant Network Diagrams

Figure 26-1 provides a summary network diagram of the Whois service provided by Verisign, Medistry's selected backend registry services provider. The figure details the configuration with one resolution/Whois site. For the .MED gTLD Verisign provides Whois service from 6 of its 17 primary sites based on the proposed gTLD's traffic volume and patterns. A functionally equivalent resolution architecture configuration exists at each Whois site.

Figure 26-1: See Medistry LLC_Q26_whois
1.3 IT and Infrastructure Resources

Figure 26-2 summarizes the IT and infrastructure resources that Verisign, Medistry's selected backend registry services provider, uses to provision Whois services from Verisign primary resolution sites. As needed, virtual machines are created based on actual and projected demand.

Figure 26-2: See attached

1.4 Description of Interconnectivity with Other Registry Systems

Figure 26-3 provides a technical overview of the registry system provided by Verisign, Medistry's selected backend registry services provider, and shows how the Whois service component fits into this larger system and interconnects with other system components.

Figure 26-3: See attached

1.5 Frequency of Synchronization Between Servers

Synchronization between the SRS and the geographically distributed Whois resolution sites occurs approximately every three minutes. Verisign, Medistry's selected backend registry services provider, uses a two-part Whois update process to ensure Whois data is accurate and available. Every 12 hours an initial file is distributed to each resolution site. This file is a complete copy of all Whois data fields associated with each domain name under management. As interactions with the SRS cause the Whois data to be changed, these incremental changes are distributed to the resolution sites as an incremental file update. This incremental update occurs approximately every three minutes. When the new 12-hour full update is distributed, this file includes all past incremental updates. Verisign's approach to frequency of synchronization between servers meets the Performance Specifications defined in Specification 10 of the Registry Agreement for new gTLDs.

2 TECHNICAL PLAN SCOPE⁄SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Medistry's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .MED gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Medistry's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support Whois services:

* Application Engineers: 19
* Database Engineers: 3
* Quality Assurance Engineers: 11

To implement and manage the .MED gTLD as described in this application, Verisign, Medistry's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 COMPLIANCE WITH RELEVANT RFC

Medistry’s selected backend registry services provider’s (Verisign’s) Whois service complies with the data formats defined in Specification 4 of the Registry Agreement. Verisign will provision Whois services for registered domain names and associated data in the top-level domain (TLD). Verisign’s Whois services are accessible over Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), via both Transmission Control Protocol (TCP) port 43 and a web-based directory service at whois.nic.<TLD>, which in accordance with RFC 3912, provides free public query-based access to domain name, registrar, and name server lookups. Verisign’s proposed Whois system meets all requirements as defined by ICANN for each registry under Verisign management. Evidence of this successful implementation, and thus compliance with the applicable RFCs, can be verified by a review of the .com and .net Registry Operator’s Monthly Reports that Verisign files with ICANN. These reports provide evidence of Verisign’s ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

5 COMPLIANCE WITH SPECIFICATIONS 4 AND 10 OF REGISTRY AGREEMENT

In accordance with Specification 4, Verisign, Medistry’s selected backend registry services provider, provides a Whois service that is available via both port 43 in accordance with RFC 3912, and a web-based directory service at whois.nic.<TLD> also in accordance with RFC 3912, thereby providing free public query-based access. Verisign acknowledges that ICANN reserves the right to specify alternative formats and protocols, and upon such specification, Verisign will implement such alternative specification as soon as reasonably practicable.

The format of the following data fields conforms to the mappings specified in Extensible Provisioning Protocol (EPP) RFCs 5730 – 5734 so the display of this information (or values returned in Whois responses) can be uniformly processed and understood: domain name status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date, and times.

Specifications for data objects, bulk access, and lookups comply with Specification 4 and are detailed in the following subsections, provided in both bulk access and lookup modes.

Bulk Access Mode. This data is provided on a daily schedule to a party designated from time to time in writing by ICANN. The specification of the content and format of this data, and the procedures for providing access, shall be as stated below, until revised in the ICANN Registry Agreement.

The data is provided in three files:

* Domain Name File: For each domain name, the file provides the domain name, server name for each name server, registrar ID, and updated date.

* Name Server File: For each registered name server, the file provides the server name, each IP address, registrar ID, and updated date.

* Registrar File: For each registrar, the following data elements are provided: registrar ID, registrar address, registrar telephone number, registrar email address, Whois server, referral URL, updated date, and the name, telephone number, and email address of all the registrar's administrative, billing, and technical contacts.

Lookup Mode. Figures 26-4 through Figure 26-6 provide the query and response format for domain name, registrar, and name server data objects.

Figure 26-4: See attached

Figure 26-5: See attached

Figure 26-6: See attached

5.1 Specification 10, RDDS Registry Performance Specifications

The Whois service meets all registration data directory services (RDDS) registry performance specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator’s Monthly Reports that Verisign files monthly with ICANN. These reports are accessible from the ICANN website at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

In accordance with RDDS registry performance specifications detailed in Specification 10, Verisign's Whois service meets the following proven performance attributes:

* RDDS availability: < or = 864 min of downtime (approx 98%)
* RDDS query RTT: < or = 2000 ms, for at least 95% of the queries
* RDDS update time: < or = 60 min, for at least 95% of the probes

6 SEARCHABLE WHOIS

Verisign, Medistry’s selected backend registry services provider, provides a searchable Whois service for the .MED gTLD. Verisign has experience in providing tiered access to Whois for the .name registry, and uses these methods and control structures to help reduce potential malicious use of the function. The searchable Whois system currently uses Apache’s Lucene full text search engine to index relevant Whois content with near-real time incremental updates from the provisioning system.

Features of the Verisign searchable Whois function include:

* Provision of a web-based searchable directory service

* Ability to perform partial match, at least, for the following data fields: domain name, contacts and registrant’s name, and contact and registrant’s postal address, including all the sub-fields described in EPP (e.g., street, city, state, or province)

* Ability to perform exact match, at least, on the following fields: registrar ID, name server name, and name server’s IP address (only applies to IP addresses stored by the registry, i.e., glue records)

* Ability to perform Boolean search supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT

* Search results that include domain names that match the selected search criteria

Verisign’s implementation of searchable Whois is EU Safe Harbor certified and includes appropriate access control measures that help ensure that only legitimate authorized users can use the service. Furthermore, Verisign’s compliance office monitors current ICANN policy and applicable privacy laws or policies to help ensure the solution is maintained within compliance of applicable regulations. Features of these access control measures include:

* All unauthenticated searches are returned as thin results.

* Registry system authentication is used to grant access to appropriate users for thick Whois data search results.

* Account access is granted by Medistry’s defined .MED gTLD admin user.

Potential Forms of Abuse and Related Risk Mitigation. Leveraging its experience providing tiered access to Whois for the .name registry and interacting with ICANN, data protection authorities, and applicable industry groups, Verisign, Medistry’s selected backend registry services provider, is knowledgeable of the likely data mining forms of abuse associated with a searchable Whois service. Figure 26-7 summarizes these potential forms of abuse and Verisign’s approach to mitigate the identified risk.

Figure 26-7: See attached

27. Registration Life Cycle

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF REGISTRATION LIFECYCLES AND STATES

Starting with domain name registration and continuing through domain name delete operations, Medistry LLC’s (“Medistry”) selected backend registry services provider’s (Verisign’s) registry implements the full registration lifecycle for domain names supporting the operations in the Extensible Provisioning Protocol (EPP) specification. The registration lifecycle of the domain name starts with registration and traverses various states as specified in the following sections. The registry system provides options to update domain names with different server and client status codes that block operations based on the EPP specification. The system also provides different grace periods for different billable operations, where the price of the billable operation is credited back to the registrar if the billable operation is removed within the grace period. Together Figure 27-1 and Figure 27-2 define the registration states comprising the registration lifecycle and explain the trigger points that cause state-to-state transitions. States are represented as green rectangles within Figure 27-1.

Figure 27-1: See Medistry LLC_Q27_registration lifecycle

Figure 27-2: See attached

1.1 Registration Lifecycle of Create⁄Update⁄Delete

The following section details the create⁄update⁄delete processes and the related renewal process that Verisign, Medistry’s selected backend registry services provider, follows. For each process, this response defines the process function and its characterization, and as appropriate provides a process flow chart.

Create Process. The domain name lifecycle begins with a registration or what is referred to as a Domain Name Create operation in EPP. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

Process Characterization. The Domain Name Create command is received, validated, run through a set of business rules, persisted to the database, and committed in the database if all business rules pass. The domain name is included with the data flow to the DNS and Whois resolution services. If no name servers are supplied, the domain name is not included with the data flow to the DNS. A successfully created domain name has the created date and expiration date set in the database. Creates are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

The Domain Name Create operation is detailed in Figure 27-3 and requires the following attributes:

* A domain name that meets the string restrictions.

* A domain name that does not already exist.

* The registrar is authorized to create a domain name in .MED.

* The registrar has available credit.

* A valid Authorization Information (Auth-Info) value.

* Required contacts (e.g., registrant, administrative contact, technical contact, and billing contact) are specified and exist.

* The specified name servers (hosts) exist, and there is a maximum of 13 name servers.

* A period in units of years with a maximum value of 10 (default period is one year).

Figure 27-3: See attached

Renewal Process. The domain name can be renewed unless it has any form of Pending Delete, Pending Transfer, or Renew Prohibited.

A request for renewal that sets the expiry date to more than ten years in the future is denied. The registrar must pass the current expiration date (without the timestamp) to support the idempotent features of EPP, where sending the same command a second time does not cause unexpected side effects.

Automatic renewal occurs when a domain name expires. On the expiration date, the registry extends the registration period one year and debits the registrar account balance. In the case of an auto-renewal of the domain name, a separate Auto-Renew grace period applies. Renewals are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

Process Characterization. The Domain Name Renew command is received, validated, authorized, and run through a set of business rules. The data is updated and committed in the database if it passes all business rules. The updated domain name's expiration date is included in the flow to the Whois resolution service.

The Domain Name Renew operation is detailed in Figure 27-4 and requires the following attributes:

* A domain name that exists and is sponsored by the requesting registrar.
* The registrar is authorized to renew a domain name in .MED.
* The registrar has available credit.
* The passed current expiration date matches the domain name's expiration date.
* A period in units of years with a maximum value of 10 (default period is one year). A domain name expiry past ten years is not allowed.

Figure 27-4: See attached

Registrar Transfer Procedures. A registrant may transfer his⁄her domain name from his⁄her current registrar to another registrar. The database system allows a transfer as long as the transfer is not within the initial 60 days, per industry standard, of the original registration date.

The registrar transfer process goes through many process states, which are described in detail below, unless it has any form of Pending Delete, Pending Transfer, or Transfer Prohibited.

A transfer can only be initiated when the appropriate Auth-Info is supplied. The Auth-Info for transfer is only available to the current registrar. Any other registrar requesting to initiate a transfer on behalf of a registrant must obtain the Auth-Info from the registrant.

The Auth-Info is made available to the registrant upon request. The registrant is the only party other than the current registrar that has access to the Auth-Info. Registrar transfer entails a specified extension of the expiry date for the object. The registrar transfer is a billable operation and is charged identically to a renewal for the same extension of the period. This period can be from one to ten years, in one-year increments.

Because registrar transfer involves an extension of the registration period, the rules and policies applying to how the resulting expiry date is set after transfer are based on the renewal policies on extension.

Per industry standard, a domain name cannot be transferred to another registrar within the first 60 days after registration. This restriction continues to apply if the domain name is renewed during the first 60 days. Transfer of the domain name changes the sponsoring registrar of the domain name, and also changes the child hosts (ns1.sample.xyz) of the domain name (sample .xyz).

The domain name transfer consists of five separate operations:

* Transfer Request (Figure 27-5): Executed by a non-sponsoring registrar with the valid Auth-Info provided by the registrant. The Transfer Request holds funds of the requesting registrar but does not bill the registrar until the transfer is completed. The sponsoring registrar receives a Transfer Request poll message.

* Transfer Cancel (Figure 27-6): Executed by the requesting registrar to cancel the pending transfer. The held funds of the requesting registrar are reversed. The sponsoring registrar receives a Transfer Cancel poll message.

* Transfer Approve (Figure 27-7): Executed by the sponsoring registrar to approve the Transfer Request. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar receives a Transfer Approve poll message.

* Transfer Reject (Figure 27-8): Executed by the sponsoring registrar to reject the pending transfer. The held funds of the requesting registrar are reversed. The requesting registrar receives a Transfer Reject poll message.

* Transfer Query (Figure 27-9): Executed by either the requesting registrar or the sponsoring registrar of the last transfer.

The registry auto-approves a transfer if the sponsoring registrar takes no action. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar and the sponsoring registrar receive a Transfer Auto-Approve poll message.

Figure 27-5: See attached

Figure 27-6: See attached

Figure 27-7: See attached

Figure 27-8: See attached

Figure 27-9: See attached

Delete Process. A registrar may choose to delete the domain name at any time.

Process Characterization. The domain name can be deleted, unless it has any form of Pending Delete, Pending Transfer, or Delete Prohibited.

A domain name is also prohibited from deletion if it has any in-zone child hosts that are name servers for domain names. For example, the domain name “sample.xyz” cannot be deleted if an in-zone host “ns.sample.xyz” exists and is a name server for “sample2.xyz.”

If the Domain Name Delete occurs within the Add grace period, the domain name is immediately deleted and the sponsoring registrar is credited for the Domain Name Create. If the Domain Name Delete occurs outside the Add grace period, it follows the Redemption grace period (RGP) lifecycle.

Update Process. The sponsoring registrar can update the following attributes of a domain name:

* Auth-Info
* Name servers
* Contacts (i.e., registrant, administrative contact, technical contact, and billing contact)
* Statuses (e.g., Client Delete Prohibited, Client Hold, Client Renew Prohibited, Client Transfer Prohibited, Client Update Prohibited)

Process Characterization. Updates are allowed provided that the update includes the removal of any Update Prohibited status. The Domain Name Update operation is detailed in Figure 27-10.

A domain name can be updated unless it has any form of Pending Delete, Pending Transfer, or Update Prohibited.

Figure 27-10: See attached

1.2 Pending, Locked, Expired, and Transferred

Verisign, Medistry’s selected backend registry services provider, handles pending, locked, expired, and transferred domain names as described here. When the domain name is deleted after the five-day Add grace period, it enters into the Pending Delete state. The registrant can return its domain name to active any time within the five-day Pending Delete grace period. After the five-day Pending Delete grace period expires, the domain name enters the Redemption Pending state and then is deleted by the system. The registrant can restore the domain name at any time during the Redemption Pending state.

When a non-sponsoring registrar initiates the domain name transfer request, the domain name enters Pending Transfer state and a notification is mailed to the sponsoring registrar for approvals. If the sponsoring registrar doesn’t respond within five days, the Pending Transfer expires and the transfer request is automatically approved.

EPP specifies both client (registrar) and server (registry) status codes that can be used to prevent registry changes that are not intended by the registrant. Currently, many registrars use the client status codes to protect against inadvertent modifications that would affect their customers’ high-profile or valuable domain names.

Verisign’s registry service supports the following client (registrar) and server (registry) status codes:

* clientHold
* clientRenewProhibited
* clientTransferProhibited
* clientUpdateProhibited
* clientDeleteProhibited
* serverHold
* serverRenewProhibited
* serverTransferProhibited
* serverUpdateProhibited
* serverDeleteProhibited

1.3 Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers

Verisign, Medistry’s selected backend registry services provider, handles Add grace periods, Redemption grace periods, and notice periods for renewals or transfers as described here.

* Add Grace Period: The Add grace period is a specified number of days following the initial registration of the domain name. The current value of the Add grace period for all registrars is five days.

* Redemption Grace Period: If the domain name is deleted after the five-day grace period expires, it enters the Redemption grace period and then is deleted by the system. The registrant has an option to use the Restore Request command to restore the domain name within the Redemption grace period. In this scenario, the domain name goes to Pending Restore state if there is a Restore Request command within 30 days of the Redemption grace period. From the Pending Restore state, it goes either to the OK state, if there is a Restore Report Submission command within seven days of the Restore Request grace period, or a Redemption Period state if there is no Restore Report Submission command within seven days of the Restore Request grace period.

* Renew Grace Period: The Renew⁄Extend grace period is a specified number of days following the renewal⁄extension of the domain name’s registration period. The current value of the Renew⁄Extend grace period is five days.

* Auto-Renew Grace Period: All auto-renewed domain names have a grace period of 45 days.

* Transfer Grace Period: Domain names have a five-day Transfer grace period.

1.4 Aspects of the Registration Lifecycle Not Covered by Standard EPP RFCs

Medistry’s selected backend registry services provider’s (Verisign’s) registration lifecycle processes and code implementations adhere to the standard EPP RFCs related to the registration lifecycle. By adhering to the RFCs, Verisign’s registration lifecycle is complete and addresses each registration-related task comprising the lifecycle. No aspect of Verisign’s registration lifecycle is not covered by one of the standard EPP RFCs and thus no additional definitions are provided in this response.

2 CONSISTENCY WITH ANY SPECIFIC COMMITMENTS MADE TO REGISTRANTS AS ADAPTED TO THE OVERALL BUSINESS APPROACH FOR THE PROPOSED gTLD

The registration lifecycle described above applies to the .MED gTLD as well as other TLDs managed by Verisign, Medistry’s selected backend registry services provider; thus Verisign remains consistent with commitments made to its registrants. No unique or specific registration lifecycle modifications or adaptations are required to support the overall business approach for the .MED gTLD.

To accommodate a range of registries, Verisign’s registry implementation is capable of offering both a thin and thick Whois implementation, which is also built upon Verisign’s award-winning ATLAS infrastructure.

3 COMPLIANCE WITH RELEVANT RFCs

Medistry’s selected backend registry services provider’s (Verisign’s) registration lifecycle complies with applicable RFCs, specifically RFCs 5730 – 5734 and 3915. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

In addition, in accordance with RFCs 5732 and 5733, the Verisign registration system enforces the following domain name registration constraints:

* Uniqueness⁄Multiplicity: A second-level domain name is unique in the .MED database. Two identical second-level domain names cannot simultaneously exist in .MED. Further, a second-level domain name cannot be created if it conflicts with a reserved domain name.

* Point of Contact Associations: The domain name is associated with the following points of contact. Contacts are created and managed independently according to RFC 5733.

* Registrant
* Administrative contact
* Technical contact
* Billing contact

* Domain Name Associations: Each domain name is associated with:

* A maximum of 13 hosts, which are created and managed independently according to RFC 5732
* An Auth-Info, which is used to authorize certain operations on the object
* Status(es), which are used to describe the domain name’s status in the registry
* A created date, updated date, and expiry date

4 DEMONSTRATES THAT TECHNICAL RESOURCES REQUIRED TO CARRY THROUGH THE PLANS FOR THIS ELEMENT ARE ALREADY ON HAND OR READILY AVAILABLE

Verisign, Medistry’s selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD’s initial implementation and ongoing maintenance. Verisign’s pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign’s quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign’s ability to align personnel resource growth to the scale increases of Verisign’s TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the registration lifecycle:

* Application Engineers: 19
* Customer Support Personnel: 36
* Database Administrators: 8
* Database Engineers: 3
* Quality Assurance Engineers: 11
* SRS System Administrators: 13

To implement and manage the .MED gTLD as described in this application, Verisign, Medistry’s selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign’s internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet’s largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

28. Abuse Prevention and Mitigation

1. COMPREHENSIVE ABUSE POLICIES, WHICH INCLUDE CLEAR DEFINITIONS OF WHAT CONSTITUTES ABUSE IN THE TLD, AND PROCEDURES THAT WILL EFFECTIVELY MINIMIZE POTENTIAL FOR ABUSE IN THE TLD

The .MED gTLD will have a comprehensive abuse policy, which includes a clear definition of what constitutes abuse in .MED, and procedures in place to effectively minimize potential for abuse in .MED. It is a core goal of .MED to provide a trusted namespace that minimizes harm to Internet users (such as identity theft, harm to children and a general erosion of trust), while not negatively impacting Internet stability or security. Medistry LLC (Medistry) takes abuse prevention and mitigation seriously, and the following core elements of the plan (what constitutes abuse, what we will do if we find abuse, how we can be made aware of abuse, and the processes and procedures we will invoke) shows Medistry’s commitment to abuse prevention and mitigation in .MED.

1.1 .MED Abuse Prevention and Mitigation Implementation Plan

Medistry takes abuse prevention and mitigation seriously. The attached .MED Abuse Prevention and Mitigation plan (the “Plan”) will be published on .MED’s registry website and details many of .MED’s policies and procedures regarding abuse prevention and mitigation. The goal of the Plan is to address significant potential harm to Internet users, including identity theft, harm to children and erosion of trust by Internet users, and to address those who abuse the DNS and otherwise engage in illegal or fraudulent activity via the .MED gTLD.

The Plan includes a single abuse point of contact responsible for addressing matters requiring expedited attention and providing a timely response to abuse complaints concerning all .MED names registered through all registrars of record, including those involving a reseller. The Plan identifies an Abuse Prevention Manager who will be tasked with being the primary point of contact for receiving all abuse complaints.

The Plan also includes a clear definition of what constitutes “abuse.” Particularly, “abuse” or “abusive use” of a .MED domain name is the wrongful or excessive use of power, position or ability with regard to a .MED domain, and includes, without limitation, the following:

* Illegal or fraudulent actions;

* Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;

* Phishing: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;

* Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;

* Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent.
Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses;

* Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);

* Distribution of child pornography; and

* Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

“Abuse” or “abusive use” of a .MED domain name also includes violation or breach of any policies or rules regarding registration and/or use of the .MED gTLD as set forth by the Cleveland Clinic (“CC”). This allows CC, as steward of the .MED gTLD, to adopt, address, evolve and enforce current and additional policies in place to prevent or mitigate any abusive use of the .MED gTLD.

The Plan also includes reservation of the right on Medistry’s part to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that Medistry deems necessary: (1) to protect the integrity and stability of .MED; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on Medistry’s and CC’s part, as well as affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by Medistry, CC or any registrar in connection with a domain name registration. Medistry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a complaint.

Medistry acknowledges that it is not capable of making final determinations of matters which are appropriately determined in other fora, such as determination of guilt on a criminal matter, determination of child pornography, or determination of other illegality. As such, with regard to any abuse claim made under color or rule of law, statute or code of any jurisdiction, Medistry will most likely defer final determination on any such claim to an appropriate tribunal in an appropriate jurisdiction. However, as set forth above, Medistry also reserves the right to lock, suspend, place on hold (or similar status) any domain which is the subject of an abuse claim while the substance of the claim is pending adjudication or otherwise final determination by the appropriate tribunal in the appropriate jurisdiction.

The Plan also includes procedures that will effectively minimize potential for abuse in the .MED gTLD, as set forth more completely in Section 1.2 below.

The Plan is aimed at illegal and abusive use of domains, and is not intended as a substitute, replacement, circumvention or alternative venue for complaints, matters and issues more appropriately addressed by trademark rights protection mechanisms set forth in response to Question 29, such as, for example, the UDRP, URS, Sunrise Period and the Trademark Clearinghouse, or the PDDRP as set forth in Question 29.

1.2 Policies for Handling Complaints Regarding Abuse

Abuse complaints may be submitted to the Abuse Prevention Manager by email (likely to be “abuse” (at) RegistryOperatorWebsite.MED or similar) or by written mail to: Attention: Abuse Prevention Manager ⁄ 3029 Prospect Avenue ⁄ Cleveland ⁄ OH ⁄ 44115 ⁄ United States, or other address as identified on .MED’s registry website. This will allow the complaint to be formally recognized and processed.

A complaint should include: the .MED domain name at issue; the nature of the alleged abuse; the date(s) the abuse allegedly occurred; any materials the claimant may have illustrating the abuse (for example, spam email, screen shots, etc.); any authority the complainant may have with regard to the claim (for example, if the complainant is with law enforcement); and the claimant’s contact information, including a preferred method of contact (such as email).

Complaints must be submitted in English. In the event a complainant is not capable of submitting a complaint in English, or is otherwise incapable of communicating in English, Medistry will take commercially reasonable efforts to accommodate the complainant and determine an effective means of communication, but makes no guarantee that any complaint will be processed in any language outside of English.

Commercially reasonable attempts will be made to respond to the complainant via the method of communication identified in the complaint (e.g., by email or written mail; by phone if requested and reasonable). If the complaint contains no contact information, or incomplete contact information that does not allow a response, the complaint will be dismissed.

Once received, a complaint will be assigned a unique identifier, which will be maintained during the life cycle of the complaint and communicated to the complainant upon Medistry’s first response to the complainant.

Every complaint will be initially screened to determine if it is to be substantively processed or otherwise identified as incomplete, frivolous, incomprehensible, stating a claim for which no relief can be granted, non-topical or otherwise not subject to substantive processing. Medistry will endeavor to make this threshold determination within ten business days of receiving a complaint, or three business days if the complainant is a member of law enforcement.

If the complaint is deemed to be incomplete or incomprehensible, Medistry will respond to the complainant asking for a complete and comprehensible complaint, and will cease processing the complaint until a complete and comprehensible complaint is received. If the complaint is deemed frivolous, Medistry will reply that the complaint is frivolous and invite the complainant to justify why the complaint is not frivolous; if the complainant cannot overcome this burden, the complaint will be dismissed. If the complaint is non-topical or makes claim for which no relief can be granted under .MED’s Abuse Prevention and Mitigation Plan, Medistry will respond accordingly and invite the claimant to respond or direct the claimant to a more appropriate forum or mechanism for addressing the claimant’s complaint, such as the UDRP, other rights protection mechanisms as set forth in the answer to Question 29, civil litigation in an appropriate forum, or referral to law enforcement. In either event, Medistry will cease processing such a complaint until a response is received from the complainant. If a review of the complaint determines that the complaint cannot be substantively processed for any other reason, Medistry will respond to the complainant accordingly and processing of the complaint will cease until a response is received from complainant.

In the event Medistry’s initial screening determines that the complaint is complete, non-frivolous, comprehensible, states a claim for which relief can be granted, topical and otherwise capable of substantive processing by Medistry, Medistry will substantively process the complaint. Medistry will establish and follow a variety of methods for tracking claimed abuse and for addressing the nature of the alleged abuse. These methods may include, but not be limited to, coordination with CC, law enforcement, engaging security vendors, internal investigations, engaging our back-end provider (Verisign) and employing Verisign’s resources regarding abuse detection⁄prevention, engaging the registrar of record, and any other industry-standard mechanisms for addressing domain abuse. Complaint processing, analysis and resource allocation will be on a case-by-case basis as needed for each complaint.

In the event Medistry initiates substantive processing of a complaint, Medistry will inform CC, the registrant of record, the registrar of record and the complainant of such initiation, and will submit requests for information, comment or feedback as required on a case-by-case basis for each complaint. The registrant of record will be contacted via the WHOIS information associated with the registration. Medistry will work with CC and the registrar of record to determine the nature of the alleged abuse, and the necessary and appropriate steps to address same. Medistry will contact the registrar of record by phone, email or other method as identified in the agreement between Medistry and the registrar.

At any time during processing of a complaint, CC may contact Medistry and direct Medistry to take any of the actions set forth herein (such as, for example, suspending the domain pending further investigation). CC is committed to working with Medistry in the fair and reasonable implementation of the Plan as set forth herein, and in the fair and reasonable processing of each complaint.

Medistry acknowledges that the registrar of record may initiate its own abuse investigation, at which point Medistry will process the complaint in parallel with the registrar. Again, Medistry will work with the registrar of record with regard to contacting the registrant (if the registrar wishes to be the point of contact with the registrant) and processing the complaint.

During Medistry’s processing of a complaint, Medistry may elect to suspend, lock, or otherwise place the domain at issue on hold pending resolution of the complaint. The registrant of record will be sent notice via contact information in the WHOIS that the domain will be suspended, locked or otherwise placed on hold pending resolution of the complaint. If the registrant of record chooses to respond, Medistry will consider their response and may release the suspension, lock or hold if appropriate. Medistry is committed to a fair and impartial process for addressing abuse complaints, and will endeavor to ensure that mistakes in processing or suspending/locking/holding do not occur, but Medistry recognizes that rarely false-positive suspension may occur. In this event, Medistry notes that the domain at issue will not be deleted (until potentially completion of complaint processing), which will allow for quick correction of the suspension/lock/hold in the rare case of a false-positive. In any event, Medistry will comply with any appropriate court or tribunal order directed to Medistry to release a suspended/locked/on-hold domain if complainant provides such to Medistry.

After processing of a complaint, Medistry may approve or deny the claim, make comments on the claim, conditionally approve the claim, suspend the claim pending further action, and may take any action set forth herein (such as, for example, cancelling or transferring the domain at issue). In matters in which the ultimate determination as to whether the substance of a claim is illegal or otherwise more appropriately determined by a court or tribunal in other fora, Medistry may delay final processing of a claim, pending resolution and/or direction in the matter from such court or tribunal. In matters in which the ultimate determination as to whether an abuse has occurred is more appropriately determined by CC in its position as steward of the .MED gTLD, Medistry may delay final processing of a claim pending CC’s determination of appropriate action.

Medistry will notify the claimant, CC, the registrant of record and the registrar of record of Medistry’s final determination regarding the complaint and any actions Medistry may take/have taken in regard to the matter. The registrant (or entity claimed to have abusively acted) or the claimant may, within ten business days of Medistry sending out such notice, inform Medistry that such entity wishes Medistry to reconsider its decision. Such reconsideration request should be submitted to the Abuse Prevention Manager in the same manner as the complaint was submitted, or otherwise as provided in the notice of Medistry’s decision. Any reconsideration request must address why reconsideration should be considered, and should identify any new information which was not considered by Medistry in Medistry’s final decision, and which would be considered material enough to justify a reversal of Medistry’s determination. If the reconsideration request contains such material new information, Medistry may decide to reopen processing of the complaint, and would then notify CC, the complainant, the registrant, the registrar and any other interested parties of such reopening. If the reconsideration request fails to contain any material new information, or if Medistry that the material new information provided is not sufficient for Medistry to change its position, Medistry will deny the reconsideration request. At that point Medistry will cease processing the claim, but will still respond to appropriate court or tribunal orders directed to Medistry regarding the matter.

In the event a complainant identifies themselves as a member of law enforcement investigating a potential illegal activity, Medistry will endeavor to initially respond to such a complaint within twenty four hours, but in no event less than seventy-two hours, and may respond sooner if the complaint requests a quicker turnaround and provides an adequate reason for needing a quicker turnaround. Medistry is committed to working with law enforcement relating to abusive actions in the .MED gTLD, and will put forth commercially reasonable efforts to communicate with law enforcement, accommodate law enforcement requests and generally work with law enforcement towards expedited processing of a complaint.

Medistry is a Delaware limited liability company with a principal place of business at 3029 Prospect Avenue, Cleveland Ohio 44115, and is subject to Ohio and Delaware law. In the event Medistry receives a court or tribunal order for any reason, Medistry will review the order to determine its reasonableness and the extent to which the issuing court or tribunal has authority over Medistry, CC or any party implicated in a complaint. Medistry may consult with outside legal counsel in such a review. If Medistry elects to respond or take action pursuant to the order, Medistry will endeavor to do so within any time frame set forth in the order, so long as practicable.

For complaints arising from matters relating to abuse or misuse of CC’s policies governing use of the .MED gTLD (“CC Policies”), Medistry will work with CC to determine the processing of such a complaint. In complaints relating to CC Policies, CC may choose to invoke any of its own policies or procedures which will be developed and adapted to address abuses or violations of CC Policies. Medistry will work with CC, at CC’s direction, to assist in processing any claim. Medistry will also comply with any direction to action given by CC related to suspension, lock, hold, transfer or cancellation of any domain in a complaint primarily regarding CC Policies. As previously stated, CC is committed to the fair and impartial implementation of the Plan.

Medistry is committed to preventing and mitigating abuse in the .MED gTLD, and will comply with all terms regarding such in the final version of the Registry Agreement and all consensus policies relating to such. Working with CC and registrars, Medistry will remain flexible on the Plan and its implementation policies/procedures to address future and unconventional abuses which are not currently known, and looks forward to working with other gTLD registry operators and ICANN in determining industry standard abuse prevention and mitigation plans, policies and procedures.

1.3 Proposed Measures for Removal of Orphan Glue Records

Although orphan glue records often support correct and ordinary operation of the Domain Name System (DNS), registry operators will be required to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct. Medistry's selected backend registry services provider's (Verisign's) registration system is specifically designed to not allow orphan glue records. Registrars are required to delete/move all dependent DNS records before they are allowed to delete the parent domain.

To prevent orphan glue records, Verisign performs the following checks before removing a domain or name server:

Checks during domain delete:

* Parent domain delete is not allowed if any other domain in the zone refers to the child name server.

* If the parent domain is the only domain using the child name server, then both the domain and the glue record are removed from the zone.

Check during explicit name server delete:

* Verisign confirms that the current name server is not referenced by any domain name (in-zone) before deleting the name server.

Zone-file impact:

* If the parent domain references the child name server AND if other domains in the zone also reference it AND if the parent domain name is assigned a serverHold status, then the parent domain goes out of the zone but the name server glue record does not.

* If no domains reference a name server, then the zone file removes the glue record.

1.4 Resourcing Plans

Details related to resourcing plans for the initial implementation and ongoing maintenance of Medistry's abuse plan are provided in Section 2 of this response.

1.5 Measures to Promote Whois Accuracy

1.5.1 Authentication of Registrant Information

As set forth in the answer to Question 18, domain name registrations in .MED will be limited to CC, its partners and other trusted parties from the medical and healthcare fields as CC so determines. As further set forth in the answer to Question 18, during the initial three years of operation of the .MED gTLD, all domains will be allocated by Request for Proposal (RFP). This will afford CC and Medistry the ability to authenticate all registrant information by reviewing and evaluating RFP proposal information. All RFP applicants will be required to identify themselves, and selected applicants will be required to provide their RFP identification information as the subject domain's Whois information. Further, by the nature of the registration limitations set forth above, registrants (and their Whois information) will relate to entities that CC knows or otherwise trusts.

Beyond the initial three years of operation, CC and Medistry will review Whois accuracy during the initial three years of operation and determine appropriate authentication processes based upon (i) their review of the initial three year's worth of Whois information and its accuracy; (ii) the needs of users as determined by CC and Medistry; (iii) the stated mission/purpose of the .MED gTLD; and (iv) any Consensus Policies or other ICANN mandates regarding Whois accuracy.

CC and Medistry will work with accredited registrars to ensure that the RFP process provides for the opportunity to evaluate applicant information with a view towards including such information in the subject domain's Whois information.

1.5.2 Regular Monitoring of Registration Data for Accuracy and Completeness

As all .MED domains during the initial three years of operation will be allocated by RFP, Medistry is confident that Whois data will remain accurate and complete. Part of compliance with the RFP criteria will be agreeing to provide complete and accurate applicant information which will be reflected in the subject domain's Whois information. During the first three years of operation, in the event that CC or Medistry receives information that a .MED domain’s Whois information is inaccurate; Medistry will investigate the matter and take appropriate action. Subsequent to the first three years of operation, CC and Medistry will determine appropriate procedures for addressing claims of Whois inaccuracy or incompleteness.

Medistry recognizes that monitoring of registration data for accuracy and completeness is an important matter to ICANN and many ICANN stakeholders. Medistry will comply with all monitoring provisions in the final version of the Registry Agreement and all consensus policies relating to monitoring. Medistry will work with all accredited registrars towards this goal. Medistry will also work with CC to establish procedures for cross-checking WHOIS data with records relating to RFP applicant information.

Verisign, Medistry’s selected backend registry services provider, has established policies and procedures to encourage registrar compliance with ICANN’s Whois accuracy requirements. Verisign provides the following services to Medistry for incorporation into its full-service registry operations.

Registrar self certification.

The self-certification program consists, in part, of evaluations applied equally to all operational ICANN accredited registrars and conducted from time to time throughout the year. Process steps are as follows:

* Verisign sends an email notification to the ICANN primary registrar contact, requesting that the contact go to a designated URL, log in with his/her Web ID and password, and complete and submit the online form. The contact must submit the form within 15 business days of receipt of the notification.

* When the form is submitted, Verisign sends the registrar an automated email confirming that the form was successfully submitted.

* Verisign reviews the submitted form to ensure the certifications are compliant.

* Verisign sends the registrar an email notification if the registrar is found to be compliant in all areas.

* If a review of the response indicates that the registrar is out of compliance or if Verisign has follow-up questions, the registrar has 10 days to respond to the inquiry.

* If the registrar does not respond within 15 business days of receiving the original notification, or if it does not respond to the request for additional information, Verisign sends the registrar a Breach Notice and gives the registrar 30 days to cure the breach.

* If the registrar does not cure the breach, Verisign terminates the Registry-Registrar Agreement (RRA).

Whois data reminder process. Verisign regularly reminds registrars of their obligation to comply with ICANN’s Whois Data Reminder Policy, which was adopted by ICANN as a consensus policy on 27 March 2003 (http://www.icann.org/en/registrars/wdrp.htm). Verisign sends a notice to all registrars once a year reminding them of their obligation to be diligent in validating the Whois information provided during the registration process, to investigate claims of fraudulent Whois information, and to cancel domain name registrations for which Whois information is determined to be invalid.

1.5.3 Use of Registrars

As of the submission date of this application, ICANN has not provided final guidance as to the nature and the details of the procedures which will be implemented by registrars to ensure accuracy and completeness of WHOIS data. Medistry has followed and will continue to follow closely the progress of the negotiations between ICANN and the Registrar Negotiations Team (NT) regarding the revised Registrar Accreditation Agreement (RAA). Medistry acknowledges the interests of law enforcement agencies (LEA), who generally are seeking greater openness, accuracy and accountability in WHOIS data. Medistry also acknowledges the countervailing position of those who wish to maintain WHOIS privacy, and those (such as registrars) who wish to keep WHOIS costs down.

In the 1 March 2012 Progress Report on Negotiations on the Registrar Accreditation Agreement, ICANN notes that ICANN and the NT are currently undertaking a “comprehensive review” of the RAA and addressing twelve enumerated requests from LEA relating to WHOIS accuracy, accountability and completeness. ICANN and the NT appear to have an agreement in principle on eleven of the twelve principals, agreeing in principle on (1) guidelines for Privacy/Proxy Accreditation Services; (2) a gross negligence standard for knowledge in permitting criminal activity regarding WHOIS information; (3) registrar contact information; (4) public display of registrar officer information; (5) registrar ownership; (6) notice of change to registrar; (7) registrar certification; (8) registrar accountability and disclosure obligations; (10) validation of WHOIS data; (11) abuse point of contact; and (12) SLA for port 43 servers – while not having an agreement in principle on (9) registrar collection and maintenance of data on the persons initiating requests for registrations, as well as source IP addresses and financial transaction information. ICANN and the NT are also addressing approximately twenty-two other issues relating to the RAA, of which approximately half have an agreement in principle.

Medistry is committed to support WHOIS accuracy and completeness procedures and policies which support the WHOIS policies and procedures which result from eventual agreement between ICANN and the NT regarding matters of WHOIS accuracy, accountability and openness as set forth in the final version of the RAA.

1.6 Controls to Ensure Proper Access to Domain Functions

To ensure proper access to domain functions, Medistry incorporates Verisign's Registry-Registrar Two-Factor Authentication Service into its full-service registry operations. The service is designed to improve domain name security and assist registrars in protecting the accounts they manage by providing another level of assurance that only authorized personnel can communicate with the registry. As part of the service, dynamic one-time passwords (OTPs) augment the user names and passwords currently used to process update, transfer, and⁄or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the one-time-password when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and⁄or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement. As shown in Figure 28-1, the registrars' authorized contacts use the OTP to enable strong authentication when they contact the registry. There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

Figure 28-1: See Medistry_Q28_Figures

2. TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Resource Planning

Medistry's management team is an experienced team which has managed a gTLD (.JOBS) for over six years and is well-acquainted with domain abuse prevention and mitigation.

During initial operation of .MED, the Abuse Prevention Manager will be the General Counsel of Medistry. In processing a complaint, the Abuse Prevention Manager may seek the assistance of any of the Executive Management Personnel, including the Vice President of Registry Operations for .MED policy-related issues. The Abuse Prevention Manager may also seek the assistance of either or both Customer Support personnel and Technical Labor personnel, depending upon the nature of the complaint and the volume of complaints. The Abuse Prevention Manager may also engage the services of outside legal counsel for advice or representation if the nature of a complaint or processing the complaint requires.

Operations of the Abuse Prevention Manager will scale as needed to accommodate the volume and nature of complaints received, including shifting allocations of time from Customer Support personnel and Technical Labor personnel. In the event registration volume and related income allow, and complaint volume dictates, additional personnel may be added to accommodate the complaints, up to and including addition of a dedicated Abuse Prevention Manager with a staff commensurate to need.

Costs for Medistry's operations as detailed above are addressed in the response to Question 47. Specifically, $5,000 has been attributed to legal as part of general administrative expenses per year (see table 3 provided in response to Question 47). In addition, per the Financial Projections Template submitted in response to Question 46, $10,000 per year is budgeted under Other Operating Costs in case of unexpected contingencies, such as outside legal counsel.

CC is a world-famous and multi-national medical institution. CC has an experienced management team, compliance team and legal team which may be employed for overseeing use of the .MED gTLD. With regard to abuse complaints that relate to CC Policies, CC will deploy appropriate management resources to establish, implement and maintain internal procedures for addressing such claims. Such procedures may involve input from management, compliance and legal, and legal may consult with outside legal counsel. CC has sufficient resources and personnel to provide the compliance services attributed to CC herein.

CC's internal costs for abuse complaint procedures will be borne by CC, and are thus not included in the response to Question 47.

Resource Planning Specific to Backend Registry Activities

Verisign, Medistry's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as “Total Critical Registry Function Cash Outflows” (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign’s quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign’s ability to align personnel resource growth to the scale increases of Verisign’s TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support abuse prevention and mitigation:

* Application Engineers: 19
* Business Continuity Personnel: 3
* Customer Affairs Organization: 9
* Customer Support Personnel: 36
* Information Security Engineers: 11
* Network Administrators: 11
* Network Architects: 4
* Network Operations Center (NOC) Engineers: 33
* Project Managers: 25
* Quality Assurance Engineers: 11
* Systems Architects: 9

To implement and manage the .MED gTLD as described in this application, Verisign, Medistry’s selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign’s internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet’s largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

3. POLICIES AND PROCEDURES IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES AT STARTUP AND ON AN ONGOING BASIS

The anti-abuse policies and procedures set forth in the answers to this Question 28 address, and are applicable, to abusive use of registered names in .MED at both startup and on an ongoing basis.

3.1 Start-Up Anti-Abuse Policies and Procedures

Medistry’s anti-abuse policies and procedures set forth above will be available as of start-up of .MED.

Verisign, Medistry’s selected backend registry services provider, provides the following domain name abuse prevention services, which Medistry incorporates into its full-service registry operations. These services are available at the time of domain name registration.

Registry Lock. The Registry Lock Service allows registrars to offer server-level protection for their registrants’ domain names. A registry lock can be applied during the initial standup of the domain name or at any time that the registry is operational.

Specific Extensible Provisioning Protocol (EPP) status codes are set on the domain name to prevent malicious or inadvertent modifications, deletions, and transfers. Typically, these ‘server’ level status codes can only be updated by the registry. The registrar only has ‘client’ level codes and cannot alter ‘server’ level status codes. The registrant must provide a pass phrase to the registry before any updates are made to the domain name. However, with Registry Lock, provided via Verisign, Medistry’s subcontractor, registrars can also take advantage of server status codes.

The following EPP server status codes are applicable for domain names: (i) serverUpdateProhibited, (ii) serverDeleteProhibited, and (iii) serverTransferProhibited. These statuses may be applied individually or in combination.

The EPP also enables setting host (i.e., name server) status codes to prevent deleting or renaming a host or modifying its IP addresses. Setting host status codes at the registry reduces the risk of inadvertent disruption of DNS resolution for domain names.

The Registry Lock Service is used in conjunction with a registrar’s proprietary security measures to bring a greater level of security to registrants’ domain names and help mitigate potential for unintended deletions, transfers, and/or updates.

Two components comprise the Registry Lock Service:

* Medistry and/or its registrars provides Verisign, Medistry’s selected provider of backend registry services, with a list of the domain names to be placed on the server status codes. During the term of the service agreement, the registrar can add domain names to be placed on the server status codes and/or remove domain names currently placed on the server status codes. Verisign then manually authenticates that the registrar submitting the list of domain names is the registrar-of-record for such domain names.

* If Medistry and/or its registrars requires changes (including updates, deletes, and transfers) to a domain name placed on a server status code, Verisign follows a secure, authenticated process to perform the change. This process includes a request from a Medistry-authorized representative for Verisign to remove the specific registry status code, validation of the authorized individual by Verisign, removal of the specified server status code, registrar completion of the desired change, and a request from the Medistry-authorized individual to reinstate the server status code on the domain name. This process is designed to complement automated transaction processing through the Shared Registration System (SRS) by using independent authentication by trusted registry experts.

Medistry intends to charge registrars based on the market value of the Registry Lock Service. A tiered pricing model is expected, with each tier having an annual fee based on per domain name/host and the number of domain names and hosts to be placed on Registry Lock server status code(s).

3.2   Ongoing Anti-Abuse Policies and Procedures

Medistry’s anti-abuse policies and procedures set forth in the answers to this Question 28 will be available on an on-going basis for .MED.

3.2.1 Policies and Procedures That Identify Malicious or Abusive Behavior

Verisign, Medistry’s selected backend registry services provider, provides the following service to Medistry for incorporation into its full-service registry operations.

Malware scanning service. Registrants are often unknowing victims of malware exploits. Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.

Verisign’s malware scanning service helps prevent websites from infecting other websites by scanning web pages for embedded malicious content that will infect visitors’ websites. Verisign’s malware scanning technology uses a combination of in-depth malware behavioral analysis, anti-virus results, detailed malware patterns, and network analysis to discover known exploits for the particular scanned zone. If malware is detected, the service sends the registrar a report that contains the number of malicious domains found and details about malicious content within its TLD zones. Reports with remediation instructions are provided to help registrars and registrants eliminate the identified malware from the registrant’s website.

3.2.2 Policies and Procedures That Address the Abusive Use of Registered Names

Suspension processes conducted by backend registry services provider. In the case of domain name abuse, Medistry will determine whether to take down the subject domain name as set forth in Section 1 of the answer to this Question 28. Verisign, Medistry’s selected backend registry services provider, will follow the following auditable processes to comply with the suspension request.

Figure 28-2: See Medistry_Q28_Figures

Verisign Suspension Notification. Medistry submits the suspension request to Verisign for processing, documented by:

* Threat domain name
* Registry incident number
* Incident narrative, threat analytics, screen shots to depict abuse, and/or other evidence
* Threat classification
* Threat urgency description
* Recommended timeframe for suspension/takedown
* Technical details (e.g., Whois records, IP addresses, hash values, anti-virus detection results/nomenclature, name servers, domain name statuses that are relevant to the suspension)
* Incident response, including surge capacity

Verisign Notification Verification. When Verisign receives a suspension request from Medistry, it performs the following verification procedures:

* Validate that all the required data appears in the notification.
* Validate that the request for suspension is for a registered domain name.
* Return a case number for tracking purposes.

Suspension Rejection. If required data is missing from the suspension request, or the domain name is not registered, the request will be rejected and returned to Medistry with the following information:

* Threat domain name
* Registry incident number
* Verisign case number
* Error reason

Registrar Notification. Once Verisign has performed the domain name suspension, and upon Medistry request, Verisign notifies the registrar of the suspension. If Medistry does not request that Verisign notify the registrar, Medistry will notify the registrar. Registrar notification includes the following information:

* Threat domain name
* Registry incident number
* Verisign case number
* Classification of type of domain name abuse
* Evidence of abuse
* Anti-abuse contact name and number
* Suspension status
* Date/time of domain name suspension

Registrant Notification. Once Verisign has performed the domain name suspension, and upon Medistry request, Verisign notifies the registrant of the suspension. If Medistry does not request that Verisign notify the registrant, Medistry will notify the registrant. Registrant notification includes the following information:

* Threat domain name
* Registry incident number
* Verisign case number
* Classification of type of domain name abuse
* Evidence of abuse
* Registrar anti-abuse contact name and number

Domain Suspension. Verisign places the domain to be suspended on the following statuses:

* serverUpdateProhibited
* serverDeleteProhibited
* serverTransferProhibited
* serverHold

Suspension Acknowledgement. Verisign notifies Medistry that the suspension has been completed. Acknowledgement of the suspension includes the following information:

* Threat domain name
* Registry incident number
* Verisign case number
* Case number
* Domain name
* Medistry abuse contact name and number, or registrar abuse contact name and number
* Suspension status

4. WHEN EXECUTED IN ACCORDANCE WITH THE REGISTRY AGREEMENT, PLANS WILL RESULT IN COMPLIANCE WITH CONTRACTUAL REQUIREMENTS

It is Medistry’s good faith belief that the plans and procedures set forth herein, when executed, will place .MED in compliance with the contractual requirements set forth in the Registry Agreement. As a final version of the Registry Agreement has not been provided, Medistry is committed to being in compliance with all abuse-prevention terms and obligations set forth in the final version of the Registry Agreement, and will amend and augment any and all anti-abuse plans and procedures set forth herein to be in compliance with the terms and obligations regarding anti-abuse plans and procedures set forth in the final version of the Registry Agreement and any Consensus Policies relating to abuse prevention and mitigation.

5. TECHNICAL PLAN SCOPE/SCALE THAT IS CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Scope/Scale Consistency

Medistry’ anti-abuse plans and procedures set forth herein are consistent with the technical, operational and financial approach and details set forth in other parts of this application, and other answers to the Questions therein. As detailed in answers to Question 47, Medistry has allocated more than adequate levels of resources on hand and committed to enable full functionality of the plan and procedures, and Medistry’s experienced management team and new hires, along with the resources of CC and Verisign, are more than capable of successfully carrying out the functions set forth herein.

Scope/Scale Consistency Specific to Backend Registry Activities

Verisign, Medistry’s selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign’s infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign’s scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .MED gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign’s pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as “Other Operating Cost” (Template 1, Line I.L) within the Question 46 financial projections response.

29. Rights Protection Mechanisms

1 MECHANISMS DESIGNED TO PREVENT ABUSIVE REGISTRATIONS

Rights protection is a core objective of Medistry LLC (“Medistry”). Medistry will implement and adhere to any rights protection mechanisms (RPMs) that may be mandated from time to time by ICANN, including each mandatory RPM set forth in the Trademark Clearinghouse model contained in the Registry Agreement, specifically Specification 7. Medistry acknowledges that, at a minimum, ICANN requires a Sunrise period, a Trademark Claims period, and interaction with the Trademark Clearinghouse with respect to the registration of domain names for the .MED gTLD. It should be noted that because ICANN, as of the time of this application submission, has not issued final guidance with respect to the Trademark Clearinghouse, Medistry cannot fully detail the specific implementation of the Trademark Clearinghouse within this application. Medistry will adhere to all processes and procedures to comply with ICANN guidance once this guidance is finalized.

As described in this response, Medistry will implement a Sunrise period and Trademark Claims service with respect to the registration of domain names within the .MED gTLD. Certain aspects of the Sunrise period and⁄or Trademark Claims service may be administered on behalf of Medistry by Medistry-approved registrars or by subcontractors of Medistry, such as its selected backend registry services provider, Verisign. Medistry will also use, as detailed in the answer to Question 18, eligibility requirements which will also provide rights protection and which will be performed by Medistry and⁄or the Cleveland Clinic (CC), with enactment (for example, suspension or transfer) by Medistry.

Sunrise Period. As provided by the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook, the Sunrise service pre-registration procedure for domain names continues for at least 30 days prior to the launch of the general registration of domain names in the gTLD (unless Medistry decides to offer a longer Sunrise period).

During the Sunrise period, holders of marks that have been previously validated by the Trademark Clearinghouse receive notice of domain names that are an identical match (as defined in the ICANN Applicant Guidebook) to their mark(s). Such notice is in accordance with ICANN’s requirements and is provided by Medistry either directly or through Medistry-approved registrars.

Medistry requires all registrants, either directly or through Medistry-approved registrars, to i) affirm that said registrants meet the Sunrise Eligibility Requirements (SER) and ii) submit to the Sunrise Dispute Resolution Policy (SDRP) consistent with Section 6 of the Trademark Clearinghouse model. At a minimum Medistry recognizes and honors all word marks for which a proof of use was submitted and validated by the Trademark Clearinghouse as well as any additional eligibility requirements as specified in Question 18.

During the Sunrise period, Medistry and⁄or Medistry-approved registrars, as applicable, are responsible for determining whether each domain name is eligible to be registered (including in accordance with the SERs).

Trademark Claims Service. As provided by the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook, all new gTLDs will have to provide a Trademark Claims service for a minimum of 60 days after the launch of the general registration of domain names in the gTLD (Trademark Claims period).

During the Trademark Claims period, in accordance with ICANN’s requirements, Medistry or the Medistry-approved registrar will send a Trademark Claims Notice to any prospective registrant of a domain name that is an identical match (as defined in the ICANN Applicant Guidebook) to any mark that is validated in the Trademark Clearinghouse. The Trademark Claims Notice will include links to the Trademark Claims as listed in the Trademark Clearinghouse and will be provided at no cost.

Prior to registration of said domain name, Medistry or the Medistry-approved registrar will require each prospective registrant to provide the warranties dictated in the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook. Those warranties will include receipt and understanding of the Trademark Claims Notice and confirmation that registration and use of said domain name will not infringe on the trademark rights of the mark holders listed. Without receipt of said warranties, Medistry or the Medistry-approved registrar will not process the domain name registration.

Following the registration of a domain name, the Medistry-approved registrar will provide a notice of domain name registration to the holders of marks that have been previously validated by the Trademark Clearinghouse and are an identical match. This notice will be as dictated by ICANN. At a minimum Medistry will recognize and honor all word marks validated by the Trademark Clearinghouse.

Eligibility Restrictions. As set forth in the answer to Question 18, domain name registrations in .MED will be limited to CC, its partners and other trusted parties from the medical and healthcare fields as CC so determines. As set forth in the answer to Question 28, during the initial three years of operation of the .MED gTLD, all domains will be allocated by Request for Proposal (RFP). This will afford CC and Medistry the ability to employ eligibility restrictions in CC's discretion in the RFP criteria. At minimum, all RFP applicants will be required to identify themselves, and selected applicants will be required to provide their RFP identification information. Further, by the nature of the registration limitations set forth above, registrants will relate to entities that CC knows or otherwise trusts.

Beyond the initial three years of operation, CC and Medistry will review RFP allocation and determine appropriate methods for complying with the eligibility restrictions set forth the answer to Question 18 based upon (i) their review of the initial three year's worth of RFP allocation; (ii) the needs of users as determined by CC and Medistry; and (iii) the stated mission⁄purpose of the .MED gTLD.

Medistry will work with accredited registrars to ensure that required back-end functionality for the above allocation method is available.

2 MECHANISMS DESIGNED TO IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES ON AN ONGOING BASIS

In addition to the Sunrise and Trademark Claims services described in Section 1 of this response, Medistry implements and adheres to RPMs post-launch as mandated by ICANN, and confirms that registrars accredited for the .MED gTLD are in compliance with these mechanisms. Certain aspects of these post-launch RPMs may be administered on behalf of Medistry by Medistry-approved registrars or by subcontractors of Medistry, such as its selected backend registry services provider, Verisign.

These post-launch RPMs include the established Uniform Domain-Name Dispute-Resolution Policy (UDRP), as well as the newer Uniform Rapid Suspension System (URS) and Trademark Post-Delegation Dispute Resolution Procedure (PDDRP). Where applicable, Medistry will implement all determinations and decisions issued under the corresponding RPM.

After a domain name is registered, trademark holders can object to the registration through the UDRP or URS. Objections to the operation of the gTLD can be made through the PDDRP.

The following descriptions provide implementation details of each post-launch RPM for the .MED gTLD:

* UDRP: The UDRP provides a mechanism for complainants to object to domain name registrations. The complainant files its objection with a UDRP provider and the domain name registrant has an opportunity to respond. The UDRP provider makes a decision based on the papers filed. If the complainant is successful, ownership of the domain name registration is transferred to the complainant. If the complainant is not successful, ownership of the domain name remains with the domain name registrant. Medistry and entities operating on its behalf adhere to all decisions rendered by UDRP providers.

* URS: As provided in the Applicant Guidebook, all registries are required to implement the URS. Similar to the UDRP, a complainant files its objection with a URS provider. The URS provider conducts an administrative review for compliance with filing requirements. If the complaint passes review, the URS provider notifies the registry operator and locks the domain. A lock means that the registry restricts all changes to the registration data, but the name will continue to resolve. After the domain is locked, the complaint is served to the domain name registrant, who has an opportunity to respond. If the complainant is successful, the registry operator is informed and the domain name is suspended for the balance of the registration period; the domain name will not resolve to the original website, but to an informational web page provided by the URS provider. If the complainant is not successful, the URS is terminated and full control of the domain name registration is returned to the domain name registrant. Similar to the existing UDRP, Medistry and entities operating on its behalf adhere to decisions rendered by the URS providers.

* PDDRP: As provided in the Applicant Guidebook, all registries are required to implement the PDDRP. The PDDRP provides a mechanism for a complainant to object to the registry operator's manner of operation or use of the gTLD. The complainant files its objection with a PDDRP provider, who performs a threshold review. The registry operator has the opportunity to respond and the provider issues its determination based on the papers filed, although there may be opportunity for further discovery and a hearing. Medistry participates in the PDDRP process as specified in the Applicant Guidebook.

Additional Measures Specific to Rights Protection. Medistry provides additional measures against potentially abusive registrations. These measures help mitigate phishing, pharming, and other

Internet security threats. The measures exceed the minimum requirements for RPMs defined by Specification 7 of the Registry Agreement and are available at the time of registration. These measures include:

* Rapid Takedown or Suspension Based on Court Orders: Medistry complies promptly with any order from a court of competent jurisdiction that directs it to take any action on a domain name that is within its technical capabilities as a TLD registry. These orders may be issued when abusive content, such as child pornography, counterfeit goods, or illegal pharmaceuticals, is associated with the domain name.

* Anti-Abuse Process: Medistry implements an anti-abuse process that is executed on domain name takedown requests. The scope of the anti-abuse process includes malicious exploitation of the DNS infrastructure, such as phishing, botnets, and malware.

* Authentication Procedures: Verisign, Medistry’s selected backend registry services provider, uses two-factor authentication to augment security protocols for telephone, email, and chat communications.

* Registry Lock: This Verisign service allows registrants to lock a domain name at the registry level to protect against both unintended and malicious changes, deletions, and transfers. Only Verisign, as Medistry’s backend registry services provider, can release the lock; thus all other entities that normally are permitted to update Shared Registration System (SRS) records are prevented from doing so. This lock is released only after the registrar makes the request to unlock.

* Malware Code Identification: This safeguard reduces opportunities for abusive behaviors that use registered domain names in the gTLD. Registrants are often unknowing victims of malware exploits. As Medistry’s backend registry services provider, Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.

* DNSSEC Signing Service: Domain Name System Security Extensions (DNSSEC) helps mitigate pharming attacks that use cache poisoning to redirect unsuspecting users to fraudulent websites or addresses. It uses public key cryptography to digitally sign DNS data when it comes into the system and then validate it at its destination. The .MED gTLD is DNSSEC-enabled as part of Verisign’s core backend registry services.

3. RESOURCING PLANS

Resource Planning

Resourcing plans for the initial implementation of, and ongoing maintenance for, the rights protection mechanisms in Part 1 of the answer to this Question 29, except for those relating to eligibility requirements, are set forth in the answer to Question 49(a) – contingency planning (detailed further below). As ICANN has not issued final guidance with regard to the Trademark Clearinghouse, and particularly the costs associated with the Clearinghouse, subcontractors and backend providers, such as Verisign, have not been able to quote costs and resource allocations for implementation of the Clearinghouse and other RPMs which incorporate the Clearinghouse. Medistry will determine which entity(ies) will provide which services, and allocate costs and resources accordingly, once ICANN has determined a Clearinghouse cost and Medistry can determine subcontractor⁄Verisign pricing and availability. In any event, Medistry has a firm commitment from Verisign that, at minimum, Verisign will work with Medistry to provide all the necessary resources and services to implement and maintain the RPMs contemplated in this answer, and as set forth in Question 49(a), Medistry has allocated sufficient committed resources to ensure sufficient resources to cover Verisign’s (or other subcontractor’s) costs.

With regard to the other RPMs identified herein, Medistry’s management team is an experienced team which has managed an sTLD (.JOBS) for over six years and is well-acquainted with domain abuse prevention and mitigation.

Medistry internal operations for all RPMs will scale as needed to accommodate the volume and nature of all matters not handled by Verisign or subcontractors, including shifting allocations of time from the management team, General Counsel, Customer Support personnel and Technical Labor personnel. In the event registration volume and related income allow, and RPM matter volume dictates, additional personnel may be added to accommodate the matters, up to and including addition of a dedicated RPM Manager with a staff commensurate to need.

Costs for Medistry’s operations as detailed above are addressed in the response to Question 47. Specifically, $5,000 has been attributed to legal as part of general administrative expenses per year (see table 3 provided in response to Question 47). In addition, per the Financial Projections Template submitted in response to Question 46, $10,000 per year is budgeted under Other Operating Costs in case of unexpected contingencies, such as the use of outside legal counsel.

With regard to operation of RPMs relating to eligibility requirements, CC is a world-famous and multi-national medical institution. CC has an experienced management team, compliance team and legal team for overseeing use of the .MED gTLD. With regard to eligibility requirement complaints or other complaints which relate to rights protection which may violate any CC policy, CC will establish, implement and maintain internal procedures for addressing such claims. Such procedures may involve input from management, compliance and legal, and legal may consult with outside legal counsel. CC has sufficient resources and personnel to provide the compliance services attributed to CC herein.

CC’s internal costs for abuse complaint procedures will be borne by CC, and are thus not included in the response to Question 47.

Resource Planning Specific to Backend Registry Activities

Verisign, Medistry’s selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD’s initial implementation and ongoing maintenance. Verisign’s pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as Line IIb.G, Total Critical Registry Function Cash Outflows, within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign’s quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign’s ability to align personnel resource growth to the scale increases of Verisign’s TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the implementation of RPMs:

* Customer Affairs Organization: 9
* Customer Support Personnel: 36
* Information Security Engineers: 11

To implement and manage the .MED gTLD as described in this application, Verisign, Medistry’s selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign’s internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet’s largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

30(a). Security Policy: Summary of the security policy for the proposed registry

1 DETAILED DESCRIPTION OF PROCESSES AND SOLUTIONS DEPLOYED TO MANAGE LOGICAL SECURITY ACROSS INFRASTRUCTURE AND SYSTEMS, MONITORING AND DETECTING THREATS AND SECURITY VULNERABILITIES AND TAKING APPROPRIATE STEPS TO RESOLVE THEM

Medistry LLC’s (“Medistry”) selected backend registry services provider’s (Verisign’s) comprehensive security policy has evolved over the years as part of managing some of the world’s most critical TLDs. Verisign’s Information Security Policy is the primary guideline that sets the baseline for all other policies, procedures, and standards that Verisign follows. This security policy addresses all of the critical components for the management of backend registry services, including architecture, engineering, and operations.

Verisign’s general security policies and standards with respect to these areas are provided as follows:

* Architecture

Information Security Architecture Standard: This standard establishes the Verisign standard for application and network architecture. The document explains the methods for segmenting application tiers, using authentication mechanisms, and implementing application functions.

Information Security Secure Linux Standard: This standard establishes the information security requirements for all systems that run Linux throughout the Verisign organization.

Information Security Secure Oracle Standard: This standard establishes the information security requirements for all systems that run Oracle throughout the Verisign organization.

Information Security Remote Access Standard: This standard establishes the information security requirements for remote access to terminal services throughout the Verisign organization.

Information Security SSH Standard: This standard establishes the information security requirements for the application of Secure Shell (SSH) on all systems throughout the Verisign organization.

* Engineering

Secure SSL⁄TLS Configuration Standard: This standard establishes the information security requirements for the configuration of Secure Sockets Layer⁄Transport Layer Security (SSL⁄TLS) for all systems throughout the Verisign organization.

Information Security C++ Standards: These standards explain how to use and implement the functions and application programming interfaces (APIs) within C++. The document also describes how to perform logging, authentication, and database connectivity.

Information Security Java Standards: These standards explain how to use and implement the functions and APIs within Java. The document also describes how to perform logging, authentication, and database connectivity.

* Operations

Information Security DNS Standard: This standard establishes the information security requirements for all systems that run DNS systems throughout the Verisign organization.

Information Security Cryptographic Key Management Standard: This standard provides detailed information on both technology and processes for the use of encryption on Verisign information security systems.

Secure Apache Standard: Verisign has a multitude of Apache web servers, which are used in both production and development environments on the Verisign intranet and on the Internet. They provide a centralized, dynamic, and extensible interface to various other systems that deliver information to the end user. Because of their exposure and the confidential nature of the data that these systems host, adequate security measures must be in place. The Secure Apache Standard establishes the information security requirements for all systems that run Apache web servers throughout the Verisign organization.

Secure Sendmail Standard: Verisign uses sendmail servers in both the production and development environments on the Verisign intranet and on the Internet. Sendmail allows users to communicate with one another via email. The Secure Sendmail Standard establishes the information security requirements for all systems that run sendmail servers throughout the Verisign organization.

Secure Logging Standard: This standard establishes the information security logging requirements for all systems and applications throughout the Verisign organization. Where specific standards documents have been created for operating systems or applications, the logging standards have been detailed. This document covers all technologies.

Patch Management Standard: This standard establishes the information security patch and upgrade management requirements for all systems and applications throughout Verisign.

* General

Secure Password Standard: Because passwords are the most popular and, in many cases, the sole mechanism for authenticating a user to a system, great care must be taken to help ensure that passwords are “strong” and secure. The Secure Password Standard details requirements for the use and implementation of passwords.

Secure Anti-Virus Standard: Verisign must be protected continuously from computer viruses and other forms of malicious code. These threats can cause significant damage to the overall operation and security of the Verisign network. The Secure Anti-Virus Standard describes the requirements for minimizing the occurrence and impact of these incidents.

Security processes and solutions for the .MED TLD are based on the standards defined above, each of which is derived from Verisign’s experience and industry best practice. These standards comprise the framework for the overall security solution and applicable processes implemented across all products under Verisign’s management. The security solution and applicable processes include, but are not limited to:

* System and network access control (e.g., monitoring, logging, and backup)
* Independent assessment and periodic independent assessment reports
* Denial of service (DoS) and distributed denial of service (DDoS) attack mitigation
* Computer and network incident response policies, plans, and processes

* Minimization of risk of unauthorized access to systems or tampering with registry data
* Intrusion detection mechanisms, threat analysis, defenses, and updates
* Auditing of network access
* Physical security

Further details of these processes and solutions are provided in Part B of this response.

1.1 Security Policy and Procedures for the Proposed Registry

Specific security policy related details, requested as the bulleted items of Question 30 – Part A, are provided here.

Independent Assessment and Periodic Independent Assessment Reports. To help ensure effective security controls are in place, Medistry, through its selected backend registry services provider, Verisign, conducts a yearly American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70 audit on all of its data centers, hosted systems, and applications. During these SAS 70 audits, security controls at the operational, technical, and human level are rigorously tested. These audits are conducted by a certified and accredited third party and help ensure that Verisign in-place environments meet the security criteria specified in Verisign's customer contractual agreements and are in accordance with commercially accepted security controls and practices. Verisign also performs numerous audits throughout the year to verify its security processes and activities. These audits cover many different environments and technologies and validate Verisign's capability to protect its registry and DNS resolution environments. Figure 30A-1 lists a subset of the audits that Verisign conducts. For each audit program or certification listed in Figure 30A-1. Verisign has included, as attachments to the Part B component of this response, copies of the assessment reports conducted by the listed third-party auditor. From Verisign's experience operating registries, it has determined that together these audit programs and certifications provide a reliable means to ensure effective security controls are in place and that these controls are sufficient to meet ICANN security requirements and therefore are commensurate with the guidelines defined by ISO 27001.

Figure 30A-1: See Medistry LLC_Q30A_security policy

Augmented Security Levels or Capabilities. See Section 5 of this response.

Commitments Made to Registrants Concerning Security Levels. See Section 4 of this response.

2 SECURITY CAPABILITIES ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Medistry's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .MED gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Medistry's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Medistry fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel role, which is described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support its security policy:

* Information Security Engineers: 11

To implement and manage the .MED gTLD as described in this application, Verisign, Medistry's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 SECURITY MEASURES ARE CONSISTENT WITH ANY COMMITMENTS MADE TO REGISTRANTS REGARDING SECURITY LEVELS

Verisign is Medistry's selected backend registry services provider. For the .MED gTLD, no unique security measures or commitments must be made by Verisign or Medistry to any registrant.

5 SECURITY MEASURES ARE APPROPRIATE FOR THE APPLIED-FOR gTLD STRING (FOR EXAMPLE, APPLICATIONS FOR STRINGS WITH UNIQUE TRUST IMPLICATIONS, SUCH AS FINANCIAL SERVICES-ORIENTED STRINGS, WOULD BE EXPECTED TO PROVIDE A COMMENSURATE LEVEL OF SECURITY)

No unique security measures are necessary to implement the .MED gTLD. As defined in Section 1 of this response, Verisign, Medistry's selected backend registry services provider, commits to providing backend registry services in accordance with the following international and relevant security standards:

* American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70

* WebTrust/SysTrust for Certification Authorities (CA)