Exhibit 1

Code of Conduct Exemption Request Form

Internet Corporation for Assigned Names and Numbers ("ICANN")
12025 Waterfront Drive, Suite 300
Los Angeles, California 90094
Attention: New gTLD Program Staff

RE: Request for Exemption from Registry Operator Code of Conduct

Bloomberg IP Finance LLC ("Registry Operator"), in connection with the execution of the Registry Agreement for the <.bloomberg> TLD (the "Registry Agreement"), hereby requests an exemption from the obligations of the Registry Operator Code of Conduct set forth in Specification 9 to the Registry Agreement (the "Code of Conduct"). Pursuant to such request, Registry Operator confirms that each of the following statements is true and correct (collectively, referred to as the "Statements"):

1. All domain name registrations in the TLD are registered to, and maintained by, Registry Operator for the exclusive use of Registry Operator or its Affiliate (as defined in the Registry Agreement);

2. Registry Operator does not sell, distribute or transfer control or use of any registrations in the TLD to any third party that is not an Affiliate of Registry Operator; and

3. Application of the Code of Conduct to the TLD is not necessary to protect the public interest for the following reasons:

Since Registry Operator will only permit registrations in its gTLD to itself and its affiliates, its compliance with the Code of Conduct would serve only to protect Registry Operator from itself, which is unnecessary. Application of the Code of Conduct to Registry Operator would thus be an inefficient use of Registry Operator resources and also ineffective to meet the purpose of the Code of Conduct of protecting the public.

Should the Exemption Request not be approved, ICANN will inform the Registry Operator as to the reason for the rejection and explain whether the Exemption Request is eligible for resubmission.

Schedule A

Registry Operator hereby acknowledges that the following are the true and correct registration policies for the TLD:

[Registry Operator to attach registration policies for the TLD]

Registry Operator represents that the registration policies attached hereto as Schedule A are a true and correct copy of the Registry Operator's registration policies for the TLD. Registry Operator agrees to notify ICANN promptly in writing in the event any of the Statements has become untrue (whether before or after an exemption has been granted). Registry Operator further acknowledges and agrees that the Exemption will be void if at any time any of the Statements has become untrue.

Submitted by: [redacted]

Position: Vice President and Counsel

Date Noted: February 11, 2014

Email: [redacted]

<.bloomberg> Registration Policies

As stated at length in the Application Number 1-1981-76785 (the "**Application**") filed by Bloomberg IP Holdings LLC ("**BIP**") to operate the gTLD <.bloomberg> (the "**gTLD**"), Michael R. Bloomberg is a former mayor of New York City and the founder and majority owner of Bloomberg L.P. ("**BLP**"). Mr. Bloomberg formed BIP for the purpose of applying to run and operating the gTLD. BIP intends to use the gTLD to register domain names for Bloomberg Philanthropies, a name describing all of Mr. Bloomberg's charitable and civic work, including personal giving, political advocacy, and fee-free consulting services for cities and municipal governments. BIP will also use the gTLD to register domain names for BLP for use by BLP and its affiliates in their lines of business, including the operation of the BLOOMBERG PROFESSIONAL service (a global financial information service) and other media and consumer businesses.

Bloomberg Philanthropies. Mr. Bloomberg believes in the power of philanthropy and political advocacy to change people's lives for the better. Toward this end, Mr. Bloomberg has donated more than $1.6 billion to a variety of causes and organizations. In 2011 alone, $330 million was distributed by Bloomberg Philanthropies, placing Mr. Bloomberg in the top five of The Chronicle of Philanthropy's list of America's top 50 philanthropists. Bloomberg Philanthropies works in several areas, primarily including:

Public Health: Bloomberg Philanthropies has invested more than $375 million over the past six-years, and has committed more than $220 million to be spent over the next four years. This money has been and will be used to combat the growing number of deaths caused by non-communicable diseases worldwide. Efforts have been directed toward reducing global tobacco use, improving global road safety, and improving maternal health in Tanzania;

The Environment: As chair of the C40 Cities Climate Leadership Group, Mr. Bloomberg is working with the world's largest cities to help reduce greenhouse gas emissions, and has made a specific investment in the Sierra Club's Beyond Coal Campaign, to help eliminate one-third of the top polluting coal plants in the United States by 2020;

Government Innovation: Bloomberg Philanthropies has invested resources to spread proven and promising ideas among cities, including the Innovation Delivery Team program to help mayors drive bold reform, and New York City's efforts to improve outcomes for young black and Hispanic men. Alongside this, Bloomberg Philanthropies has contributed to work with Cities of Service, Mayors against Illegal Guns, and the Mayor's Fund to Advance NYC. In December 2013, Mr. Bloomberg formed Bloomberg Associates Foundation, which will provide fee-free consultation to cities and municipalities to support public service projects;

The Arts: Bloomberg Philanthropies invests in strengthening New York City arts and cultural organizations, which include a world-class management training program; and

Education: Bloomberg Philanthropies has targeted efforts to strengthen leadership within school communities and advance good public policy at the federal, state and local levels.

Bloomberg L.P. In 1981, Mr. Bloomberg founded the company that would come to be called Bloomberg L.P. BLP has since become one of the largest worldwide providers of financial news, data, analytics and information and related goods and services.

BLP's international expansion began in 1987 with the opening of offices in London and Tokyo, and continued with establishment of offices in Sydney (1989), Singapore (1990), Frankfurt (1992) and Hong Kong (1993). BLP employs more than 15,000 people in over 135 offices, including over 2,300 professionals in more than 152 news bureaus.

To distinguish its products and services, BLP adopted the "Bloomberg" trade name and BLOOMBERG trademark and service mark (the "**BLOOMBERG Marks**") at least as early as August 1987. In 2007, BLP reorganized and placed ownership of its BLOOMBERG Marks and the related domain names in a subsidiary, Bloomberg Finance L.P. ("**BFLP**"), and regional subsidiaries of BFLP (BLP, BFLP and their subsidiaries, collectively, "**Bloomberg**"). Bloomberg has registered BLOOMBERG Marks in the United States over 100 other jurisdictions. Bloomberg has also registered over 1,000 domain names incorporating "bloomberg" or a misspelling thereof.

In addition to providing financial information, data and transactional services through its terminal product and over the Internet, Bloomberg collects and reports news through *Bloomberg Markets, Bloomberg Businessweek* and *Bloomberg Pursuits* magazines, over the radio through WBBR - 1130 AM in New York City and syndication throughout the United States and through satellite radio providers, and over cable and satellite television provided 24-hours a day throughout the world and local television partnerships in India, Turkey, Russia, Mongolia, Middle East, sub-Saharan Africa, and Mexico/Latin America.

Because BIP will confine use of the gTLD to the charitable purposes of Bloomberg Philanthropies and the commercial services of Bloomberg, the reputation of these entities will be paramount in such use. It will thus clearly be in BIP's interest to ensure the highest level of service to these related entities. To further this goal, BIP will follow the policies and procedures required by the Registry Agreement. BIP will also adopt a privacy policy providing that it will: (i) only collect personal data from users that is directly required for the registration process; (ii) notify users as to how their personal data will be collected and used; (iii) give users the choice to opt out of providing personal data; (iv) permit the transfer of users' personal data to third parties only as needed; (v) mandate reasonable efforts to prevent the loss or unauthorized disclosure of personal data; and (vi) allow users to review and access their personal data.

Verisign, BIP's back-end service provider, employs user accounts to provide access to system and network components. Verisign specifically determines and manages all accounts and account types to help ensure that only explicitly authorized accounts are allowed to exist on any given host. Individual accounts may comprise both real physical users as well as software entities that are needed for the proper execution of Verisign software. Where a physical user is concerned, only current Verisign employees with a specific need for access to a specific host are allowed access. In compliance with Verisign access control policies, this need is determined, reviewed, and ultimately approved through the change management process. No guest, anonymous, or temporary accounts are allowed. Groups and group membership are determined on an as-needed basis and also created, modified or deleted via the change management process.

Verisign Architecture and Technology Services determine system-level accounts. The engineering team responsible for Verisign code and Verisign Architecture and Technology Services determines application accounts for any third-party software running on the information system.

Verisign enforces access control through operating system access control lists ("**ACL**s"), router ACLs, firewall rules, content switching engine rules, Windows domain authentication, application-level ACLs, and "jump servers" for its systems. Verisign restricts each user to the least privileged level of access required to perform his or her duties, and it logs both successful and failed accesses. Modifications to any enforcement rule are managed through the change control process and its approval step(s). Verisign further controls administrative-level network access to servers in the information system by using jump servers to restrict access. Only after satisfying all other control rules, policies, and subsequently accessing a jump server (subject to the same rules mentioned above) can a user acquire server-level access over the network to a component of the information system.

Verisign uses Sourcefire intrusion detection systems ("**IDS**") (the commercial version of the open-source Snort software) actively to monitor system network behavior. The Sourcefire Defense Center application centrally manages these systems. Verisign also actively monitors system network activity via Checkpoint firewalls deployed with built-in IDS capabilities. Only authorized personnel can access the Sourcefire IDS and Checkpoint firewalls. In addition, all servers and workstations deployed within Verisign maintain and make available system logs as described in Verisign's Secure Logging Standard.

Verisign's Network Operations Center ("**NOC**") is staffed and operational 24/7 to monitor systems. NOC personnel are required to follow a shift operator checklist that details hourly responsibilities and tasks. The NOC uses multiple tools to support analysis of event data on systems. A Nagios-based monitoring system is also deployed on critical systems to watch events. The NOC staff proactively runs reports on system errors by examining intrusions through Sourcefire. The NOC also uses Syslog reporting to monitor website links, website performance and hardware (*e.g.*, switches, routers, and firewalls). Syslog also ensures that system backups complete as scheduled. In addition, Verisign's Security Group conducts daily vulnerability scans (*e.g.*, Nessus and Qualys) against all production (*i.e.*, Internet-accessible) servers.

The NOC can modify the monitoring systems to recognize emerging threats and known "compromise patterns," based on information relayed to Verisign by credible sources. Engineers can also configure the systems to alert Verisign security teams when they detect threats or compromises. Verisign backs up system access logs for each applicable server, network device and component, and these logs support security audits or focused incident investigations.

Verisign conducts management of updates between the registry systems and name servers remotely over secure VPNs or other secure mechanisms and monitored around the clock.

To ensure effective security controls, Verisign conducts a yearly American Institute of Certified Public Accountants/ Canadian Institute of Chartered Accountants SAS 70 audit on all its data centers, hosted systems and applications. Verisign also performs numerous audits to verify its security processes and activities that cover many different environments and technologies and validate Verisign's capability to protect its registry and DNS resolution environments. For each audit program or certification, Verisign generates assessment reports conducted by the listed third-party auditor. These audit programs and certifications ensure effective security controls sufficient to meet ICANN security requirements and therefore are commensurate with the guidelines defined by ISO 27001.

While denial of service ("**DoS**") and distributed denial of service ("**DDoS**") attacks are frequent, Verisign reports that its DNS has maintained operational accuracy and stability 100 percent of the time for all TLDs under Verisign's management, and TLD zone data has never been corrupted as a result of a DoS or DDoS attack. All Verisign systems are fully operationally redundant as well as geographically redundant. Verisign also leverages different types of operating systems and software to minimize the impact of vendor-specific vulnerabilities. In addition, Verisign's optimized software, by its proprietary nature, reduces the risk of malicious actors exploiting vulnerabilities that may be detected and publicized should the code exist in the public domain. Finally, Verisign has implemented security features into its network to address certain types of common DoS attacks, such as SYN floods, where an attacker sends a succession of SYN requests to a target's system.

In the event of a DoS or DDoS attack, the Verisign NOC notifies the TLD support group immediately. The Information Security and Networking groups also contribute to attack response, which can include IP address blocking, rate limiting, content filtering, and even transition to alternate facilities.

Verisign formally documents its incident response policies and procedures in the Verisign Security Incident Response Process document. This document defines the incident response process's purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance policies. The Incident Response Process document is published on the Verisign intranet and is updated annually.

All Verisign personnel are responsible for immediately reporting suspected security incidents to the Information Security Department. The notified personnel coordinate notification of additional personnel as needed. Internal or external escalation of incidents is based upon contractual agreements and legal requirements and is outlined in the Incident Response Process document.

Automated mechanisms such as Sourcefire, Palo Alto, and Damballa assist in reporting security incidents to designated officials.

Verisign tracks and documents each information system security incident by creating an incident response report, incident response escalation report, and post mortem report as required by the Information Security Policy. Verisign's internal Incident Response wiki pages track incident reporting procedures and incident monitoring and reporting. An Oracle web-based application tracks corporate network incidents.

Verisign employs a comprehensive security plan through all phases of system development, deployment, and operation. The Verisign Information Security Secure Coding Questionnaire captures the data necessary to guide a Vulnerability, Attack, Misuse Analysis ("**VAMA**") review process that is designed to expose and address security flaws and potential policy violations within an information system prior to production deployment. This reduces the risk of unauthorized access to systems or tampering with registry data. Subsequent releases and architecture changes require re-submission to the VAMA review process. Prior to production deployment, Qualys, Nessus, and/or Cenzic scanners scan all systems for known flaws and vulnerabilities.

Verisign's security staff uses Qualys and Nessus scanners to conduct daily vulnerability scans against all production servers that are accessible via the Internet. This scanning automatically conducts periodic scans that include scanning for enumeration software flaws. The Qualys scans rank the vulnerabilities based on impact. Monthly vulnerability scans are conducted against all internal non-production machines.

Verisign also conducts regular security tests to identify vulnerabilities and attack vectors that could be used to exploit enterprise systems. Tests focus on simulating attacks from inside and outside the network perimeter (*e.g.,* the Internet or wireless frequencies around the organization). Verisign also performs periodic exercises to test the readiness of Verisign teams to identify and respond to attacks. Discovered systematic problems are fully mitigated. Verisign employs outside assessors to conduct security tests bi-annually against Verisign's products.

In accordance with Verisign's security vulnerability management process, Information Security performs daily reviews of all publicly known security vulnerabilities identified through system scans or disclosure by public sources. Information Security determines the severity of the issues and initiates an emergency patch process, a trouble ticketing system to route for correction all vulnerabilities that do not meet the criteria for emergency patching.

To implement its Security Patch Management process, Verisign has five security levels:
Level 5: emergency security incident; mitigation to be implemented within 24 hours;
Level 4: high-level security incident; mitigation to be implemented within 48 hours;
Level 3: moderate-level security incident; mitigation to be implemented within five business days; Level 2: low-level security incident; mitigation to be included in next point release; and Level 1: low-level security incident; mitigation to be included in next major/minor release. This framework accomplishes the objectives of the Patch and Vulnerability Group ("**PVG**") function,

outlined in National Institute of Standards and Technology ("**NIST**") SP 800-40, by providing a systematic, accountable and documented process for managing exposure to vulnerabilities through the timely deployment of patches.

Verisign's diligence processes further manage risk and identify new vulnerabilities, and help maintain security in all environments under Verisign's management.

Verisign information security practices include the following diligence processes:

Development and Architectural Reviews: Information security is an integral part of the standard system development lifecycle ("**SDLC**"). Verisign implements methods at the development level to prevent known attacks and possible failures and to help ensure an expedient and secure SDLC. Internal Information Security staff members perform audits and give approvals at the architecture level to help ensure compliance with applicable standards;

Pre-Production Audit: All implementations of software and hardware undergo an Information Security audit before deployment to production environments. This audit includes vulnerability scanning, internal configuration review against standards, and patch-level review against known vulnerabilities;

Vulnerability Scanning: Verisign performs weekly vulnerability scanning on all its external facing systems, including the DNS registry infrastructure. Vulnerability information is updated daily to reflect the latest identified threats. Reports are distributed to all respective environment owners for remediation, and specific internal service levels are attached to each severity level;

Advisory Monitoring: Verisign performs daily reviews of vulnerabilities as they are made public. Advisories are categorized based on their severity. Internal service levels are associated with each category and specify the timeframe in which the advisory must be resolved. The completion of these tasks is monitored through the vulnerability scanning process, which is performed daily; and

Internal/External Audit and Review: Verisign performs numerous audits to verify its security processes and activities, covering many different environments and technologies.

Verisign's Information Security audit process outlines the controls used to audit environments and conduct internal risk assessments of those controls. Verisign's risk assessment process examines the effectiveness and applicability of controls and is performed twice a year. Verisign revises and enhances controls as a result of the risk assessment and applies the enhanced control set to the next security assessment of the environment.

Verisign incorporates automated mechanisms such as the Sourcefire IDS, Damballa, FireEye malware analysis tool, Palo Alto firewalls, Checkpoint firewalls, and McAfee antivirus suite in order to track, collect, and analyze security incident information.

The gTLD will also benefit from threat analyses from Verisign iDefense Security Intelligence Services. Verisign iDefense proactively manages threat intelligence to provide informed recommendations for threat mitigation across global and regional threat landscapes. Verisign iDefense intelligence includes in-depth country and regional intelligence reports, a real-time threat feed, and access to subject matter experts across vulnerability, malicious code and global cyber security teams.

Verisign iDefense intelligence enables Verisign security teams to: understand the global implications of any emerging or existing threat as it evolves; proactively protect Verisign's registry systems from the threats that matter most; prioritize threat mitigation strategies and focus internal resources; and make more accurate and efficient decisions to support successful incident and fraud response strategies and actions.

Verisign periodically examines audit records for indications of inappropriate or unusual activity. The frequency of audits is defined in Verisign's Secure Logging Standard. Activities that raise suspicion are investigated in accordance with organizational policy. Investigation findings are reported to appropriate organizational officials and acted upon in accordance with the Secure Logging Standard. Verssing's system integrates audit review, analysis and reporting processes based upon review of these activities.

In addition, Verisign monitors information obtained from various organizations, including law enforcement, intelligence and other credible sources. Verisign increases its level of audit monitoring and analysis as specified whenever an increased threat is perceived. To ensure compliance with the Account Management Policy, all accounts are audited quarterly to evaluate and validate users' need for access to resources and to ensure appropriate permissions are in effect.

Verisign's data center facilities provide the secure underlying physical infrastructure required to support a growing critical Internet infrastructure at a time when external attacks are increasing. Physical security includes 24/7 onsite security officers and access control for all Verisign owned and operated data centers, and all co-location name server facilities.

Verisign data center facilities are monitored and recorded 24/7 via closed-circuit television, with cameras located outside and inside the facilities. All aspects of the Verisign registry provisioning, distribution and resolution systems—including system health, system performance, system load and attempted system intrusions—are monitored in 60-second increments. Furthermore all card access and biometric access is monitored and logged. Facility security also addresses the entire spectrum of threats, including inadvertent or malicious activity, natural disasters and terrorist activities.

Physical security for Verisign's data centers includes: low profile (*e.g.*, no external markings or signage); isolation from easements, rights of way, and adjoining tenants; hardening against regional weather events (*e.g.*, high winds, hurricanes); location outside of flood areas; and

multilevel physical security, including a 24/7 onsite security force, badge readers, and biometric access control devices.

All Verisign production systems operate within a Tier 4 facility, meaning that four physical separation and validation points must be passed to access the facility. Verisign's requires both card and biometrics verification for Tier 4 access.

This system includes closed-circuit television on sensitive racks, door contact alarms, and alerts to the Verisign global NOC. In the event that a rack or data center is accessed via unauthorized means, the NOC is notified and corrective actions are taken.

Verisign's dedicated Information Security Group is responsible for: managing and owning all aspects of information security within Verisign; maintaining the security of organizational information processing facilities and information assets accessed by third parties; maintaining the security of information when processing has been outsourced to another organization; facilitating authorized access to corporate data by third parties, and managing the steps to prevent and detect unauthorized access of this kind; maintaining security policies, standards and guidelines to support the mission of the company; performing an annual risk analysis and creating a Security Program Plan aligned with the business and its objectives; managing the execution of audits and supporting the compliance program; providing training on information security-related topics to all stakeholders; working with stakeholders to ensure that technology is implemented in a secure and business-oriented manner; maintaining a secure coding program that ensures the successful and secure deployment of code throughout Verisign; maintaining a threat and vulnerability program that proactively monitors and detects threats to Verisign's information systems; conducting incident response activities for both the production and Verisign corporate environments; and engaging outside agencies as needed with the support of legal, human resources, and business units to achieve business objectives and/or to protect Verisign information.

The Security Intelligence team provides global security monitoring and support for incident response over Verisign's corporate and production systems. The team's activities include full lifecycle management of the intrusion detection system ("**IDS**"), threat and vulnerability management, network access control audits, and the creation of custom toolsets.

The Incident Response team supports large-scale incident management and information security projects. Under the direction of the Information Security Incident Response manager, the team performs incident handling and response activities and implements technical security controls in the operational and non-operational environments. The team designs and applies security controls in an efficient and effective manner to ensure maximum service availability.

The Audit Risk and Compliance team is responsible for implementing the Information Security Program's risk and control framework and IT risk strategy, information technology audits

(internal and external); security risk management; security governance; security awareness and training; application security; and incident response support.

All teams work together to provide a ring of protection to safeguard Verisign's IT infrastructure components and supporting systems from cyber-attack and to help ensure the confidentiality, integrity and availability of these systems.

It is critical to Verisign's business to adopt processes and procedures that protect the relationship of trust Verisign enjoys with its customers. A key component of this trust is Verisign's assurance that all Verisign employees must pass background investigations prior to being hired. Verisign employees who have access to critical areas, such as production systems, submit to an enhanced level of background investigation.

One of two types of background investigations is performed on Verisign contractors, consultants, and prospective employees. All personnel are required to pass the Basic Background ("**BBIS**") and must re-qualify every five years. The BBIS checks for items such as criminal records, employment records, education records, motor vehicle records, national identification numbers, and professional references. Personnel requiring access to data center facilities or other restricted areas are required to pass an Enhanced Background ("**EBIS**"), which adds a credit check to the BBIS.

Verisign operates a robust and reliable SRS that enables multiple registrars to provide domain name registration services in the gTLD. Verisign's proven reliable SRS serves approximately 915 registrars, and Verisign 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: a web interface, which allows customers to access the authoritative database for accounts, contacts, users, authorization groups, product catalog, product subscriptions, and customer notification messages; an EPP interface, which enables registrars to use EPP to register and manage domains, hosts, and contacts; and a Verisign developed application 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 will allow registrars to manage the gTLD domain names in a single architecture.

To flexibly accommodate the scale of its transaction volumes, as well as new technologies, Verisign employs: scale to handle current volumes and projected growth; scale to twice base capacity to withstand "registration add attacks" from a compromised registrar system; database CPU utilization Limits to no more than 50 percent during peak loads; and allocation of a small

segment of memory to each user's login process to perform connection overhead, sorting and data caching. Verisign allocates no more than 40 percent of the total available physical memory on the database server to these functions.

Verisign's SRS is built upon a three-tier architecture: "Gateway Layer" servers use EPP to communicate with registrars and interact with application servers; "Application Layer" servers contain business logic for managing and maintaining the registry business particular to the gTLD's business rules and requirements and store BIP's data; the Database Layer stores all essential information provisioned from registrars through the gateway servers and separate servers query the database, extract updated zone and Whois information, validate that information, and distribute it around the clock to Verisign's domain name resolution sites.

Verisign implements its scalable SRS on a supportable infrastructure employing patterns of simplicity and parallelism in its software and systems. Verisign intentionally minimizes the number of lines of code between the end user and the data delivered, resulting in a network of restorable components that provide updates. Local redundancy is maintained for each layer as well as each piece of equipment and this enhances operational performance while enabling the future system scaling necessary to meet additional demand created by this or future registry applications. Local SRS redundancy also enables Verisign to take down individual system components for maintenance and upgrades.

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 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 service availability and the server configuration. To ensure continuity of operations for the gTLD, Verisign uses a minimum of 100 dedicated servers per SRS site, virtualized to meet demand.

Verisign uses synchronous replication to keep the Verisign SRS 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. 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."

Scalability and performance are consistent with the overall business approach and planned size of the registry. Verisign is an experienced backend registry provider, which uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include server capacity, data storage volume and network throughput 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 and provide the means to link the projected infrastructure needs of the gTLD with necessary implementation and sustainment cost. Verisign derived the infrastructure required to implement and sustain the gTLD by examining projected usage volume for the most likely scenario.

Verisign's proprietary resourcing models project the number and type of personnel resources necessary to operate the gTLD and adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Verisign derived the necessary personnel levels required for the gTLD's initial implementation and ongoing maintenance by assessing the projected usage volume for the most likely scenario. .

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. Drawing from this pool of on-hand and fully committed technical resources, Verisign reports that it 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 that it will use the following personnel roles to support SRS performance: 19 application engineers; 8 database administrators; 3 database engineers; 11 network administrators; 4 network architects; 25 project managers; 11 quality assurance engineers; 13 SRS system administrators; 4 storage administrators; and 9 systems architects.

To implement and manage the gTLD, Verisign 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, who are interviewed by the leads of the relevant technical areas. By scaling one common team across all its TLDs, 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 the 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.

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. 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. Moreover, prior to deployment, BIP will provide to ICANN updated documentation of all the EPP objects and extensions supported in accordance with Specification 6, Section 1.2.

Verisign's SRS meets all EPP Registry Performance Specifications detailed in Specification 10, Section 2, which can be verified by a review of the <.com> and <.net> Registry Operator's Monthly Reports filed with ICANN. These reports detail the operational status of the <.com> and <.net> registries, which use an SRS design and approach comparable to the one proposed for the 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: ≤ 864 minutes of downtime (≈98%); EPP session-command round trip time (RTT): ≤4000 milliseconds (ms), for at least 90 percent of the commands; EPP query-command RTT: ≤2000 ms, for at least 90 percent of the commands; and EPP transform-command RTT: ≤4000 ms, for at least 90 percent of the commands.