Requirements/ Scope of Work for Web Application VA Testing

1. The system involved in the web application VA testing is limited to external facing portal/website(s) of the information processing system used to handle domain name registration and related activities, such as request for modifications to domain name registrations, including renewals and transfer of domain name registration, changes of registrar, updates to information and other requests submitted by the registrants.

2. The vendor shall conduct the web application VA test on the website URL specified by the client/registrar.

3. The vendor shall scan for vulnerabilities including but not limited to:

   3.1. Weak SSL/TLS ciphers & protocols used by the web application;
   3.2. Cross-Site Scripting (XSS);
   3.3. Cross-Site Request Forgery (CSRF);
   3.4. SQL Injections;
   3.5. Insecure configurations (e.g. not setting Secure and HTTP Only flags in the cookie); and
   3.6. Click-Jacking.

4. The vendor shall ensure that the tools used for the web application VA test(s) and the activities carried out do not affect the client/registrar's business operations.

5. The vendor shall assess all vulnerabilities found (minus false positives) and shall submit and present the deliverables listed below to the client/registrar.

   a) Executive / Management Summary Report summarizing the security status of the system,
   b) Technical Report highlighting the list of vulnerabilities with:
      i. Severity of the vulnerability (High, Medium or Low);
      ii. Description of the vulnerability;
      iii. Potential impact;
      iv. Affected areas;
      v. Reference to the vulnerability or exploit (i.e. CVE reports);
      vi. Ease of exploitation; and
      vii. Recommendation on how to remediate the vulnerability.

6. The vendor shall perform one post/follow-up web application VA test review to verify that the web application VA test findings have been remediated, and provide the final web application VA test report to the client/registrar, prior to ending the engagement.

The following are recommended requirements that a registrar may consider when the registrar requests for proposals and quotations from pre-screened VA security vendors.

Recommended Web Application Vulnerability Assessment (VA) Requirements

1) The vendor shall propose a detailed and comprehensive methodology(s) on how the web application VA tests will be conducted.

2) The vendor shall provision and use a reputable web application VA test scanner (e.g. in Gartner Leader's Quadrant) to perform automated scanning. The test scanner shall have deep and high accuracy in its vulnerability scanning with low false positives being reported, and it shall be configurable to fine tune the scanning of vulnerabilities.

3) The vendor shall ensure that the web application VA test scanner is updated with the latest vulnerability signatures, and shall not be more than one (1) month old. The test scanner shall also be able to identify all known web application security vulnerabilities.

4) The vendor shall provide details of the qualifications of their personnel to the client/registrar, including information/evidence of the following professional certificates: Certified Information Systems Security Professional (CISSP), OSSTMM Professional Security Tester (OPST), EC-Council Certified Security Analyst (ECSA), CREST Registered Penetration Tester (CRPT). Certification numbers, if available, should also be provided.

5) The vendor shall provide evidence showing that the personnel that will be involved in the web application VA test(s) each have a minimum of 3-5 years of experience in performing web application VA testing or in any other related field.

6) The vendor shall provide detailed track records, including customer feedback, if any, of at least 3 similar web application VA test projects undertaken by them in the past.