

Security Assessments

December 30, 2014

Last updated: December 30, 2014

1. Rate

Currently, there is no direct charge to State of Nebraska agencies for this service.

2. General Overview:

Computer and network security vulnerability management provides an accurate check of an agency's network, servers, desktops or web applications for security weaknesses. Functionality includes:

- Scan computers and apps on the Internet or in your network.
- Detect security vulnerabilities and the patches needed to fix them.
- View interactive scan reports by threat or by patch.
- Test websites & apps for OWASP Top Risks and malware.
- Test computers against SCAP security benchmarks.

The Office of the CIO provides this service through the QualysGuard Cloud Platform. Qualys is a web based application that scans the IP addresses of PC- based systems for known vulnerabilities. Once the scan has been completed, the Qualys tool produces a report listing vulnerabilities, locations, and methods for mitigation. Once the Qualys scan is completed and mitigation methods are implemented, the system scanned can be certified as PCI (Payment Card Industry) compliant.

3. Service Description:

The Nebraska Information Technology Commission (NITC) has adopted a set of security policies and standards. These are published on the NITC website: <http://www.nitc.nebraska.gov/standards/>. These include the requirement for periodic vulnerability scanning and other measures for promoting security of information assets. NITC Standard 8-401 also establishes a requirement for incident response and reporting (<http://www.nitc.nebraska.gov/standards/8-401.html>).

The Qualys service is a web based application. Users who request access to the application will receive a user ID and password, created by the office of the CIO, which will allow the user to log in and administer the scan of their systems. The systems scanned are based on IP Addresses that are provided to the Office of the CIO when requesting access. The IP addresses are populated to the user's profile when it is created, enabling the user to scan all systems within the agency. The user will not be able to scan any systems connected to IP addresses that are not authorized to that user's profile.

Qualys can scan systems within the state's network as well as public facing systems. It is recommended that scanning not be done during normal business hours, because scanning initiates a number of requests to the system which may disrupt service on those systems by competing for system resources. The scan can be initiated manually, or can be scheduled to start at a specific time automatically.

The recommended frequency for scanning non-critical systems is once per quarter (at least every 90 days). Critical systems should be scanned once per month. The scan should also be initiated after major updates, patches, etc. are applied to the system.

The service includes:

- Access to the Qualys application via specific User ID and Password.
- Report produced after scan that lists vulnerabilities on system, where they exist on system, and mitigation methods.
- Online training for the Qualys application.
- Periodic classroom-style training for the Qualys application.
- PCI compliance certification

The service does **NOT** include:

- Actual mitigation of vulnerabilities.
- Penetration testing.
- Application testing.
- Testing for AS400 systems.

4. Roles and Responsibilities:

The CIO is responsible for maintenance and administration of the Qualys application. This includes creation of user IDs and passwords, annual maintenance, customer support and escalation. If requested, Chris Hobbs, State Information Security Officer, will administer the Qualys scan to an agency's system.

The agency requesting service is responsible for administering the scan (unless requested that the Office of the CIO administer the scan) as well as mitigation of vulnerabilities discovered during the scan.

5. Requesting Service

Contact the Office of the CIO system administrator or OCIO Help Desk to utilize the system.

The request must be initiated or approved by the IT Manager for the agency requesting service.

When requesting the service, the following information must be included:

- IP Addresses for systems to be scanned.

6. Billing Information:

The Office of the CIO uses a system of Billing Accounts, Job Codes and Work Orders for authorizing work and tracking costs for specific projects. The customer may designate which job code and work order to use or request a new job code and work order. Contact the Office of the CIO for assistance with developing an accounting structure that meets the needs of the agency.

7. Service Hours, Response Times and Escalation:

The Qualys application is available 24x7x365. The service has built in redundancy and has an uptime reliability of 99.9%. Requests for access to the Qualys application will be processed during normal business hours.

Customers may contact the CIO Help Desk 24 X 7. Help can be obtained by calling 402-471-4636 or, for less urgent problems, directing e-mail to cio.help@nebraska.gov. Customers can also open tickets by visiting <https://ciohelpdesk.nebraska.gov/user/>. The help desk web site can be accessed at http://www.cio.nebraska.gov/tech_serv/help_desk.

For further information, please contact:

Office of the CIO Help Desk
cio.help@nebraska.gov
402-471-4636 or 800-982-2468