



ADMINISTRATIVE OFFICE OF THE COURTS

GOVERNMENT RELATIONS
INFORMATION TECHNOLOGY
INTERNAL AFFAIRS
JUDICIAL COLLEGE OF MARYLAND
OPERATIONS
PROGRAMS

Questions/Answers #3 JIS Vulnerability Assessment Scan RFP K16-0034-29 April 25, 2016

To our prospective Business Partners:

The following question for the above referenced RFP were received by email and answer will be posted for all prospective Offerors. The statements and interpretations contained in the following responses to questions are not binding on the Judiciary unless the RFP is expressly amended. Nothing in the Judiciary's response to these questions is to be construed as agreement to or acceptance by the Judiciary of any statement or interpretation on the part of the Offeror asking the question.

- 1. Question: Is the environment to be audited segmented from the rest of your network(s)? If so, how?**

Answer: [No](#)

- 2. Question: Do you outsource any form of its payment processing to third party service providers? If so, what services are provided and by whom?**

Answer: [Not included in scan.](#)

- 3. Question: Do you have more than one in-scope site? If yes, how many?**

Answer: [Scan to be performed from one location](#)

- 4. Question: Size of in-scope network...**

- a. # of Servers**
 - i. Physical**
 - ii. Virtual**
- b. # of workstations (desktops & notebooks)**
- c. Thin clients:**
- d. # of routers/firewalls:**
- e. # of network switches**
- f. Load balancers and gateway devices:**

Answer:

[Section 2.4.1 - no more than 1500 systems](#)

5. Question: What operating systems are in use?

Answer: Windows, AIX and Oracle

6. Question: If multiple sites, how many Internet Connections?

Answer: Scan to be performed from one location

7. Question: Is a full, updated/accurate, detailed network diagram available?

Answer: Having this answer does not impact scope of services

8. Question: Is there an up-to-date detailed system inventory of all system components, including: Point-of-Sale systems?

- g. Network components**
- h. Servers and other systems (mainframes, mid-range, etc.)**
- i. Devices performing security functions**
- j. End-user devices (such as laptops and workstations)**
- k. Virtualized devices**
- l. Critical software**

Answer:

Having this answer does not impact scope of services

9. Question: Are all in-scope systems hardened in accordance with industry standards such as DISA STIG, CIS Benchmarks, etc.?

Answer: Yes

10. Question: What tools or processes do you use to monitor all in-scope system audit logs daily for evidence of compromise?

Answer: Having this answer does not impact scope of services

11. Question: Do you run at least quarterly internal and external vulnerability scans against all in-scope components?

Answer: Having this answer does not impact scope of services

12. Question: Do you develop any in-house software in any in-scope systems? If so, please describe.

Answer: We do not have any in house written applications in scope for this scan.