WEB APPLICATION VULNERABILITY ASSESSMENT ("VA")
PRE-SCREENED SECURITY VENDOR

APPLICATION FORM

General information:

1. Please complete the application form fully and provide all necessary supporting documents. Applications and the accompanying supporting documents should be in PDF format and submitted to securityprogramme@sgnic.sg.

2. All applications and supporting documents should be in English. Any translations, if so requested by SGNIC, must be provided to SGNIC at the Applicant's own expense.

3. All applications are subject to SGNIC's approval.

Supporting documents required as part of the application:

1. Please propose detailed and comprehensive methodology(s) of how you intend to deliver the web application VA service according to the scope of work detailed in Annex.

2. Please provide details of the web application VA scanner(s) to be used to perform automated scanning. The scanner shall have deep and high accuracy in its vulnerability scanning with low false positives being reported, and shall be configurable to fine tune the vulnerability scanning.

3. Please provide evidence that the VA scanner shall be updated with the latest vulnerability signatures, and that it shall not be more than one (1) month old. Examples of such evidence could be screenshots showing the date of vulnerability signatures and/or the scanner engine version.

4. Please provide details to demonstrate that the scanner is able to identify all known web application security vulnerabilities.

5. Please provide the professional qualifications of your personnel such as 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 be provided.

6. Please provide details to demonstrate that your personnel have at least 3-5 years of experience in performing VA or any relevant field.

7. Please provide detailed track records, including customer feedback if any, of at least 3 past similar VA projects undertaken by your company.

APPLICATION DETAILS	
Name of Applicant (Company Name)	
Name, email and phone number of Applicant's contact person	
Business Registration Number	
Country of Business Incorporation	
Email Contact for web application VA service	

If your request is approved by SGNIC, you will be deemed an 'SGNIC pre-screened security vendor' and may assist SGNIC's registrars to perform web application VA. Additionally, SGNIC intends to list your company in the 'SGNIC Pre-screened Security Vendor' list (**List**) which SGNIC will publish online as a guide to SGNIC registrars who may need assistance to select a vendor for VA services.

If you wish to Opt OUT of the List, please tick (✔) here: ☐

Declaration by Applicant's Authorised Representative:

1. The Applicant declares that the information provided by it in this application form and the accompanying documents are true and accurate.

2. The Applicant acknowledges and agrees that SGNIC shall have the sole and absolute discretion to accept or reject the application made, without being liable or obliged to provide any reason thereof.

3. SGNIC's approval to accept the Applicant as a SGNIC pre-screened security vendor does not constitute or represent any form of endorsement by SGNIC of the Applicant's services and work. The Applicant undertakes not to represent in any way to any person that the Applicant is endorsed by SGNIC in any way.

4. SGNIC may remove the Applicant as a pre-screened IT security vendor at any time and at the sole discretion of SGNIC. The Applicant may also write to SGNIC to remove the Applicant as a pre-screened security vendor and/or from the List.

5. SGNIC may periodically require the Applicant to resubmit the Application with updated information for reassessment.

6. The Applicant understands if any SGNIC registrar decides to engage the Applicant, the registrar shall be the party to negotiate the price and work with the Applicant.

7. SGNIC assumes no responsibility or liability for the pricing, schedule, quality of the work or services arising from the Applicant's engagement with the registrar, and the Applicant will indemnify and keep SGNIC indemnified against, and hold SGNIC harmless from, any and all loss, damage, claim or expense (including legal expenses).

Name of Applicant's Authorised Representative

Designation of Authorised Representative

Signed for and on behalf of

_____

Signature and Date

Applicant's Company Stamp (if applicable)

Requirements/ Scope of Work for Web Application VA Testing

1. The system involved in this web application VA should be limited to the 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 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.

   5.1 Executive / Management Summary Report summarizing the security status of the system
   5.2 Technical Report highlighting the list of vulnerabilities with:
      i. Severity of the vulnerability (High, Medium, 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 remedied, and provide the final web application VA test report to the client/registrar, prior to ending the engagement.