RFP Application Security Assessment and Analysis Services
Q & **A** **#3**
September 17, 2020

1. Section II.C.2.a. Security Assessment:
    a. Total no of Application in scope=24
    b. Lines of code for each Application in scope=N/A
    c. Apart from Source Code Review what other activities in scope? Salesforce Community Navigation
    d. VA or PT of the Application VA and PT
    e. if VA/PT is also part of scope kindly provide below details.
    f. No of dynamic Page=~2000
    g. user role=~50
    h. API=~7
    i. External IP=~20
    j. Internal IP=~20

2. Section II.C.2.b. Application Analysis and Testing:
    a. No of Application for Source code Review=21
    b. Count of databases in scope=20

3. Section II.C.2.c. Penetration Testing:
    a. No of Application in scope =21
    b. No of databases in scope=19
    c. No of Systems/IP in scope=16 (including Cloud Based)
    d. No of Application for Source code Review along with Lines of code in Application=21
    e. No of Mobile application in scope N/A
    f. Please share below details N/A
    g. Platform of App(Android/iOS)
    h. no of screen=
    i. user roles to test=
    j. API with methods=

4. Section II.C.2.c. Penetration Testing, Point no ii: Conduct external and internal penetration testing to exploit the vulnerabilities in the Bar's system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.
    a. Kindly share the bifurcation of External & Internal system/IP/Application in scope 8 internal; 7 external

5. Misc
    a. Which applications, databases, and assets reside in the cloud? From the list of applications provided in the RFP, about 20% of those applications reside in the cloud.
    b. Is remediation support for penetration testing in scope for this RFP? Yes
    c. Would you like a separate cybersecurity assessment / gap analysis to cover the following tasks outside of a standard application penetration assessment? If so, would you want this priced as a mandatory or an optional piece of the work?

i. Review current application implementation (i.e. release management) procedures and provide recommendations. Yes, please include.
ii. Identify, collect, and review existing IT security policies, guidelines, standards, practices, processes, and procedures. Yes, please include.
iii. Analyze the security assessment findings and prepare documentation to provide a detailed analysis of the desired security posture in relation to industry best practices and provide a prioritized action plan. Yes, please include.
iv. Timelines and sequencing of tactical and strategic next steps. Yes, please include.

d. What does "UC" mean in "UC Assets"? UC = Unified Communications.
e. Is section III,B,4 a hard requirement or "nice to have"? Nice to have.

6. Internal Penetration Assessment (internal assets)
   a. What is the environment's name? Calsb.org, Calsbdmz.org
   b. What is the environment's function? Those are the two primary domains, Intranet and public server domains.
   c. What business risks are associated with the environment? For the DMZ domain the risks are from external attacks and hackers. For the Intranet, risks are from internal resources and external resources trying to penetrate via remote connection.
   d. What would be the worst-case outcome of an attack or breach? There are many risks associated with such attacks, one primary one is the security of our attorneys' information.
   e. What is the goal of the assessment? Ensuring that our applications and environment are secure and follow security industry (OWASP) protocols and best practices.
   f. Would you like us to include any specific attack scenarios during the assessment? Yes, SQL injections, cross site scripting, encryption.
   g. Roughly, how many live internal hosts are expected to be assessed? Roughly 25.
   h. How will the environment be accessed? (Remotely via an NTT jump box, Remotely via VPN) Remotely via VPN (but open for discussing other options).
   i. Please provide additional information, comments, or known issues.
   j. What are the database names and types in scope? Will be discussed during "discovery phase" of the project.

7. External Penetration Assessment (Internet facing assets) See above for all questions in this section, unless answered below.
   a. What is the environment's name?
   b. What is the environment's function?
   c. What business risks are associated with the environment?
   d. What would be the worst-case outcome of an attack or breach?
   e. What is the goal of the assessment? (Typically, this is to penetrate the external perimeter and gain access to internal assets)
   f. Would you like us to include any specific attack scenarios during the assessment?
   g. What external domains and/or networks will be in scope? (Include all known DNS domains and network ranges)
   h. Roughly, how many external live hosts are expected to be assesed?
   i. Roughly, how many web applications are expected?
   j. What is the number of web apps that may be encountered (unauthenticated). Will be discussed during "discovery phase" of the project.

k. Are any web applications (authenticated) are included in the scope. Yes.
l. Please provide additional information, comments, or known issues.

8. Application Penetration Assessment
    a. What are the application names? Listed in RFP section II.1.
    b. What are the application URLs? Will be discussed during "discovery phase" of the project.
    c. Brief description / overview of the application(s)? Will be discussed during "discovery phase" of the project
    d. What business risks are associated with the environment? Answered above.
    e. What would be the worst-case outcome of an attack or breach? Answered above.
    f. Would you like us to include any specific attack scenarios during the assessment? Answered above.
    g. How will each application be accessed (e.g. Remotely via VPN)? Answered above.
    h. What platforms will be tested? (e.g., Web, Mobile (Device and API), API (Machine consumer), Thick client, Thick client (Citrix hosted) All but Citrix Hosted.
    i. What application environments are in scope (e.g. production, development)? Production.
    j. What is the Authentication type for each application (e.g. one time password, form, Certificate, Multi-factor (form/token))? Forms authentication, tokens, multi-factor, AD).
    k. Roughly, how many unique forms are offered by each application? Will be discussed during "discovery phase" of the project.
    l. If machine-consumed APIs are in scope, how many functions will be tested by each application? Will be discussed during "discovery phase" of the project.
    m. If machine-consumed APIs are in scope, are any of the APIs documented? Yes.
    n. If machine-consumed APIs are in scope, will sample requests be made available? Will be discussed during "discovery phase" of the project.
    o. Which applications are web apps and which are mobile? If they are mobile, what platform do they operate on? All Web, no mobile apps.

9. What API documentation standard (if any) is currently being used? (e.g. Swagger, OpenAPI 3.0) For internally developed APIs, Swagger.

10. What are your security requirements around continuous testing with a vulnerability management solution? Will be discussed during "discovery phase" of the project.

11. What is your typical release cadence with development activity (e.g. monthly or weekly sprints?)? Bi-weekly sprints.

12. How is security currently being embedded throughout development activity? Will be discussed during "discovery phase" of the project.

13. What is the average time for vulnerability remediation? Varies, depending on system.

14. How are remediation efforts currently being tracked? Jira.

15. Beyond (Dynamic Application Security Testing) DAST efforts, what are future goals for implementing security controls on future releases? Will be discussed during “discovery phase” of the project.

16. Mobile device security testing is mentioned in the RFP. Can you please describe in detail what is desired? This refers to testing applications that have responsive design, that are accessed from mobile devices.

17. What approach should be taken to identify targets?
    a. Black Box – Targets and goals are identified by NTT Security. Prefer this approach, and work with vendor to confirm results.
    b. Grey Box – Targets and goals are provided