COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF HUMAN SERVICES, INSURANCE AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Infrastructure Vulnerability Assessment**	Number: **STD-ENSS028**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of:
Date Revised: **05/05/2017**	 Robert Doren, Chief Systems Engineering Section

Abstract:

The purpose of this standard is to describe the minimum expectations for infrastructure security vulnerability assessment and mitigation within the Commonwealth of Pennsylvania's Departments of Human Services, Insurance and Aging ("Departments").

No information system or network is without defect and the complexity inherent in technology can result in several weaknesses in its configurations. Together, these defects and weaknesses represent vulnerabilities that may be exploited by both internal and external threat sources seeking to weaken the confidentiality, integrity, and availability of the Departments' information systems. In order to protect these systems, threats and vulnerabilities must be identified, assessed for the risk they pose to the Departments and findings reported to the Departments' Chief Information Security Officer (CISO) for timely remediation.

The infrastructure security vulnerability assessment helps identify security vulnerabilities at the operating system, network configuration and service levels, and provides technical recommendations/mitigation steps to control these vulnerabilities. This standard complements other vulnerability testing standards already in place within the Departments; however, the scope of this standard does not include web application security vulnerability testing[1]. The following activities are to be performed to improve infrastructure security posture:

Scoping and Planning
This activity helps determine the type and depth of the infrastructure being assessed in order to derive the most applicable plan to complete the assessment.

Infrastructure Vulnerability Testing
As part of this activity, controlled network vulnerability tests should be conducted to identify potential security exposures at the operating system, network configuration

and service level. These tests are to be performed from both an authenticated and non-authenticated user perspective. This activity helps identify potential inherent weaknesses in the deployment and configuration of the Departments' information systems.

Vulnerability Analysis, Mitigation Planning and Reporting
Analysis of any findings is conducted and a report is prepared that provides a listing of all vulnerabilities identified, risk ratings and remediation measures. This activity provides the CISO with the information needed to take the appropriate action to reduce and mitigate the risks posed to the Departments' network infrastructure.

Security Risk Assessment
A security risk assessment is conducted by the responsible representative for the underlying infrastructure and the submission of a security risk self-assessment questionnaire. Please refer to the Departments' Risk Management Standard[2] for additional details on this activity.

General:

The Infrastructure Security Vulnerability Assessment Standard applies to the Departments' network infrastructure. The requirements outlined in this document are the minimum considered adequate to identify potential vulnerabilities due to improper configuration, access controls, patch management and inadequate training and awareness during deployment of networked information systems by the Departments.

Standard:

The Departments conduct both periodic and ad-hoc infrastructure security vulnerability assessments on at least an annual basis, when major infrastructure changes are made to hardware supporting Internet-facing information systems, or as determined by the Departments' CISO. Examples of major infrastructure changes that may require an infrastructure security vulnerability assessment include, but are not limited to the following:

- The introduction/integration of new or existing information systems or services
- Major hardware/software changes to public-facing systems
- Operating System (OS) upgrades

The scope of this assessment includes the Departments' network infrastructure and any accessible hardware contained within. The Departments expect the assessment to be performed as much as possible during non-business hours. The appropriate system owners shall work with the CISO and/or staff to identify the system infrastructure targeted for this assessment. All vulnerability assessments must be approved by the CISO.

Scoping and Planning
The scanning need, whether necessitated by auditing or regulatory compliance, system implementation, or periodic review, will dictate the scope and depth of the scanning efforts required. Maintaining a current inventory of network server and devices promotes the use of automated tools and manual techniques for the establishment of a comprehensive scanning plan for the target environment in order to fulfill the scanning requirements.

Once a network segment is targeted, some additional discovery steps to promote the scope and plan may include the following:

- Ping sweeps to identify accessible systems (not required if assessing specific systems after a major production change)
- Specialized scans using port scanning software to identify any open ports or services

- Connecting to open ports using network utilities to identify specific versions of software and network protocols running target systems

The Departments use the open source port scanning tool, Nmap, as its standard for these activities. Use of other tools should be approved by the CISO. Nmap[3] and any other alternate port scanning tools should be updated with the most current definitions prior to conducting any vulnerability scan.

Infrastructure Vulnerability Testing

The Departments shall perform network vulnerability testing by actively testing the connection points of the target infrastructure as determined in the scoping and planning phase and in order to identify potential vulnerabilities exposed by the underlying servers and/or network devices. As information is gathered, it should be cross-referenced with databases of known vulnerabilities and past attack for methods for proper identification and mitigation planning purposes. Vulnerability scanning will be performed on a monthly basis on a random sampling of infrastructure.

The Departments' use Tenable's Nessus Vulnerability[4] testing tool as its standard for these activities while coordinating scanning efforts with the CISO and other affected stakeholders. Use of other tools should be approved by the CISO. Nessus and any other alternate vulnerability testing tools shall be updated with the most current definitions prior to conducting any vulnerability scan.

Some additional methods of the network vulnerability testing steps and activities may include the following:

- The execution of automated and/or manual exploitation techniques to identify specific vulnerabilities or exposure points in operating systems and network services.
- The execution of advanced techniques, such as credentialed or content scanning
- The execution of targeted vulnerability port scans based on Nmap-provided ports collected in the initial scoping and planning phase

The identified security vulnerabilities should be communicated to the CISO and mitigated according to the guidelines defined in the section "Vulnerability Analysis, Mitigation Planning and Reporting" or as defined by the CISO.

Vulnerability Analysis, Mitigation Planning and Reporting

The results of the infrastructure vulnerability and security risk assessment should be shared with the Departments' CISO as soon as each of the tests is completed. Upon obtaining mitigation plan approval from the CISO, an integrated infrastructure security assessment report should be submitted including the following details:

- Security vulnerability/Risk Identifier
- Security vulnerability/Risk Category
- Security vulnerability/Risk Title
- Brief description of the Security vulnerability/Risk
- Potential business impacts
- Mitigation status
- Mitigation plan
- Date first reported
- Departments' approval status (Approved-Mitigated/Approved-Waiver Submitted/Unapproved)
- Departments' waiver status (Open/Closed/Expired)

It is expected that the vulnerabilities, or bugs, identified by the testing activities be handled by management similar to any other application bugs, documented and addressed using the steps outlined below:

- Open a Bug attached to a work item in Team Foundation Server (TFS) 2010 when a vulnerability is identified
- Prioritize the resolution for each vulnerability based on severity (business impact)
- Identify the mitigation strategy for each critical and high severity Bug during the current release of the application
- Monitor the bug for timely closure
- Once fixed, re-validate with a repeat scan to confirm that the vulnerabilities no longer exist
- For any vulnerability that is not mitigated, the respective program office must submit a security risk acceptance request to the CISO using the Departments' IT Risk Management (ITRM) solution. This request should be placed during the integration test phase of Software Development Methodology
- Obtain risk acceptance (if required) from the CISO and monitor the Bug for timely closure

Security Risk Assessment

The Departments have established an ITRM solution to assist their efforts of continuously monitoring the regulatory compliance posture of the information technology assets. As part of this effort, the Departments require the appropriate program office representative to conduct a security risk assessment and submit a security risk self-assessment questionnaire on the network infrastructure. Through the recurring assessment process, the Departments should:

- Update the list of known vulnerabilities at least quarterly or when new vulnerabilities are identified and reported
- Pro-actively determine trends related to infrastructure vulnerabilities to ensure policies, standards and/or procedures are up to date in the efforts to eliminate or reduce future vulnerabilities

The security risk self-assessment questionnaire should be submitted using the Departments' ITRM solution. The submitted self-assessment questionnaire will be reviewed by the Departments' Security Architecture Team to identify potential security, regulatory risks, and advise on mitigation planning going forward. Please refer to the Departments' Risk Management Standard[2] for details on conducting this activity.

Leading Network Infrastructure Security Practices

The Departments should, as part of leading industry practices, perform the activities summarized below in order to secure the network infrastructure:

- Periodic Patches and Security Updates
  - Ensure network devices are running the most current and secure version of the firmware
  - Define patch management policies that include testing the patch before deployment

- Non-Default Settings
  - Ensure that all default user names and passwords are removed or changed, and that other default security settings are set as appropriate as per Departments security policy

- Strong Access Controls

- Ensure that the access control lists (ACLs) and rule sets are correctly defined as required by the Departments
- Block all unnecessary ports and services and lock down administrative interfaces so they are inaccessible via the Internet and only accessible from specific hosts on the internal network
- Administrative interfaces may also require two-factor authentication and other user constraints
- Use the 'Default Deny' security principle
- Third-parties should not be granted access to the hosting infrastructure for services unless agreed upon by the Departments

- Audit Logging, Monitoring and Reporting
  - Ensure that logging is enabled for all dropped or denied traffic
  - Ensure the logs are stored centrally in a secured location, preferably on a separate network segment reserved for logging and auditing
  - Ensure that all server clocks are synchronized for logging
  - All login failures must be logged along with the failed login source
  - Resource access failures must be logged
  - Log files must be regularly backed up and archived to a secure location
  - Logs must be retained according to the defined Departments retention schedule

- Intrusion Detection/Prevention System (IDPS)
  - Set up IDPS sensors in the Demilitarized Zone (DMZ) and in the trusted network to detect attacks and assist in the event of an incident
  - Set up remediation workflows that include automatic event notification

- Network Compromise Diagnostic
  - Set up a workflow to ensure that infrastructure logs are analyzed regularly to detect potentially compromised systems and other network abnormalities

Exemptions from this Standard:

Any exemptions to comply with this standard should be discussed with the Departments' CISO.

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the Departments' Information Technology Standards Team.

Standard Supplements:

None

References:

1. STD-ENSS034: Web Application Security Vulnerability Assessment
   http://mydhs/cs/groups/webcontent/documents/communication/p_031992.pdf
2. STD-ENSS031: Risk Management
   http://mydhs/cs/groups/webcontent/documents/communication/p_031988.pdf
3. Nmap (Network Mapper)
   http://nmap.org/
4. Nessus Vulnerability Scanner
   (http://www.tenable.com/products/nessus)

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Incident Reporting	Clifton Van Scyoc
10/24/2013	1.1	Vulnerability Identification & Information Gathering	Mathieu Saury
01/24/2014	1.2	Standard update	Christopher Kajder
03/26/2015	1.3	Standard review, updated frequency of scans	Pamela Skelton
05/05/2017	1.4	Annual Revision	John Miknich