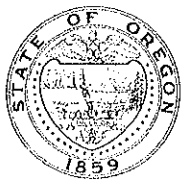
TED WHEELER
STATE TREASURER

DARREN BOND
DEPUTY TREASURER



PHONE 503-378-4000
FAX 503-378-7051

STATE OF OREGON
OREGON STATE TREASURY
350 WINTER STREET NE, SUITE 100
SALEM, OREGON 97301

MEMORANDUM

To: Oregon State Agencies Required to Report Compliance with PCI DSS Standards

From: Curtis Hartinger, Information Assurance Officer

Subject: Oregon State Treasury E-Commerce Program: Payment Card Industry Data Security Standards (PCI DSS) Scanning Requirement (11.2)

Date: April 1, 2011

Based on Treasury's numerous discussions with agency staff and the State's Qualified Security Assessor, Coalfire Systems, it is apparent that the Payment Card Industry Data Security Standard (PCI DSS) requirement 11.2 regarding scanning can be confusing to many state agencies. To address this issue, this memorandum is intended to provide additional information to state agencies to help clarify this requirement. If you have additional questions after reading the memo, please contact Curt Hartinger at (503) 378-3150 or Sharon Prentice at (503) 373-7312.

PCI DSS Scanning Requirement 11.2

Section 11.2 from the PCI DSS is required for all merchants that must complete Self Assessment Questionnaire (SAQ) C or D based on their payment application processing environment. Section 11.2 reads:

> Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades) as follows:
>
> 11.2.1 (a) Are quarterly internal vulnerability scans performed?
>
> (b) Does the quarterly internal scan process include rescans until passing results are obtained, or until all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved?
>
> (c) Are internal quarterly scans performed by a qualified internal resource(s) or qualified external third party?

Purpose of External and Internal Vulnerability Scans

External Scans

The purpose of an external vulnerability scan is to best protect payment card systems from access by hackers over the Internet. Because external scans are only required for computers that process, transmit, or store sensitive cardholder data using "routable" IP addresses, they are not required for most agencies.

To clarify what we mean by routable IP address, an address is routable if a hacker outside your network can perform a port scan (using a network mapping tool or – NMAP), and determine which ports and services are open and running on your computers that are processing credit card transactions (e.g. via your web-based virtual terminal). On the other hand, if the IP addresses of computers that process, transmit, or store sensitive cardholder data are protected by Network Address Translation (NAT) (e.g. by lying behind a NAT Firewall), and are not routable over the Internet, they do not need an external scan. This is the most common scenario for State agencies.

External Scanning Requirement Options

If you are required to perform external scans, please note that an external scan cannot be performed by you (the merchant). The external scan must be performed by a Qualified Security Assessor (QSA).

- DAS Enterprise Security Office manages the contract with the State's QSA, Coalfire, to perform external scans for State agencies.
- Agencies also have the option of contracting for their own QSA.

Please contact Curt Hartinger (503) 378-3150 if you have any questions about QSA options.

Internal Scans

The purpose of an internal vulnerability scan is to best ensure that computers that process, transmit, or store sensitive cardholder data, and all computers in the same segment of the network, are properly protected, and to validate that the protection in place is effective. This protection includes a hardened configuration standard for the system, an updated version of anti-virus, and all applicable security patches for the applications on those computers.

This PCI DSS requirement is meant to address risk of loss of sensitive cardholder information via preventable vulnerabilities on computers processing credit card transactions (this includes swiped or key entered transactions). For example, the existence of malware (such as a key logger or memory capture application on a merchant's computer) could be detected by an internal vulnerability scan. Of note, even though the processing of credit card transactions may actually occur at a hosted virtual terminal vendor's data center (e.g. US Bank's data center in the case of Virtual Merchant), there is still a risk that sensitive cardholder data could be captured at the time it is being entered by the merchant; thus, the requirement for internal scans.

Is my agency required to perform an internal scan?

Every State agency required to complete SAQ C or SAQ D is required to perform internal scans and remediate critical vulnerabilities quarterly. Examples of processing environments that require completion of SAQ C or SAQ D include:

- Processing cardholder data through one or more computers on an agency network by accessing a vendor hosted solution through a web browser, including US Bank/Elavon's Virtual Merchant. (SAQ C)

- Processing cardholder data through applications installed on agency computers and/or networks, e.g., licensing, cashiering systems, or payment applications that transmit, process, or store sensitive cardholder data. (SAQ D)

Internal Scanning Requirement Options
Internal vulnerability scans can be performed by internal staff to the agency as long as the staff performing the scans has the technical knowledge to properly configure and understand the results of the scans. See Appendix A for information about Internal Scanning Tools.

Option 1: Scan ALL computers on a network segment where cardholder data is transmitted, processed or stored. The intent of the PCI DSS is for merchants to perform internal scans on all computers where credit card information is being entered and on all computers on the same segment of the network where those computers reside. The reason that all computers in the segment should be scanned is because if one of those computers is infected with a piece of malware it is easier for a computer used to process cardholder data to be infected by the other computer because there is a trust relationship between computers in the same segment.

Option 2: Segment Virtual Terminal Computers (SAQ C). Version 2.0 of the PCI DSS was published in November 2010. In that version, the Security Council created a new Self Assessment Questionnaire (SAQ) SAQ C-VT. This questionnaire was written specifically for virtual terminal solutions, and does **not** require internal scans; however, one of the eligibility requirements for using SAQ C-VT is the following:

> Merchant accesses the virtual terminal via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment.

Information about Version 2.0 of the PCI DSS SAQs can be found on the following website: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

Option 3: Segment Card Processing Applications (SAQ D). Applications installed on a local computer and/or network should be segmented to reduce the number of computers in the segment and therefore the number of computers that need to be internally scanned and remediated. This segmentation can be achieved via a firewall or other form of network segmentation to isolate the computer processing merchant card transactions from other systems.

Treasury recognizes that it may be difficult and costly to comply with the Internal Scanning Requirement. For example it may be costly to scan and remediate "High" vulnerabilities on every computer residing in the same network segment as those computers used for processing credit card transactions. Additionally, we understand that it may be costly and reduce the computers functionality for merchants to install hardware to isolate computers in their own segment. This is why Treasury, DAS Enterprise Security Office (ESO), and Coalfire Systems are continuing to work together to identify solutions that will simplify the use of virtual terminals. We will notify agencies as soon as we have any new information to share.

Summary
Agencies are required to fully comply with the scanning requirements of PCI DSS section 11.2. If you have concerns about how you will comply with the scanning requirement options provided above, please contact Curt Hartinger or Sharon Prentice. They will assist you with a risk analysis of your current card processing environment taking into consideration the number of transactions processed and how you accept the card information, e.g. over the phone or point of sale. The information gathered during the analysis will help your agency determine which scanning option to implement or if it makes sense to switch to a different card processing environment such as dial up terminals.

Treasury values the partnership we have with agencies, and we sincerely appreciate your efforts and commitment to protecting sensitive cardholder data for the benefit of the State and your customer.

Attachment A

Internal Vulnerability Scanning Tools

Following are a few vulnerability scanning tool recommendations from DAS's Enterprise Security Office Senior Security Analyst, Shaun Gatherum.

- **Open VAS** - This tool is a split off of the original Nessus project, built from Nessus version 2.0, it utilizes their own community built NVT plugins. As of Dec 2010 they had roughly 19,000 nvt's. Here is the catch as it is to some degree with Nessus, whether or not a given vulnerability has a NVT is up to the community. Open VAS can be reliably downloaded from http://www.openvas.org/index.html
- **OSSIM** – Open Source Security Information Management. Is a suite of tools which includes Nessus 2.0 they offer their own plugins on an open source and paid subscription model.
- **Nmap** - Some people are utilizing the **Nmap** Scripting Engine as a framework for creating vulnerability scanning scripts
- **Nessus 2.0.10a** - is included as part of the still open version of **Helix** http://linux.softpedia.com/get/System/Operating-Systems/Linux-Distributions/Helix-7873.shtml and can be run from their live cd environment.

It is important to note that using Nessus 2.0 without plugins after July 2008 cannot be considered a valid vulnerability scan. Nessus does offer a home version with up to date plugins but using it on a state agency network will create legal issues for the state and the agency.

Please feel free to contact Shaun Gatherum for more information about scanning tools: (503) 378-5373 or shaun.a.gatherum@state.or.us