University of Tennessee Institute of Agriculture: UTIA IT0124P2 – Vulnerability Assessment Procedures	
Version: 3.0	Effective Date: November 18, 2016

Objective:
To ensure compliance with the Vulnerability Scanning section of UTIA IT0124 - Information Technology Risk Assessment Plan, certain University of Tennessee Institute of Agriculture (UTIA or Institute) systems will be subject to routine vulnerability assessments. Vulnerability assessments will consist of identifying networked assets, scanning for vulnerabilities and potential vulnerabilities, and remediation of vulnerabilities.

Scope:
These procedures apply to all Institute-owned IT assets classified as moderate, high, or business critical. All users of these IT assets are required to be familiar with and comply with these procedures.

Procedures:
The Institute's Chief Information Security Officer (UTIA CISO) will initiate the vulnerability scans on a monthly basis during a time that will not affect normal network operations. These scans will be run using Qualys Enterprise Suite.

The UTIA CISO will produce a full report for each system that has been scanned. The report will include all vulnerabilities and potential vulnerabilities associated with the system. The report will also include pertinent information such as the actual threat, impact, and suggested solution. The report will be sent via UT's Secure Courier (Vault) email system to the information system owner (i.e., system administrator). The information system owner will review the report and complete remediation of vulnerabilities, including potential vulnerabilities, based on the level as outlined below:

Vulnerability & Potential Vulnerability Level	Time Frame for Remediation
5 - Urgent	Immediately
4 - Critical	Within 7 days
3 - Serious	Within 30 days
2 - Medium	Within 90 days
1 - Minimal	Within 90 days

Each information system owner will confirm the successful completion of the remediation steps and notify, in writing, the UTIA CISO of completion. The UTIA CISO will run a new vulnerability scan on the system(s) to verify remediation of vulnerabilities. This procedure will continue until all vulnerabilities are remediated and verified by the UTIA CISO.

Should the information system owner believe that a reported vulnerability is actually a false positive, they are required to read UTIA IT0302 - Information Technology Formal Exception Plan**, then submit an exception request, if applicable**, explaining the false positive belief**.** In addition, if there is a valid business reason the information system owner cannot remediate a vulnerability, they are required to read UTIA IT0302 - Information Technology Formal Exception Plan, and submit an exception request detailing the risk and the plan for risk mitigation. There must be one request submitted per system owned.

References:

UTIA Glossary of Information Security Terms
UTIA IT0124 – Information Technology Risk Assessment Plan
UTIA IT0124P1 – Information Technology Risk Assessment Procedures
UT Policy IT0124 – Risk Assessment
UTIA IT0302 - Information Technology Formal Exception Plan

For more information, contact Sandy Lindsey, UTIA CISO, at (865) 974-7292, or email sandy@tennessee.edu.