Figure 23-1: Registry Services. *Each proposed service has been previously approved by ICANN to ensure registry security and stability.*

Registry Service	Description of Technical Component	Description of Business Component
A. Receipt of data from registrars concerning registrations of domain names and name servers	The Verisign-operated registry accepts registration information for domain names and name servers from registrars using the IETF EPP as defined in RFCs 3915, 5730 – 5734, and 5910. For more information about EPP please see the response to Question 25, EPP.	All registry systems under Verisign's management use EPP with no security or stability issues. Approximately 915 registrars use the Verisign EPP service, and Verisign, as a company, has handled more than 140 million EPP transactions daily without performance issues.
B. Dissemination of TLD zone files	Verisign disseminates top-level domain (TLD) zone files through its Domain Name System (DNS) resolution infrastructure, which fully complies with all IETF DNS specifications. Verisign ensures updates are processed and distributed rapidly to meet end-user needs. In addition, Verisign, as a company, provides DNS resolution services through its globally distributed constellation of resolution sites, which currently process an average of 60 billion queries per day. Question 35, DNS Service provides details of zone file dissemination.	Any TLD must have the capability to quickly and accurately distribute zone information to a set of globally distributed name servers. In Verisign's experience, end users demand rapid updates of zone information in the DNS. Verisign's system supports this capability in full compliance with applicable RFCs by updating its zone files incrementally every three minutes with a complete zone update every 12 hours.
C. Dissemination of contact and other information concerning domain name registrations (i.e., port-43 WHOIS, Wedb-based Whois, RESTful Whois service)	Verisign uses the Whois service as defined in RFC 3912 to disseminate contact and other information regarding registered data objects. Like all other components of its registry service, Verisign's Whois system is designed and built for both reliability and performance. Its 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. Verisign commits to implementing a RESTful Whois service upon finalization of agreements with the IETF. For more information about Whois, please see the response to Question 26, Whois.	The Whois service facilitates the timely resolution of many technical problems, assists investigatory phases of law enforcement, and provides many other legitimate, non-abusive uses of domain name registration meta-data. One of the fastest growing uses for Whois data today is in the automated, analytic engines of Internet reputation services used to prevent spam and combat Internet-based identity crimes such as phishing.
D. Internationalized domain names (IDNs)	At this time, ICE does not plan to offer IDNs. If it offers IDNs in the future, ICE will contact ICANN to initiate the ICANN processes required to gain the applicable approvals to offer IDN services.	
E. DNSSEC	Verisign's registry system supports the registration and resolution of DNSSEC-enabled domain names. Verisign's DNSSEC implementation provides end-to-end authenticity and integrity and helps protect the Internet from certain types of attacks, such as man-in-the-middle and cache poisoning attacks. Verisign has always worked closely with the Internet community in the development of standards and solutions related to topics of Internet security, including DNSSEC. Verisign recognizes that Internet security is constantly evolving, and DNSSEC is one of many measures that are currently underway to enhance security on the Internet. Please see the response to Question 43, DNSSEC, for details of Verisign's approach.	DNS was not originally designed with strong security mechanisms to provide integrity and authenticity of DNS data. Over the years, a number of vulnerabilities have been discovered that threaten the reliability and trustworthiness of the system. DNSSEC addresses these vulnerabilities by adding data origin authentication, data integrity verification, and authenticated denial of existence capabilities to the DNS.