The specifications below are recommended requirements for registries and address those following questions: System model **[SM-xx-yy]],** Compliance **[CM-xx-yy]** and Data accuracy **[DA-xx-yy]**. In addition, 1.a addresses Data privacy **[DP-xx-yy]**.

**1. An independently-tested, functioning Database and**

**Communications System that:**

a. Allows multiple competing registrars to have secure access (with encryption and authentication) to the database on an equal

(first-come, first-served) basis.

b. Is both robust (24 hours per day, 365 days per year) and scalable (i.e., capable of handling high volumes of entries and inquiries)

c. Has multiple high-throughput (i.e., at least T1) connections to the Internet via at least two separate Internet Service Providers.

d. Includes a daily data backup and archiving system.

e. Incorporates a record management system that maintains copies of all transactions, correspondence, and communications with registrars for at least the length of a registration contract.

f. Features a searchable, on-line database meeting the requirements of Appendix 2.

g. Provides free access to the software and customer interface that a registrar would need to register new second-level domain names.

h. An adequate number (perhaps two or three) of globally- positioned zone-file servers connected to the Internet for each TLD.

2. **Independently-reviewed Management Policies, Procedures, and Personnel including:**

1. Alternate (i.e., non-litigation) dispute resolution providing a timely and inexpensive forum for trademark-related complaints.

(These procedures should be consistent with applicable national laws and compatible with any available judicial or administrative remedies.)

b. A plan to ensure that the registry's obligations to its customers will be fulfilled in the event that the registry goes out of business. This plan must indicate how the registry would ensure that domain name holders will continue to have use of their domain name and that operation of the Internet will not be adversely affected.

c. Procedures for assuring and maintaining the expertise and experience of technical staff.

d. Commonly-accepted procedures for information systems security to prevent malicious hackers and others from disrupting operations of the registry.

3. **Independently inspected Physical Sites that feature:**

a. A backup power system including a multi-day power source.

b. A high level of security due to twenty-four-hour guards and appropriate physical safeguards against intruders.

c. A remotely-located, fully redundant and staffed twin facility with ``hot switchover'' capability in the event of a main facility failure caused by either a natural disaster (e.g., earthquake or tornado) or an accidental (fire, burst pipe) or deliberate (arson, bomb) man-made event. (This might be provided at, or jointly supported with, another registry, which would encourage compatibility of hardware and commonality of interfaces.)