Q1. How many external IPs are in scope for the pen test?

A. 1

Q2. How many departments are the agency?

A. 6 departments

Q3. How many employees total?

A. Less than 30 employees

Q4. How many systems are in scope for the penetration test?

A. Less than 80 total assets (IP phones, servers, routers, firewalls, systems, etc.)

Q5. Will all testing be unauthenticated or is testing required using credentials?

A. Credentialed

Q6. Has SVCE had a similar IT Security Audit conducted in the past? If so,

1) Who conducted it? 2018 – Teamlogic IT, 2019 – GreyCastle
2) How long ago was it conducted? Annually, last year
3) May we receive a copy of the report? Yes
4) What were the fees and hours expended for the most recent IT Security Audit? Fees were based on submittal, not based on hours.

Q7. Is all of IT centralized at a single location or is IT decentralized and managed partly by in-house IT staff and partly by a third-party?

A. IT is centralized in house. One contractor is used for some server maintenance.

Q8. How many Environments does SVCE have? An Environment is defined as a single location housing people and/or technology used by the agency. Thus, a building for sales or customer satisfaction representatives is probably a separate environment from the HQ building, which could be a separate environment from the data center(s), or cloud implementation(s), or places where developers write code for the website(s).

A. SVCE has one physical location; all staff is located in one office.

Q9. There appears to be overlap between the two RFPs. A substantial portion of both RFPs can be addressed through a detailed or "deep dive" CIS Top 20 Critical Security Controls assessment. Would SVCE be amenable to us submitting a combined proposal for the two

RFP's to identify a common policy, procedure, security control baseline and address the other individual requirements in the two RFP's separately?

A. SVCE would be willing to accept one proposal for both RFP'S if all requirements in the SOW are met. SVCE issued two separate RFP's as we aware that not all submitters will have the ability to address all of the requirements specified in both of the RFP'.s

Q10. Will SVCE make available an Inventory of computing assets, a network topology diagram and data flow diagram(s)?

A. SVCE will make available an inventory list of assets as well as a network topology diagram.

Q11. Enumerate different operating system versions deployed (E.g. RedHat 6.4, 6.5, Windows 8.1, Windows 10, Windows Server 2016, Windows Server 2019 are all separate evaluations).

A. Windows 10, Server 2016r2, EXSI

Q12. Number of locations in which computing assets exist

A. 1 location

Q13. Number of subnets involved in the SVCE's operations?

A. 1

Q14. Name the different existing cloud deployments (e.g. AWS, GCP, Azure, Rackspace each have to be evaluated separately)

A. none

Q15. Name the different types of web servers deployed (e.g. IIS, Nginx, Apache)

A. none

Q16. For the internal network penetration test and vulnerability assessment, how many target systems will be in scope?

A. Less than 80 total assets (IP phones, servers, routers, firewalls, systems, etc.) ~40 systems

Q17. Does a formal asset inventory and data classification scheme exist today?

A. In this context: no

Q18. What Policies are in scope? And, can you provide the name of the in scope policies and total number to be assessed?

A. SVCE currently has 15 Board approved policies (see below)

ITP 01_Information Systems Use Policy (F) ITP 02_E-mail Use Policy (F)

ITP 03_IT Asset Management Policy (F)

ITP 04_Internet Usage Policy (F)

ITP 05_IT Security Plan Policy (F)

ITP 06_Access Control Policy (F)

ITP 07_Password Protection Policy (F)

ITP 08_Malware Defense Policy (F)

ITP 09_Security Audit Policy (F)

ITP 10_Disaster Recovery Policy (F)

ITP 11_Threat-Risk Assessment Policy (F)

ITP 12_IT Satisfaction Policy (F)

ITP 13_Data Breach Policy (F)

ITP 14_Workstation Security for HIPPA Policy (F)

ITP 15_Clean Desk Policy (F)

Q19. In regards to policies, are you looking for revisions as part of this engagement or general recommendations?

A. Revisions, reductions additions. Would like to mature SVCE and tie to an agreed upon framework.

Q20. The RFP references California Public Utilities Commission D.12-08-045. As such, does SVCE want the vendor to assess the privacy practices against California Public Utilities Commission D.12-08-045 customer privacy requirements?

A. This was included as an FYI as this decision drives much of SVCE policies and direction. Wanted submitters to be aware of what the decision entails.

Q 21. Can SVCE elaborate on the expectations to distinguish what a standard penetration test covers versus a basic penetration test versus an advance persistent penetration test? (What are the expected goals of each type of test?)

A. SVCE is seeking a Penetration test that is based on the globally recognized NIST SP-800 115 and other established standards for information security testing. Test should include identified weaknesses, vulnerabilities and exploits in SVCE's information systems, networks, applications and facilities identified in the testing scope.

Should include:

Internal Network testing

Wireless Network Testing

Physical Testing

Social Engineering

Sample tools to use:

Google – Google hacking, target research and reconnaissance
NMAP – Network mapping, custom packet configuration, vulnerability discovery
PeepingTom - Webserver screenshot utility
Alpha - Proprietary backdoor and remote administration tool
theHarvester – Recon and intelligence gathering tool
Nessus – Vulnerability scanning
FIERCE – DNS mapping and mapping
Foca – Metadata extraction tool
Maltego – Data mining
MetaSploit – Target scanning, IPS obfuscator, exploit engine
The Social Engineering Toolkit (SET) – Penetration testing and Social-Engineering tool

Q22. For the external web application penetration test, how many web application servers will be in scope?

A. none

Q23. For the web application penetration test, does SVCE require authenticated/credentialed vulnerability assessment scans?

A. N/A

Q24. For the internal network penetration test and vulnerability assessment, does SVCE require the entire population of workstations/laptops to be in scope or just a sample? Please provide the number of workstations/laptops or sample number expected.

A. Less than 80 total assets (IP phones, servers, routers, firewalls, systems, etc.)

Q25. For the firewall assessment, are you looking for a rules assessment or including it as part of the external test?

A. It can be included as part of external test.

Q26. Approximately how many IT policies and procedural documents would need to be reviewed?

A. 15 current approved policies

Q27. For the external network penetration test and vulnerability assessment, how many target systems will be in scope?

A. One public facing IP

Q28. For the APT testing, is SVCE looking to use the firewall AAT&CK framework to simulate the APTs? If so, will we have access to an internal system to deploy software on?

A. SVCE is not tied to a specific framework, however SVCE can provide an internal system to deploy software on.

Q29. Can SVCE provide details on what its critical business process / assets are?

A. Yes

Q30. How many applications are in scope?

A. Nothing specific

Q31. How many IT staff (FTE) are there at SVCE? Can you please list out the title/position and the number for each?

A. 1 FTE – Management Analyst

Q32. In addition to IT staff, how many business unit interviews should we anticipate conducting?

A. SVCE has 6 departments, not sure if interviews for each is needed, up for discussion.

Q33. Does SVCE utilize outsourced IT support to provide management and administration of any aspect of the IT environment and operations? If yes, could you please list the functions that are managed outside of internal IT?

A. SVCE currently has 1 vendor that manages the server. SVCE is contracted for several cloud based (email, data, MDR, RMM, ETC) vendors for additional tools.

Q34. SVCE listed Compliance as an in-scope area. Could you please provide the industry or government regulations with which SVCE needs to comply? (e.g., NERC CIP, FTC Red Flags, PCI DSS, etc.)

A. Currently SVCE only has to stay in compliance with California Public Utilities Commission D.12-08-045. SVCE would like to work towards compliance to industry standards.

Q35. Given the industry and government regulations that require compliance, does SVCE require the vendor to gauge the organization's compliance with ALL of the regulations to which it is subject?

A. See answer to question 34

Q36. Does SVCE require the IT Security Audit to primarily gauge SVCE's alignment with the CIS Security Top 20 CSC? In other words, should we use the CIS Security Top 20 CSC as the best practice framework in order to assess and audit IT and security-related policies and procedures, disaster recovery measures and planning, compliance activities, risk management, risk mitigation practices, and asset protection?

A. Yes, that is what the previous IT audits used to measure. Open to newer more robust methods if presented.

Q37. Does SVCE require a formal presentation toward the end of the engagement to executive management and/or the Board of Directors? In total, how many formal presentations (of our findings and recommendations) should we anticipate?

A. One short presentation to the audit committee and management will be required.

Q38. Does SVCE desire, or claim, to adhere to any specific security standard(s)? When performing the assessment what standard(s) should we use to measure any compliance gaps against?

A. SVCE desires to adhere to a specific security standard. Guidance through the Focused Security Assessment will be appreciated.

Q39. Total number of web pages or forms displayable from the websites

A. Website is hosted through offsite hosting company.

Q40. Name the different databases used (e.g. Oracle, MySQL, Redis)

A. none

Q41. Number of locations from which code and/or systems development is performed?

A. One

Q42. Different programming languages used (e.g. iOS, Android, Javascript, Ruby, perl, MySQL)?

A. MySQL, ARCGIS

Q43. Number of roles/perspectives to be tested for (e.g. staff-user, consumer-user, manager, admin, super-admin, database administrator)?

A. staff-user, admin

Q44. What is the scope of the Enterprise Environment?

A. Need more information from you to answer this question.

Q45. What is the scope of the Security Management Practices?

A. Need more information from you to answer this question.

Q46. Will a "trophy" be provided for the external test or will some other objective be provided for the exploitation attempts?

A. Need more information from you to answer this question.

Q47. Can SVCE provide details on what its critical business process / assets are?

A. yes

Q48. To help us prepare a proposal and design a project approach that best meets SVCE's needs, what is SVCE's cost estimate for the requested services?

A. All competitive submittals will be reviewed. Final selection will be based on submittals meeting the criteria listed in the RFP along with price.

Q49. Is it expected that the vendor covers administrative security controls such as employee onboarding/offboarding, system change management procedures, security awareness training, self-auditing practices, IT security governance, and similar non-technical controls?

A. Yes

Q50. SVCE-RFP-IT-Audit-2020 has penetration testing and vulnerability assessment as part of its SOW. Is it expected that the IT Security Audit will cover more technical infrastructure security controls; whereas, the Focused Security Assessment is expected to cover more administrative security controls? (We're trying to understand the differences in the SOWs in the RFPs from SVCE's perspective.)

A. I think your questions describes our vision for the two RFP's.

Q51. There appears to be a lot of overlap in the SOW between the IT Security Audit RFP and the Focused Security Assessment RFP. For example, the IT Security Audit RFP lists Compliance, Risk Management, Risk Mitigation, and Security Policy – all of which are natural areas of review under Assess the Security Management Practices in the Focused Security Assessment RFP. Is SVCE expecting a considerable distinction between these assessment areas in approaching the review from an IT Security Audit versus Focused Security Assessment perspective?

A. SVCE's past two audits were limited in their assessments. We had some areas of concern that were not audited. Other companies may have a more comprehensive audit package that may cover both the audit and assessment. SVCE will look at that as well.

Q52. In SVCE-RFP-IT-Audit-2020 RFP, the scope of work lists the CIS Security Top 20 Critical Security Controls yet the Focused Security Assessment lists NIST and Cybersecurity Framework (assuming this refers to the NIST Cybersecurity Framework) as a review area. Which of these two frameworks does SVCE wish to be gauged against if that is indeed the intent?

A. SVCE past two auditors used the CIS Security Top 20 Critical Security Controls. SVCE is open to other alternatives.