Vulnerability Assessment and Penetration Testing

RFP FY22-SCIT-01

Addendum #2

Issued October 13, 2021

1) General: Is there a defined budget for this project?
   Yes, but it is not set as of now.

2) General: Pen testing – how many vulnerabilities should we attempt to exploit?
   As many as time allows for as long as it does not impact other duties. Also, vulnerabilities do not necessarily have to be exploited if there is already a know CVE that can be referenced.

3) Section IV.A.4: # of wireless physical sites for scanning?
   Two.

4) Section IV.A.4: # of SSID's for scanning?
   Four.

5) Section IV.A.5: # of web applications to test? It shows 3, plus "custom public web applications," but not how many.
   Two (2) web applications.

6) Section IV.A.6: # of users to include for:
   a. Phishing tests. Fifty.
   b. Phone Impersonation tests. Ten.
   c. On site physical test? Ten.

7) Are there any socio-economic preference points allocated to small businesses, disadvantaged small businesses, economically disadvantage women-owned small businesses (EDWOSB), women-owned small businesses (WOSB), and/or minority owned small businesses? [Application RFP Section: N/A]
   Sandoval County adheres to the New Mexico Procurement Code, which recognizes New Mexico Resident Business Preferences and New Mexico Resident Veteran Business Preferences (NMSA 1978 13-1-21).

8) Is this the first time that you will contract a vendor for the services in question? If not, then would a copy of the final contract and amount of the previous successful vendor be available? [Applicable RFP Section: N/A]
   No, public records may be accessed at: https://www.sandovalcountynm.gov/public-records-request/

9) Given the COVID-19 pandemic, can work be performed remotely to the maximum possible extent? [Applicable RFP Section: N/A]
Yes.

10) Please provide the number of locations to be included in the wireless network penetration test? Can sampling be used? [Applicable RFP Section: IV.A.7]
One.

11) Please provide the number and types of social engineering scenario tests that you would like us to perform. [Applicable RFP Section: IV.A.7]
Two. Phishing, and impersonation either in person or over the phone.

12) Please provide a high-level idea of the size and scope of the technical infrastructure that we would encounter. [Applicable RFP Section: IV.A]
Firewalls, collapsed core, access layer switches and access points.

13) How many URLs are present for each Web application?
Two.

14) For any Web applications using APIs, how many APIs will be tested for each?
Two external API to be tested.

15) Will wireless testing focus on any bands outside 2.4GHz/5GHz?
No.

16) Are "Mission-critical" applications to be tested included in Web application scoping, or are these separate systems?
Both, there are some mission-critical applications that are web applications and there are other mission-critical applications that are not web based.

17) Should social engineering efforts consist of both broad and focused attacks (e.g. organization-wide phishing and vishing/whaling/etc. for key individuals)?
Yes.

18) What will be the frequency of testing for Penetration Testing i.e., Weekly/Monthly/Quarterly/Annual?
Annual, with the option to allow continuous monitoring performed by a device.

19) What will be the number of emails for the Social Engineering Vulnerability Assessment and Penetration testing?
Fifty.

20) How many Internal IP addresses ae to be scanned and how many devices are in scope?

1500. No devices are outside of the scope as long as the scanning does not disrupt services or severely impact performance.

21) How many WiFi SSID's, Access Points and Controllers, and locations are in scope? Is sampling permitted, and if so how many locations would you like to be included in the scope?
SSID's: four. Testing can be done through two (2) access points. There are no controllers. Two locations. Sampling is allowed, two locations.

22) How many users do you have in total, and how many would you like targeted in social engineering?
500. Ten to fifty depending on the type of attack; fifty if it is a phishing attack, ten if it is an in person/over the phone impersonation.

23) Do you have a preferred timeline for completing the services?
Completed by March 2022.

24) How many locations are in scope for wireless testing? What is the approximate distance between locations?
Two locations, 500 feet.

25) IV.A.5: Application Vulnerability Assessment and Penetration Testing
    a. How many Custom Web Applications are in scope for testing? Two.
    b. Is code review in scope? If yes, what language and how many lines of code? No.
    c. How many live web pages are in scope for testing on each application? Five.
    d. How many web forms (pages) that require user interaction are present on each application? Two.
    e. What is the number and type of user roles? Two: admin and user.
    f. If web services are to be tested, how many endpoints are in scope (i.e., the number of parameters per method)? Five.

26) Would you consider accepting email or electronic submissions in lieu of the hardcopy submissions as required in Section III Response Format and Organization of the RFP?
Sandoval County is only accepting hard copies as indicated in Section III at this time.

27) Page 20. Do you need separate reports for technical, vulnerability, and executive reports, or many they be different sections in one larger report?
They can be different sections in one larger report.

28) How many Internet facing hosts comprise the internal and external environment (servers, routers, firewalls, IDS/IPS)?
    a. Servers – what is their purpose (mail, web, etc.)?
    Ten. Mail and web applications.
    b. How many firewalls? (Would you like a configuration review)?
    Two (it's an HA pair). Yes.

c. IDS/IPS – do you utilize one and if so, is it locally managed?
One, it is locally managed.
d. How many Internet facing sites/applications (URLs) are included? Ten.

29) How many databases are to be examined in the Finance, Health, Sheriff, Human Resources, and Detention Center areas?
Six.

30) How large is each of the in-scope databases?
500MB – 1TB

31) Page 13, Section 2.A. Do you want one flash drive with Technical and Cost proposals on it or do you want them to be on separate flash drives?
One flash drive is sufficient.

32) Page 6, Item 7.B. Will you accept a redacted copy of our proposal?
Sandoval County is not accepting redacted proposals at this time.

33) Page 13, Section 3. In reference to the required tabs in the Technical Proposal, are we to insert tabs for items A-F and sub-items 1-9 as well, or will it be acceptable to only provide tabs for items A-F?
Please provide tabs for the sub-items 1-9 as well.

34) Internal Infrastructure & Wireless
a. Is the network segmented or flat? Segmented.
i. Can all networks/VLANs in scope be accessed from one network point? Yes.
ii. Number of networks/VLANs in scope? Thirty Class C networks.
b. Per network segment:
i. Number of workstations? 600 total.
ii. Number of servers? 120 total.
iii. Which operating systems are in use?
Win 7 and Win 10, and server OS 2003-2016
c. Is there any Wireless capability?
i. Is the solution centrally configured? Yes.
ii. Number of Access Points? 100.
iii. Number of SSIDs broadcasted? Four.
iv. Are 2.4GHz, 5GHz or both frequently broadcasted? Both.
v. What types of authentication are in use, if any?
Multiple: WPA2, AD authentication, MAC filtering.
d. Where is geographical location of the internal environment? Inside Sandoval County.
i. If there are multiple sites, where are the location for each?
Bernalillo, NM and Rio Rancho, NM. Albuquerque, NM for colocation.
ii. Call all locations be accessed from one main site? Yes.

35) Email/OWA
    a. Is authenticated testing also required? Yes.

36) Helpdesk Portal
    a. How will the application be accessed? Browser.
    b. A brief summary on what the application is used for. IT ticketing and assets, solutions database.
    c. What functionality exists before login, and approximate number of pages (e.g. login, register, forgotten password)? None.
    d. What functionality exists after login, and approximate number of pages (e.g. instant message/chat, email system, log a ticket, review a ticket/status)? Depends upon role.
    e. Please list the user roles that are in scope and what additional functionality can they access? Admin, user, technician. Admin can access additional applications settings, asset and user features and configurations for the application. Technician can access additional settings and features for users and assets.

37) Beyond Trust
    a. How will the application be accessed? Browser and software application.
    b. A brief summary on what the application is used for. Remote Support.
    c. What functionality exists before login, and approximate number of pages (e.g. login, register, forgotten password)? None.
    d. What functionality exists after login, and approximate number of pages (e.g. add users, change user permissions, unlock users)? Depends upon role.
    e. Please list the user roles that are in scope and what additional functionality can they access? Admin, technician, special access roles. Access roles are limited to specific devices and credentials. Technician can access pinned devices with proper credentials and host and control user machines with user approval. Admin has full device and configuration access.

38) Custom Web Application. For each application:
    a. The URL/IP address if publically accessible:
       https://eaweb.sandovalcountynm.gov
       https://etweb.sandovalcountynm.gov
        i. If not, how are the applications accessed? N/A
    b. A brief summary on what the application is used for. Access public records for assessor and treasurer.
    c. What functionality exists before login, and approximate number of pages (e.g. login, register, forgotten password)? Public lookup access for account information.
    d. What functionality exists after login, and approximate number of pages (e.g. add to basket, payment, write blog post, account management – change password)? No login.
    e. Howe many user roles are there and what additional functionality can they access? N/A

39) Social Engineering
    a. Total number of employees in the organization? 500.

b. Approximate number of employees to be targeted? Ten to fifty, depending on the type of attack.

40) Please advise as to how many internal hosts are there? 500.

41) Please advise as to the number of external networks? Fourteen public IPs.

42) Will this engagement require any phishing? Yes.

43) Reference Section III Response Format and Organization, 3. Proposal Format, 1 Technical Proposal items D and E: These Items refer to Contract Terms and Conditions, however a sample contract was not provided in the bid package. Could you provide that as soon as possible so we can get it through our review process?
Section II.C. lists the terms and conditions that will be utilized in a contract.