1. General description of the sub-CAs operated by third parties.
These sub-CAs are operated under our GeoRoot product definition and guidelines. This product is geared toward large enterprises that operate their own certificate authority software and desire the ubiquity of a public root to issue their own client or server SSL and SMIME certificates. Enterprises are vetted to insure they meet the GeoRoot requirements for Net Worth, Errors and Omissions insurance, Certificate Practices Statement, minimum FIPS 140-2 HSM for key storage and approved CA product.

2. Selection criteria for sub-CAs
An application for GeoRoot must include Articles/Certificate of Incorporation and an incumbency certificate with a corporate seal attached. A enrolment form is completed by the customer and reviewed by the product manager to verify that each enterprise CA complies with the requirements. Each organization must maintain a CPS and Subscriber agreement which can be reviewed by Symantec. The template for such CPS is the GeoTrust CPS.

3. The CP/CPS that the sub-CAs are required to follow.
The GeoTrust CPS is at http://www.geotrust.com/resources/repository/legal/.

4. Requirements (technical and contractual) for sub-CAs in regards to whether or not sub-CAs are constrained to issue certificates only within certain domains, and whether or not sub-CAs can create their own subordinates.
Customers are contractually bound to issue certificates only to domains they own. Symantec has audit rights to insure enforcement of this rule. Sub-CAs cannot issue subordinate CAs.

5. Requirements (typically in the CP or CPS) for sub-CAs to take reasonable measures to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of our Mozilla CA certificate policy.
Sub-CA customers are contractually obligated to maintain authentication procedures that meet or exceed the requirements set forth in these sections of the GeoTrust CPS or AICPA WebTrust standards. Here's an excerpt from the GeoTrust CPS:

3.2.2 Authentication of Organization Identity
Whenever an organization name is included in the Certificate, GeoTrust or the RA will take reasonable steps to establish that a Certificate request made on behalf of that Organization is legitimate and properly authorized. GeoTrust will ensure the following:

(a) the Organizational Name appears in conjunction with a country and possibly a state or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and

(b) in the case of an Organization that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances GeoTrust will obtain, view and verify copies of the registration documents. For instance, GeoTrust may

(a) verify the validity of the registration through the authority that issued it, or

(b) verify the validity of the registration through a reputable third party database or other resource, or

(c) verify the validity of the Organization through a trusted third party, or

(d) confirm that the Organization exists if such Organization is not the type that is typically registered or is capable of being verified under clause (b).

3.2.3 Authentication of Domain Name
When a domain name is included in a Certificate together with an organization name, GeoTrust or the RA will verify that the Subscriber had the right to use the domain name submitted by the Subscriber at the time it submitted its application. For instance, GeoTrust may perform this verification by confirming that

the Subscriber is the same person or entity that holds the domain name registration from the relevant domain name registrar or that the Subscriber is otherwise authorized to use such domain name.

Domain name verification as described above is performed for **TrueBusiness ID, Enterprise SSL** and **Enterprise SSL Premium**, **RapidSSL Enterprise** and **FreeSSL Server** Certificates.

True Business ID Certificates may contain an IP address in the *CommonName* field. **RapidSSL Enterprise** Certificates may contain a private IP address in the *CommonName* field.

When a domain name is included in a Certificate without authentication of the entity owning the domain name, GeoTrust or an RA will verify that the Subscriber has control over such domain name at the time it submitted its enrolment form by accessing a third party database of domain names and their owners. To do this, GeoTrust will send an e-mail message to one of the following 7

e-mail addresses requesting confirmation of the Certificate order and authorization to issue the Certificate in the domain name:

(a) an e-mail address listed as the administrative or technical contact for the domain name in an official InterNIC domain name registry that includes the domain name,
(b) a limited list of the most commonly used generic e-mail addresses for authorized persons at domain names (e.g., "*admin@domain.com*," or "*hostmaster@domain.com*" for the domain name domain.com), or
(c) using a manual process of verification conducted by GeoTrust, to an e-mail address identified as the registered owner of the domain per the *whois* database. Optionally, a verification phone call may be substituted to the domain owner phone number listed in the *whois*.

Upon receipt of a confirming e-mail message authorizing issuance of the Certificate, GeoTrust will issue the Certificate as described below. Additionally, a confirmatory phone call to the applicant may be performed for Domain Control Certificate applications.

6. Description of audit requirements for sub-CAs (typically in the CP or CPS)
   - Whether or not the root CA audit includes the sub-CAs. All current contracts with SubCA customers stipulate that Symantec has the right to require an audit.
   - Who can perform the audits for sub-CAs. Audits will be performed by a Qualified Auditor that meets all the requirements set forth in Section 17.6 of the CA/Browser Forum Baseline Requirements.
   - Frequency of the audits for sub-CAs. Audits must be performed on a yearly basis.