Network Scanning, Evaluation and Remediation Process

AMAS Evaluation Process – Scans are performed on a selected sub-net basis remotely from on campus, from off campus, and in some cases from within the administrator's network. Vulnerabilities are cross-checked using the scan outputs from the various tools and manual verification. False positives are excluded from reporting. Scanning results are documented, consolidated and reviewed to determine if vulnerabilities identified are valid. Once validated, vulnerabilities are reported and discussed with the network administrator on a relative risk basis (critical/high/medium/low).

Remediation Process – Reported vulnerabilities are considered and evaluated further by the network administrator and AMAS, on a relative risk basis. If the administrator has a remediation plan to mitigate the risk, it is noted. In the event that AMAS and the network administrator do not concur on the risk assessment and the remediation, AMAS reserves the right to elevate the decision to unit management. After network administrator correct significant security threats, AMAS will re-scan to validate that corrective actions have been implemented, either during the audit or during subsequent audit follow-up procedures.

Network Scanning Tools

1. NMap scans – Nmap (Network Mapper") is a free open source utility for network exploration or security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap is free software available with full source code. Nmap is a starting point in the vulnerability assessment and helps lay the groundwork for the more sophisticated scanning tools.

2. Nessus – Nessus is a proprietary vulnerability assessment tool produced by Tenable Network Security Inc. that identifies known security vulnerabilities and assists in prioritizing (risk-ranking) threats for remediation. The tool is designed to perform fast, non-intrusive scanning technology that incorporates a current and comprehensive vulnerability database. Nessus helps inforce internal security policies and standards through custom policy audits. Nessus delivers a comprehensive report that details all vulnerabilities and recommends the appropriate corrective actions and fixes.

3. WebInspect – WebInspect by HP is a proprietary web application security assessment scanning tool used to identify vulnerabilities within the web application layer. WebInspect also helps check that a web server is configured properly and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and others. It can assess a web service by discovering all XML input parameters and performing parameter manipulation on each XML field looking for vulnerabilities within the service itself. WebInspect delivers reports that detail all

vulnerabilities found and recommends the appropriate corrective actions and fixes. WebInspect can be configured in a number of ways. AMAS scanning criteria are currently limited to top ten Open Web Application Security Program (OWASP) vulnerabilities. Detailed application program code scanning, while functionally available, has not been conducted to date due to resource constraints.