**RFP 21-01 PCI Assessor Bidder Questions & Answers**

1. Page 24 of RFP 21-01 states, "The project manager shall provide the Arizona State Treasurer a copy of the following audits performed no more than twelve (12) months ago within seven (7) days of issuance of the contract." There are no audits listed directly after that statement. To what audits is that statement referring?

This is referring to the certifications required by the PCI Security Standards Council. That any work performed by the Contractor and its employees must provide evidence that they are certified by the PCI Standards Council to perform such work.

1. PCI DSS Assessment Specific:
   1. How many SAQ-Ds are there expected as part of deliverables?   
      One and a statement regarding an internal service provider.
   2. How many and what type of additional “agency specific” SAQs are expected as deliverables? (*non* SAQ-D, as specified in question #1)  
      2020 audit, there were 101 SAQs from the agencies that ranges between SAQ A, SAQ B, SAQ B-IP, SAQ C, SAQ C-VT, and SAQ P2PE.
   3. Describe the scope for each, individual separate SAQ as follows:
      1. Number of servers in scope for each particular SAQ 50+
      2. Number of datacenters in scope for each particular SAQ should this be blank or ‘0’?
   4. For each individual separate PCI SAQ, please specify if it is a repeat certification, or a first-time certification. Repeat.
      1. If repeat certification, please list the PCI DSS recertification date for each respective, individual SAQ

PCI DSS Recertification date will be 12/16/2021.

Associated Managed Security Services:For each separate individual SAQ specified in Questions 1 through 4 (*not* cumulatively or in the aggregate):

1. How many *external* (web facing) IPs will there be in scope for external vulnerability scanning (ASV) and external network penetration testing? In 2020, we did not require a penetration test, but we did in prior years.
2. How many *internal* IPs will there be in scope for internal vulnerability scanning and internal network penetration testing? In 2020, we did not require a penetration test, but we did in prior years.
3. How many applications will there be in scope for application penetration testing and how many associated externally facing URLs are there in total? In 2020, we did not require a penetration test, but we did in prior years.
4. How many assets (servers, PCs, etc.) will there be in scope for unencrypted card data discovery scanning services? We will not be requiring any ASV. In 2020, we did not require a penetration test, but we did in prior years.

Example:

XYZ Arizona Agency: SAQ-A.

Number of servers in scope:10

Number of datacenters in scope: 2

Repeat certification

Recertification date: June 30, 2021

# External IPs: 8

# Internal IPs: 38

# Applications: 3

# Associated URLs: 4

# assets for card data discovery: 35

1. Your RFP has “…PCI Qualified Security Assessor (QSA) to perform assessment and validate the State’s PCI DSS compliance” however it is not clear if you are truly looking for the:
   1. PCI QSA auditor
   2. PCI DSS assessor who may utilize the SAQs, assessments and advise
   3. PCI ASV certified scanner

These are very different, and some may NOT be the same Firm, by rules of the PCI Council.

PCI QSA Company for auditing and consulting.

If it is the PCI QSA auditor, and their services, the scanner may not be the same Firm, however the PCI DSS assessor and ASV scanner can be, although they may NOT offer the annual report.

1. How many locations? N/A
2. How many PCI assets or PCI ranges with assets? N/A
3. What is your rotation of scans and tests to remediation? NA
4. What type assets are you PCI scanning (databases, systems, anything at the network level)? N/A
5. How many merchants will require a Report on Compliance?  
   From the past PCI audits, two agencies (including ASTO), required a report on compliance.
6. How many merchants will require a SAQ?  
   From our prior year audit, we received one SAQ D report.
7. Roughly how many IP addresses are in scope for internal and external vulnerability scans and penetration tests? We will not be requiring any ASV. In 2020, we did not require a penetration test, but we did in prior years.
   1. Can this information be broken down by the number of merchants?
8. Does each merchant have their own IT and security personnel or are IT and security services centralized under ASTO or the State?  
   Most agencies have their own IT or use the statewide IT staff for assistance.
9. Does each merchant maintain their own policies and procedures when it comes to payment card handling or are these centralized?  
   We have set Statewide policies in our State of Arizona Accounting Manual (SAAM) - <https://gao.az.gov/publications/saam>. Agencies also implement their own internal policies and procedures.
10. Is each merchant responsible for conducting awareness training or is this process centralized?   
    PCI awareness for the State is conducted through computer-based training from the State’s centralized training portal.
11. Are all merchants in the Phoenix area or spread throughout Arizona?  
    We have agencies located throughout Arizona.
12. Do all merchants currently use P2PE devices? If not, how many do not use P2PE devices for card present transactions?   
    No, not all agencies use P2PE devices. About 20 agencies do not use P2PE devices.
13. Are backend systems such as servers, databases, network devices located at the merchant or within the state’s data centers?   
    They are located with the agency, at their location(s).
14. Is there a breakdown on the number of merchants that use card-present, e-commerce, mail/telephone orders, or other payment channels?  
    
15. Is the size and complexity of each merchant the same? If not, please describe the size and complexity of the largest and smallest merchant.  
    No, the size and complexity of each agency is not the same. At our simplest, we have smaller agencies that accept e-commerce payments only, to larger agencies that have 75 facilities throughout Arizona and accept payments through different channels.
16. How does ASTO prefer to see the pricing details, by merchant size and complexity or by overall costs for all merchants?  
    Overall cost for all merchants per Product/Service.

## High-level description of your business. Including revenue, physical locations, total employees, IT staff, staff dedicated to PCI, etc. The State of Arizona accepts payments for products and services provided by State agencies which may include but are not limited to: licenses, taxes, fees, assessments, and more, as required per Arizona Revised Statues. The gross sales for payment card transactions in 2020 was $485 million. There are about 175 locations that are part of the PCI audit scope. Each agency has their own designated IT or PCI staff.

1. Do you have an ISA on staff?  
   We currently do not.
2. Who handles PCI? Describe the person, team, etc.  
   The Arizona State Treasurer’s Office oversees the PCI compliance at a high level and each agency that accepts credit card payments has an individual that handles PCI compliance.
3. Describe at a high-level how you accept credit cards?   
   Payments are accepted through e-commerce, card-present or mail-order and telephone-order transactions process the data using analog, cellular, or IP-connected POI terminals, P2PE-validated solutions, dedicated workstations or tablets to enter cardholder data into online payment gateways.
4. What are your payment channels?  
   Payments types accepted by the State are cash, check, cashier’s check, money order, payment card, e-check, ACH, and wire.
5. Who is your acquirer?  
   Bank of America
6. What is the name of your credit card processor?  
   Bank of America Merchant Services
7. Does your company have a relationship with one or more third-party agents? (for example, web hosting companies, card gateways like Cybersource or Authorize.net). If so, please explain.  
   Yes. We contract with third-party gateway providers as they are able to provide services required to meet the needs of the agency, while being PCI compliant.
8. Do you access card present transactions? If so, please describe all elements, PoS, PoI, hardware, etc.  
   Most State agencies that process card-present transactions process the data using analog, cellular, or IP-connected POI terminals provided by Bank of America. Several P2PE-validated solutions from Clover Networks and Bluefin Payment Systems are also used.
9. Do you have a defined CDE? If so, please describe it in detail. Include all servers, including: web, application, database, authentication, mail, proxy, NTP, DNS, etc. Each merchant may be setup differently. This would need to be determined during a scoping exercise for each merchant.
10. Describe network components. Including firewalls, switches, routers, wireless access points, network appliances, and other security appliances.   
    Statewide firewall standards can be found: <https://aset.az.gov/sites/default/files/P8350%20System%20and%20Communication%20Protections_Sept2018_1.pdf>
11. Is virtualization used? If so, detail virtualization components including virtual machines, virtual routers / switches, virtual appliances, virtual desktops / applications, hypervisors, etc.

There is at least two merchants that use virtualization.

1. Do you use segmentation? If so, detail.

Yes. Segmentation is used to provide standalone kiosks for agencies.

1. Where is CHD stored?  
   Cardholder Data is stored by the payment gateway and not electronically stored by the agency.
2. Do you have diagrams with data flows?  
   Each State agency has a different setup and data flow for their process and payment acceptance.
3. Do you use payment applications? If so, are these payment applications in-house developed or COTS?  
   Payment applications are both in-house developed and contracted.
4. Describe cloud services used around CHD. If cloud services is used for CHD, it would be different for each agency.
5. Is CHD stored in your data centers? If so, what are the locations? We aren’t aware of CHD being stored at the call centers.
6. Do you use call center to accept credit card payments? If so, where are they located and roughly how many CSA are there?   
   We have one call center and they are located in Phoenix. There are approximately 20 CSAs.
7. Do you use call recording software? If so, what vendor and version? Where are the call record files stored? How long are these recording stored for? No.
8. Do you have specific PCI security policies and processes?  
   Yes, they are located in our State of Arizona Accounting Manual (SAAM) - <https://gao.az.gov/publications/saam> Topic 40, Sections 16, 17, 18, & 19
9. Is tokenization used? If so, details how. Including method, vendor, etc. Yes. Through our current vendor for merchant services and the applications that they provide.
10. How do administrators connect to the CDE? This can be different for each merchant.
11. How do users connect to payment applications? Desktop, virtual desktop, etc.  
    Desktop, virtual desktop, POS terminal.
12. Do you use multi-factor authentication? If so, describe how it is used including vendor, method, hardware/software, etc… Yes. Each merchant that uses multi-factor authentication may use a different vendor and use it differently.
13. Is internal and external vulnerability scanning of the CDE done? If so, describe how. Yes. Performed by a company.
14. Have penetration tests been done against the CDE? If so, please describe. Yes. A company performed the test.
15. Do you back up any of the CHD? This includes cached data, files, net shares, etc.   
    No, Cardholder Data is not stored or backed up.
16. Where are backups stored? N/A
17. Do you use outsourced service providers that have access to the CDE or CHD? If so, details the policies and processes in place for access. Yes. There are Statewide policies and each merchant may have additional internal policies.
18. Penetration Testing Scoping Questions for Card Data Environment (Answer all that Applicable) We did not require penetration testing last year, but did require penetration testing in prior years for only one merchant.

**Web Applications**

**For each application:**

* The URL/IP address if publicly accessible. Yes.
  + If not how are the applications accessed?
* A brief summary on what the application is used for. Purchasing products or services provided by each merchant.
* What functionality exists before login, and approximate number of pages (e.g. login, register, forgotten password)? This can be different for each merchant.
* What functionality exists after login, and approximate number of pages (e.g. add to basket, payment, write blog post, account management – change password)? This can be different for each merchant.
* How many user roles are there and what additional functionality can they access? This can be different for each merchant.
* Where is the application hosted (cloud etc.)? This can be different for each merchant.

**External Infrastructure**

* Total number of live/active Internet facing IP addresses 50+
* Types of publicly accessible services (e.g. FTP, SFTP, SMTP) This can be different for each merchant.

**Internal Infrastructure**

* Number of workstations? Possibly 25+
* Number of servers? 50+
* Which operating systems are in use? This can be different for each merchant.
* Is the network segmented or flat? Could be either based on the merchant.
  + Can all networks/VLANs in scope be accessed from one network point? It will be different for each merchant.
  + Number of networks/VLANs in scope? 50+
* Is there any Wireless capability? There wasn’t any wireless capability in scope for 2020.
  + Number of Access Points? -N/A
  + Number of SSIDs broadcasted? N/A
  + What types of authentication are in use, if any? N/A
* Where is geographical location of the internal environment? Across Arizona.
  + If there are multiple sites, where are the locations for each? There are multiple sites across Arizona.
  + Can all locations be accessed from one main site? No.

1. How many internal and web applications store, process or transmit cardholder data?  
   No internal or web applications store cardholder data.
2. How many databases support the in-scope applications? Possibly 50+
3. List all database platforms that store credit card data.  
   Merchants do not store credit card data.
4. How many servers store, process or transmit cardholder data to support the applications in- scope? Merchants do not store cardholder data.
5. What are the operating systems for the servers? This can be different for each merchant.
6. Is there segmentation between the systems storing credit card data and the rest of the network? Yes.
7. How many Internet, DMZ, or segmentation firewalls are in place? 50+
8. How is segmentation achieved? This can be different for each merchant.
9. Is wireless technology in use anywhere on the network? If so, how many locations? Wireless technology is not used currently.
10. Is credit card data transmitted over wireless devices at any point? Yes.
11. Are credit card transactions accepted through a web server? Yes.
12. Are credit card numbers stored on the POS systems for any length of time? No.
13. How many data centers store, process or transmit cardholder data and where are they located? 50+, throughout Arizona.
14. How many call centers store, process or transmit cardholder data and where are they located?  
    One call center and they are located in Phoenix.
15. Is any part of the environment outsourced? Yes.
16. Are there third parties, outsourcers, or business partners connected to the network? Yes.
17. How many internal departments/business units are in-scope for PCI? This would include any team that has access to systems and applications that store, process and transmit credit card data.  
    From last year’s audit, there were 102 business units in scope for PCI.
18. How many IP address ranges should be considered in scope, and the size of the block of IP’s (e.g. /24, /16, etc)? This is in regards to both Internal and External Penetration Testing. 20+ IP addresses. The size may be different per merchant.
19. What is the approximate number of live devices (servers, workstations, network devices such as routers and switches, etc.) within these IP address ranges? 100+
20. How many live External facing IP’s are on the network? 50+
21. Are there any excluded IPs or IP ranges, or excluded types of devices? Not that we are aware.
22. Are there any WAN or extranet links to partner/third-party networks that should be excluded from testing? Not that we are aware.
23. If authenticated web application testing is to be included in scope, how many accounts / security levels will need to be tested? 50+
24. Are any of the system components that are considered in scope owned/managed/hosted by a third-party? Yes.