IMRF RFP – Information Technology Security Auditing Services

Questions and Answers

What are the number of internal and external IP addresses, and how many devices are there in those networks?

IMRF Response: Approximately 1000 to 1500 IP addresses.

Do you want web application testing to be unauthenticated or authenticated roles (If so, how many roles)? How many pages are involved in each of the three websites (roughly to see how big your site is)?

IMRF Response: We would like to consider that type of testing based on the rules of engagement and minimal impact to system(s) performance and availability. Please include a separate cost for such activities so cost and value can be evaluated and considered prior to start of engagement.

Do you have a budget for the application security portion of this project, very rough budget because it will help us determine how much we can do with your applications?

IMRF Response: Funds have been budgeted for 2023, but amount cannot be disclosed.

How many users do you want social engineering with advanced phishing testing?

IMRF Response: Under 300 users.

Have you done like assessments in the past 2-3 years? If so, who were the vendors of choice that performed assessments?

IMRF Response: Yes, assessments have been performed in that past 2-3 years. To obtain information on IMRF contracts, a FOIA request must be submitted.

Can you describe what risks your trying to evaluate with this statement: “Validate the protection mechanisms in place with the use of sanctioned outbound communication.” It sounds like you are interested in testing egress filtering controls, but could you expand on the goals and objectives you have in mind with this testing?

IMRF Response: We have authorized outbound flows through our main perimeter firewall. We want to validate that current controls in place are sufficient to minimize the exfiltration of data and/or block any outbound requests that may initiate any command and control for system compromise.

Can you describe what risks your trying to evaluate with this statement: “Attempt to install or alter software on target systems.” Are you wanting us to determine if we can utilize hacker tools within the environment, or are there particular applications you want us to “alter” in your environment?

IMRF Response: We want to validate that through the use of the vendor’s hacker tool kit that IMRF systems cannot be compromised based on current or unforeseen vulnerabilities and/or based on errant configurations deployed.

Regarding wireless infrastructure – how many different wireless networks are in use and what is their business purpose (internal/corporate, guest, etc.)?

IMRF Response: Staff and visitors.

During our External Penetration Test, we will evaluate the security posture of your web applications from an external, unauthenticated perspective. If you desire a deep dive Web Application Penetration Test where you provide credentials for us to login and evaluate the security of the entire app, then we need the following information for each in-scope web application. This can also be assessed in future assessments if you do not want that included this year.

IMRF Response: Major benefit of performing the authenticated scans is that it will validate whether internal vendor is performing their level of due diligence from a vulnerability and secure code practice. The output from this activity should align/compare with the reports received from said vendor.

On page 5, your RFP states we can request prior years' audit reports – can you provide that to us?

IMRF Response: Upon further review, IMRF cannot release prior years' reports. Reference addendum issued April 28, 2023.

The RFP states between 500-1000 IPs for the internal test. Do you have an exact number, or would you like a quote for 500, 1000, or 500 and 1000?

IMRF Response: Reference response to Question 1 above.

For the External test would you like the 8 live IPs quoted, or did you want all 24 that was stated in the call?

IMRF Response: Ten live IP's.

For the Web App Vulnerability, you only have the 3 unauthenticated URLs, correct?

IMRF Response: Yes, three unauthenticated URL's.

The RFP also state wireless testing. How many SSID's would you like tested?

IMRF Response: Three. Guest, visitor & staff.

You also mentioned a phishing exercise. How many users do you have and how many would you like tested in this exercise?

IMRF Response: Reference response to Question 5 above.

We offer a retest within 6 months to confirm any remediation you have done at a discounted price. Would you like this done for the internal, external, web app vulnerability, and/or wireless testing?

IMRF Response: Follow-up testing will not be required under proposed contract.

Is Retirement Fund's IT organization centralized or decentralized?

IMRF Response: Centralized

When does the Retirement Fund intend to respond to vendors' questions? Is there any chance of a deadline extension as the turnaround time is very short?

IMRF Response: May 2, 2023. Not currently.

What is the Retirement Fund's budget for this project?

IMRF Response: Funds have been budgeted for 2023, but amount cannot be disclosed.

Has the Retirement Fund had this type of assessment performed in the past?

IMRF Response: Yes.

As an organization, is the Retirement Fund confined to awarding to the lowest bidder?

IMRF Response: No. IMRF may award the proposal that presents the best value to the organization. Our Board of Trustees must approve the award.

Re: External Network vulnerability assessment and penetration testing, is exploit testing included in the external network vulnerability scans? How many IPs are active?

IMRF Response: Reference response to Question 1 above.

Re: Internal Network vulnerability assessment and penetration testing, approximately how many IPs or subnets are in scope? Can all internal network testing be done from a single location?

IMRF Response: Refer to question 1. Yes, can be performed from single location.

Re: Web Applications, how many web applications are in scope? Are the web applications Internet-facing or internal only? Is web application testing included?

IMRF Response: 30 internal facing applications. Two external facing applications. Yes, application testing to be included in scope of services.

Re: Wireless Network vulnerability assessment and penetration testing, is the wireless network controller-based or access-point-based? How many locations are in scope for wireless network testing?

IMRF Response: Controller-based. Just one in Oak Brook, Illinois.

Under Request for Proposal, can you also please confirm that the Retirement Fund does not require a CPA to perform the requested IT security auditing services.

IMRF Response: IMRF will not require a CPA to perform requested services.

Page 5, 1st Paragraph. Will you please consider removing the CPA requirement?

IMRF Response: IMRF will not require a CPA to perform requested services.

Is a recording available of the pre-proposal conference that was held on April 20, 2023?

IMRF Response: No video is available.

Experience and Qualifications, Pages 11-12, Items c-f. What do these requirements have to do with Internal/External Penetration Testing?

IMRF Response: Reference Addendum issued on April 28, 2023

How many Internet facing hosts comprise the in-scope environment (servers, routers, firewalls, IDS/IPS)?

- # Servers in scope? 10
- How many firewalls? 1
- IDS/IPS – do you utilize one and if so, is it locally managed? Zero
- How many Internet facing sites / applications (URLs) are included in the scope? 3 sites
- Would you like any applications tested without credentials? Yes
- Would you like any applications tested with regular credentials? Yes
- Would you like applications tested with admin credentials? Yes

Please list all internal network segments in scope (management, production, development, DMZ, etc.).

IMRF Response: Production, UTA & DEV segments

Please list any persistent connections to 3rd-party vendors (HVAC, IT service provider, etc.).

IMRF Response: None.

Do you want any cloud environments tested such as Azure or Amazon Web Services?

IMRF Response: M365

Any remote access services in-scope (on-demand VPN, GoTo my PC, LogMeIn, etc.)?

IMRF Response: Corporate VPN

How many employees have remote access?

IMRF Response: 200+

Any in-bound modems (or remote access) in use?

IMRF Response: None

How many servers in-scope? 500

- Windows servers? Yes
- Other operating systems (please list)? None

How many users?

IMRF Response: Under 300 users

What database technologies are in use (Oracle, Microsoft SQL, IBM DB2, MySQL, PostgreSQL, etc.)?

IMRF Response: Microsoft SQL

What type of Social Engineering exercise is desired?

IMRF Response: Digital exercises such as phishing simulation(s).

Is there a formally adopted security framework in use?

IMRF Response: Moving toward formal adoption of the NIST CSF.

Is there to be a wireless assessment?

IMRF Response: Yes.

Do you have cybersecurity policies currently and if so, how many exist?

IMRF Response: Yes, eight to ten.

What are the drivers or conditions that are leading to this this project?

i. Compliance/Regulatory checks of network security

ii. Verification of security configurations

iii. Test monitoring tools

iv. Assumed compromise – measure and test the impact of a compromise of a normal user workstation

v. Other

Who are the stakeholders for the deliverable? For example is this meant to be only a report for IT or will this material be summarized to Management, Leadership, Governance Boards/Committees? What is the intended use of the report and distribution?"

IMRF Response: All parties - Presentation to Board of Trustees in November. Provided to audit committee for insights and awareness throughout organization.

Have pentesting procedures been performed before? Yes

i. If so, were there any availability or performance issues experienced? No

ii. If so, has the network changed significantly since the last procedures? No

The proposal has specified 500-1000 endpoints. Can you provide additional context around the breakdown of how many assets are externally facing and will be included in the external pentest?

IMRF Response: Refer to above responses.

Are all in-scope assets owned and operated by the organization?

a. Examples include leased modems and third-party appliances

IMRF Response: Yes

Are any in-scope assets supported via cloud resources?

a. Examples include cloud service providers such as, Azure, AWS, GCP, IBM

IMRF Response: No, with exception of M365

Are most assets visible from a single point of connectivity?

a. Is segmentation testing required? How many segments will be included?

b. How many different connections will need to be made throughout testing?

IMRF Response: Yes, asset visible form single point. Yes, all thirty VLANs.

Are all in-scope assets owned and operated by the organization?

a. Examples include leased modems and third-party appliances.

IMRF Response: Yes.

Are any in-scope assets supported via cloud resources?

a. Examples include cloud service providers such as, Azure, AWS, GCP, IBM

IMRF Response: Yes, M365

Our assumption is that for procedures such as exfiltration testing that these will be done with shared knowledge and awareness from an IT and Internal Audit representative with the focus being on testing the technical control capabilities. Is this aligned with expectations?

IMRF Response: Yes, aligns with expectations.

Will IMRF provide a test user account to perform authenticated procedures in the event credentials are not compromised throughout the beginning phases of the pentest?

IMRF Response: Yes, credentials will be provided.

For the purposes of internal audit, do we need to perform a vulnerability scan with a domain admin equivalent credential? No

a. How many domains or authentication zones are included? One

Is there a preference between how the internal penetration testing is performed between onsite and remote approaches? Are remote solutions where a representative from IMRF assists in deploying a testing drone on the internal network approved?"

IMRF Response: No preference. Testing drone is acceptable.

The RFP references Attachment A, yet there does not appear to be an Attachment A in the RFP document or in a separate file provided. If this attachment is relevant to our response, please provide it.

IMRF Response: Not relevant.

On page 10, is letter e., Company Background and General Description, under #1. Letter of Transmittal, supposed to be part of the letter or a separate item in the larger response (i.e. #2)?

IMRF Response: Designate has a second separate section.

Pages 11-12, 3. Experience and Qualifications, letters c-f do not seem applicable to us based on the scope. Are we required to answer these items or is it acceptable to answer N/A?

IMRF Response: Please refer to addendum issued on April 28, 2023.