

Minnesota State Retirement System

Project Title: System, Network and Operational Penetration Testing

Vendor questions submitted:

Device/Firewall/Architecture review:

1. How many device configurations need to be reviewed (generally routers and firewalls, please provide make/model)?
 - a. *1 each Firewall PA-4020, PA-2020, PA-2040.*
 - b. *2 Extreme 450a switch routers. (two)*
 - c. *1 ASA 5510 VPN*
 - d. *2 extreme wireless controllers*
2. Total approximate number of ACLs/Policies?
 - a. *300*
3. Any policy review in scope?
 - a. *Yes*
 - b. If so, how many pages of documentation?
 - i. *5 Policies/standards – 23 pages total.*
4. Is virtual architecture in scope?
 - a. *Yes*
5. Is Storage architecture in scope?
 - a. *Yes*
6. How many physical locations need to be reviewed?
 - a. *1*
7. Is an External Penetration Test in scope? *Yes.*
 - a. What is the number of active IP addresses?
 - i. *156.99.73.64/27*
 - b. What is the number of externally facing applications or urls?
 - i. *3*
 - c. Is validation testing included after the first test is completed?
 - i. *Very likely*
 - d. What are the scan windows?
 - i. *1800-0600hrs weekdays*
8. Is an Internal Penetration Test in scope? *Yes.*

- a. How many systems and applications are in scope?
 - i. *150-200 systems*
 - b. Do you have standard internal builds?
 - i. *Yes, for workstations*
 - c. Is sampling an alternative?
 - i. *Yes*
9. Is an authenticated application penetration test in scope?
- a. *No*
10. What are the key IT risks/concerns that MSRS is currently facing?
- a. *Will discuss upon vendor selection.*
11. Does MSRS have a defined time frame for execution of the testing and presentation of deliverable reports?
- a. *Completion prior to December 31, 2013.*
12. Does MSRS expect to have the selected firm re-test remediated observations within the period of the contract?
- a. *No.*
13. Does MSRS expect any significant change in operations/information technology in the upcoming future that would impact our approach?
- a. *No*
14. Does MSRS expect the assessment to include review and feedback related to IT policies?
- a. *Yes*
15. External IT infrastructure:
- a. How many external (Internet facing) IP addresses does MSRS have/own that should be considered as in-scope for external testing?
 - i. *A /27 external address scope.*
 - b. How many websites are running from MSRS's infrastructure?
 - i. *0*
 - c. Please describe the Internet facing systems/applications run by MSRS that are hosted on in-house systems.
 - i. *Exchange and VPN*
 - d. Please list any Internet facing systems that are conducting some form of e-commerce or payment activity.
 - i. *MSRS maintains account management systems which may include financial information.*
 - e. Please list the number of different operating systems and web servers (i.e. IIS, Apache, etc...) that are running.
 - i. *Windows 2008r2 for exchange*
 - f. Please describe each form of remote access provided to staff, IT, and/or vendors.
 - i. *ASA5510 Clientless SSL vpn*

- g. Are there any hosted applications (not on MSRS infrastructure) that should be considered in-scope for this assessment?
 - i. *No*
- h. Are there any modems/RAS in scope for testing (i.e. War Dialing)?
 - i. *No*

16. Internal IT infrastructure:

- a. Please list the number of active directory domains in operation.
 - i. *1*
- b. Please describe any (centralized) authentication mechanisms in place.
 - i. *AD and Radius*
- c. Please describe the number of in-house servers, including their operating systems.
 - i. *10 Ubuntu 10.04 servers*
 - ii. *14 Win2008R2 Servers*
 - iii. *4 esxi 4.1 servers*
 - iv. *1 redhat server*
 - v. *6 Cisco VOIP servers (Linux and windows)*
- d. How many are virtualized?
 - i. *24*
- e. What is the virtualization technology in use?
 - i. *VMware*
- f. Does MSRS have an accurate, up to date inventory of which systems/servers contain sensitive data (personally identifiable information, credit cards, attorney-client privileged information, criminal records and health insurance information).
 - i. *no*
- g. Is any of the sensitive data contained on workstations/laptops/mobile devices?
 - i. *No, but possibly*
- h. How many desktops, laptops, and other peripheral systems are on the internal network?
 - i. *100+*
- i. What different operating systems are in use for desktops and laptops?
 - i. *Windows 7 and Windows XP*
- j. Please describe the number of business applications that are considered Commercial Off The Shelf (COTS), vs. internally developed/maintained/programmed.
 - i. *No COTS.*
- k. Please describe any in-house developed/programmed applications.
 - i. *Customized. Deferred Compensation Plans*
 - ii. *Customized. Health Care Savings Plan*
 - iii. *Customized. General Employee Retirement Plan*
- l. How many wireless nodes are in operation (infrastructure AND client/end points)?
 - i. *12 Aps. A few dozen wireless devices on guest access.*
- m. Does MSRS allow staff to use personally owned devices (laptops, tablets, smart phones) to access resources?
 - i. *No. (Have a mobile device policy, but no BYOD Policy)*
- n. Is there a BYOD policy in place?
 - i. *No*
- o. Please describe any mobile applications in use that should be considered in scope.
 - i. *None.*

17. Will MSRS provide us with network diagrams?
 - a. *Yes*

18. Has MSRS adopted a governance framework (i.e. COBIT, ISO, ITIL, etc...)?
 - a. *ITIL in development*
 - b. *NIST SP800 Series*

19. What third-party service providers are currently being utilized by MSRS from an IT perspective
 - a. *MN.IT for application hosting, ISP, and voice T1s*

20. Is there a preference for “White Box” vs. “Black Box” testing approach (i.e. Informed vs. Uniformed testing)?
 - a. *MSRS prefers that the vendor bring recommendations to us for discussion and decision.*

21. Will social engineering techniques be considered in-scope?
 - a. *Yes*
 - i. *Email phishing? Yes*
 - ii. *Pre-text phone calls? Yes*
 - iii. *In person attacks? Yes*

22. Does MSRS’s internal IT/Security staff perform periodic vulnerability scanning as part of their administrative maintenance procedures?
 - a. *Yes*

23. Has MSRS made a determination as to whether it needs to be PCI-DSS compliant?
 - a. *No PCI-DSS compliance requirements*
 - b. Has MSRS made a determination as to whether it needs to be HIPAA compliant?
 - i. *Yes, HIPAA compliance requirements*
 1. *If yes, how long has MSRS been engaged in HIPAA compliance activities?*
 - c. What portion/percentage of the infrastructure is in-scope for HIPAA compliance?
 - i. *Those involving disability applications, physician’s certifications on HCSP reimbursements, possibly others.*

24. Are there any other compliance frames to be considered as part of the assessment?
 - a. *Yes. FINRA “clean desk” policy*