

**Office of the Chief Information Officer  
Enterprise Policy**

**Policy Number:** CIO-082

**Effective Date:** 05/15/2004  
**Revision Date:** 11/21/2008  
**Reviewed Date:** 11/03/2014

**Subject:** Critical Systems Vulnerability Assessments

**Policy Statement:** The purpose of this policy is to establish procedures for network vulnerability assessments of the servers and operational environments of critical systems by state agencies utilizing the Kentucky Information Highway (KIH), hereinafter referred to as "Agency." The scanning and testing is only permitted to target the resources owned or managed by the Agency or managed through Enterprise Shared Services.

**Policy Maintenance:** The Commonwealth Office of Technology, Office of Chief Information Security Officer, Security Administration Branch, has the responsibility for maintaining and updating this procedure.

**Authority:** KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies that support and promote the effective application of information technology within the executive branch of state government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

**Applicability:** This policy is to be adhered to by all staff, including employees, contractors, consultants, temporaries, volunteers, vendors and other workers within the Executive level cabinet of state government.

**Responsibility for Compliance:** Each agency is responsible for assuring that appropriate staff within their organizational authority have been made aware of the provisions of this policy, that compliance by the staff member is expected, and that the failure to comply with this policy may result in disciplinary action pursuant to KRS 18A up to and including dismissal.

It is also each Agency's responsibility to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for the Commonwealth Office of Technology's efforts to remediate issues related to the lack of adequate systems/network infrastructure security.

**Review Cycle:** This policy will be reviewed at least every two years.

**Definitions:**

Application – A software program designed to perform a specific function.

Critical Systems – The servers and computing infrastructure that support an automated business process identified as critical by the Agency based on the nature of the information stored (sensitive/confidential), importance to the agency's mission, or as stipulated by statute or regulation.

Network Environment – Includes the communications hardware and software components that are utilized by the system to exchange information with internal or external users of the system. Includes technical configuration, maintenance procedures, and overall functional compliance with Commonwealth security policy.

Operational Environment – Includes server hardware and software components used to process, store, or backup/recover information on a critical system. Includes technical configuration, maintenance procedures, and overall functional compliance with Commonwealth security policy.

Penetration Testing – A security testing procedure to proactively identify computer system vulnerabilities in order to locate and identify any weaknesses that could be exploited by intruders.

Scanning – An automated process to query computer systems in order to obtain information on services that are running the level of security.

System – An automated business process that is operated on computer hardware and software and is connected to the network.

Appropriate and Qualified Organization – Any contract or government organization that is not a part of the Agency's organizational structure and has demonstrated the technical capability to conduct security assessments for government agencies. This may include state or federal auditing agencies, state approved security contract vendors, or other external organizations whose capabilities and experience can be determined sufficient to conduct these assessments.

**Policy:** Agencies will be responsible for identifying critical systems based on the nature of the data and the system's business function or mission. The term "critical system" refers to the server, or servers, that support one or more critical business application. This may include web servers, database servers, and other servers that are essential to the operation of the business application. Each Agency shall engage a third party to assess all critical systems under the Agency's responsibility both upon initial implementation into production use and every two (2) years thereafter. These network and server vulnerability assessments do not include the development environments, or application software, related to these systems, which must be tested separately. Each agency shall follow the appropriate notification process outlined in this policy prior to conducting these assessments. It is the responsibility of the Agency, in consultation with the Cabinet CIO, to engage an appropriate and qualified organization that is considered an external or third party entity to ensure objectivity and accuracy in the assessment. It is the responsibility of the Agency to ensure that the entity conducting the vulnerability assessment has signed an appropriate confidentiality statement prohibiting the divulgence of sensitive information. This requirement may not apply to certain state or federal agencies, such as the Auditor of Public Accounts.

It is important that scanning and penetration testing activities are conducted in a manner that will not disrupt or otherwise degrade the quality of services that the Commonwealth Office of Technology (COT) provides to agencies not involved in the assessment process. To this purpose, COT will aggressively block any scans suspected to be causing any service disruption until this activity can be determined to be a part of an agency's authorized security assessment, after which, appropriate action will be taken to allow the assessment activity to continue.

**Procedure:** Vulnerability assessments to identify potential security vulnerabilities in an Agency's IT infrastructure are recommended and encouraged by the Commonwealth Office of Technology. However, prior notification of performing vulnerability scanning and/or penetration testing of KIH devices/infrastructure must be provided to the manager of the Commonwealth Office of Technology's Security Administration Branch (SAB) before such activity can commence.

A Vulnerability Assessment Notification form ([COT-F110](#)) must be fully completed and submitted to the SAB manager at least three (3) full business days prior to the assessment activities. The form must be

signed by the Agency's CIO or designated executive management and submitted to the Commonwealth Office of Technology's Security Administration Branch, 120 Glenn's Creek Drive, Frankfort, KY 40601. The form may be emailed without signature to the SAB Manager if an email originated by the Agency CIO or other designated executive management accompanies the form. Upon receipt of a completed Vulnerability Assessment Notification form, the Security Administration Branch will review the declared targets to ensure that they are not shared resources with any other agency.

If the Agency's vulnerability assessment activities are detected by COT's security and intrusion detection systems, the offending device may be blocked. This may temporarily suspend the Agency's assessment activities, and could possibly affect Agency services. In this case, the Agency will be required to open a Service Desk ticket by contacting the Commonwealth Office of Technology's Service Desk at 502.564.7576. COT will then unblock the activity in order for the assessment to resume.

If the assessment is to be scheduled after normal business hours, the Agency may request that COT staff be onsite to restore any affected services. This request should be included on the Notification form in the *Additional Information* section. Assessments performed after normal business hours without this specific support request may result in a significant delay to unblock devices, which were stopped by the Intrusion Detection System.

Upon receipt of the completed form, SAB will notify the contact person and CIO/Executive Management listed on the form via email as to the status of the request. Response time between SAB's receipt of the form and notification to the Agency should be no more than two (2) business days. The form will be assigned a tracking number and electronically stored in GOTSource along with associated correspondence. Appropriate COT staff will be made aware of the scheduled vulnerability assessment in order to field any inquiries concerning this activity and to arrange after hours staff availability onsite if necessary.

**References:**

- COT-F110, Vulnerability Assessment Notification form:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-298795/>

**\*\* END \*\***