

## Information Technology Services Division

<b>Vulnerability Assessment Methodology</b> <i>Policy Rescinded July 1, 2005</i>	<b>Document Number:</b> ITGS0011
	<b>Effective Date:</b> 03/25/04 <i>Rescinded July 1, 2005</i>
	<b>Published By:</b> Information Technology Services Division

### 1.0 Purpose

This assessment is intended to provide state agencies with a way to determine the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

### 2.0 Scope

Missouri State Agencies must annually complete a vulnerability assessment using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, Security Self-Assessment Guide for Information Technology Systems, and submit a completed copy to the Information Technology Services Division in the first quarter of the Fiscal year. Between October 1, 2004 and September 30, 2005, agencies must complete a vulnerability assessment on what they determine is their most critical system. As a guideline, agencies should determine this by evaluating what system they would want brought back up first in the event of a total disaster. Each agency may choose to perform the assessment themselves or contract with an independent 3<sup>rd</sup> party as identified by the established state of Missouri contracts.

Do not distribute the assessment based on public request. This assessment is exempt from public disclosure based on RSMo Chapter 610, Section 610.021 Sub-Paragraph (20) which states:

610.021 Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

- (20) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body.

### 3.0 Background

The National Institute of Standards and Technology (NIST) have issued a Vulnerability Self-Assessment Guide for Information Technology Systems. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which a group of interconnected systems can be tested and measured. Performing this assessment and mitigating any of the weaknesses found in the assessment is one way to determine if the system and the information are adequately secured.

### 4.0 References

- 4.1 Executive Orders
  - 03-26 Authorizes the OIT to coordinate information technology initiatives for the state  
[http://sos.mo.gov/library/reference/orders/2003/eo03\\_026.asp](http://sos.mo.gov/library/reference/orders/2003/eo03_026.asp)
  - 02-15 Establishes the Missouri Security Council  
[http://www.sos.mo.gov/library/reference/orders/2002/eo02\\_015.asp](http://www.sos.mo.gov/library/reference/orders/2002/eo02_015.asp)
  - 03-25 Designates OIT as principle forum to improve cyber security policies and procedures  
[http://sos.mo.gov/library/reference/orders/2003/eo03\\_025.asp](http://sos.mo.gov/library/reference/orders/2003/eo03_025.asp)
- 4.2 Cyber Security Committee Report
  - February 7, 2003
  - June 3, 2003
- 4.3 March 26, 2003 ITAB Meeting Minutes  
[http://oit.mo.gov/itab/minutes/ab\\_03\\_03.pdf](http://oit.mo.gov/itab/minutes/ab_03_03.pdf)
- 4.4 NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems  
<http://csrc.nist.gov/publications/nistpubs/index.html>
- 4.5 Security Assessment letter of Recommendation to CIO  
<http://oit.mo.gov/SecurityPolicyRecommendation.pdf>

### 5.0 Revision History

Date	Description of Change
03/25/2004	Initial Standard Published
02/18/2005	Due date changed from first quarter of calendar year to first quarter of Fiscal Year.... Between October 1, 2004 and September 30, 2005, agencies must complete a vulnerability assessment on what they determine is their most critical system. As a guideline, agencies should determine this by evaluating what system they would want brought back up first in the event of a total disaster.
06/08/2005	Policy Rescinded – Letter of recommendation from Tom Stokes and RD Porter to Dan Ross, CIO recommending Governance Standards ITGS0011 and

	ITGS0013 be rescinded. The Vulnerability Assessment Methodology and the Security Assessment Questionnaire will be replaced by a three step process outlined in the letter of recommendation. This letter may be accessed by clicking on the link in paragraph 4.5 above.
--	--

## 6.0 Definitions

Refer to ITAB Security Glossary and Acronyms:

<http://siipc.mo.gov/PortalVB/DesktopDefault.aspx?tabindex=7&tabid=8>

## 7.0 Distribution

This document will be distributed to the following:

Cabinet Members  
Elected Officials  
State Court Administrator  
Senate Administrator  
Chief Clerk

## 8.0 Inquiries

Direct inquiries about this document to:

Information Technology Services Division  
Truman Building, Room 280  
301 W. High Street  
Jefferson City, MO 65102  
Voice: 573-526-7741  
FAX: 573-526-0132