STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

March 24, 2010

The Honorable Judy Burges, Chair
Joint Legislative Audit Committee

The Honorable Thayer Verschoor, Vice Chair
Joint Legislative Audit Committee

Dear Representative Burges and Senator Verschoor:

Our Office has recently completed an 18-month followup of the University of Arizona (UA) regarding the implementation status of the 13 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in June 2008 (Arizona's Universities—Information Technology Security, Auditor General Report No. 08-04). As the attached grid indicates:

- 8 have been implemented;
- 4 are in the process of being implemented; and
- 1 is substantially implemented.

Unless otherwise directed by the Joint Legislative Audit Committee, this concludes our follow-up work on UA's efforts to implement the recommendations from the June 2008 performance audit report.

Sincerely,

Melanie M. Chesney, Director
Performance Audit Division

MMC:sjs
Attachment

cc: Joel Sideman, Executive Director, Arizona Board of Regents
Floyd Roman, Assistant Comptroller, University of Arizona
Michele Norin, Chief Information Technology Officer, University of Arizona

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

ARIZONA'S UNIVERSITIES—
INFORMATION TECHNOLOGY SECURITY
For University of Arizona
Auditor General Report No. 08-04
18-Month Follow-Up Report

Recommendation	Status/Additional Explanation

Finding 1: Universities need to improve Web-based application security

1.1 ASU, UA, and NAU should:

a. Develop and implement a plan for conducting regular security assessments of their Web-based applications. This plan should include:
- Creating and regularly updating an inventory of Web-based applications and determining the criticality of the applications and the data processed.
- Developing and implementing procedures for regularly conducting security reviews that assess whether security requirements and controls are functioning effectively.
- Remediating, based on risk, the problems identified during these security reviews.

Implementation in Process
UA has developed procedures for conducting regular security assessments of its Web-based applications and remediating problems identified during those assessments, and is in the process of implementing the assessments.

b. Enhance or develop and implement university-wide standards or procedures for updating and maintaining their Web servers. The standards or procedures should include:
- Developing a method for identifying relevant, widely known Web server vulnerabilities.
- Creating a timeline for reacting to notifications of newly discovered Web server vulnerabilities.
- Developing a process for determining whether to apply a software update, establish another control to address the Web server vulnerability, or accept the risk of not updating the software.

Implemented at 12 Months

c. Establish and implement a set of university-wide standards for developing secure Web-based applications. These standards should encompass all phases of development and include:
- Gathering security requirements.
- Developing a set of up-to-date secure coding standards or conventions.
- Using threat modeling exercises during development.
- Performing security testing before releasing an application to the live environment.

Implementation in Process
UA has established a standard for developing secure applications that requires threat modeling exercises and testing before releasing applications to the live environment. However, UA is still in the process of implementing this standard.

Recommendation	Status/Additional Explanation
d. Provide guidance and training to Web developers on secure Web-based development practices as part of a wider security awareness education and training effort.	**Implementation in Process** UA is in the process of developing mandatory training modules, which will include training on secure coding for Web developers, and expects to have the modules completed by June 30, 2010.
e. Work with the Board's Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.	**Implemented at 12 Months**

Finding 2: Universities need to develop comprehensive IT security programs

2.1 ASU, UA, and NAU should:

a. Seek additional opportunities while implementing their information security programs to ensure that their ISOs' authority is communicated and understood university-wide.	**Implemented at 12 Months**
b. Take additional steps to establish a university-wide security awareness education and training program that is in line with IT standards, including requiring security awareness education and training for all users and gearing it toward their functions.	**Substantially Implemented at 18 Months** The universities have taken significant steps toward establishing a university-wide security awareness education and training program that is in line with IT standards, including requiring security awareness education and training for all users and gearing it toward their functions. However, the universities have indicated that they are having trouble finding a way to make IT security awareness training mandatory for students, and there are probably some students who do not receive IT security training, such as transfer students or students enrolled only in on-line classes. The universities have also indicated that they intend to continue to identify ways to address this issue. For example, UA held a security awareness session for incoming students during the 2009 summer orientation and is developing a new employee training and a refresher training to meet UA's standard on management responsibilities for information security.
c. Determine their resource needs for implementing a formal information security program. In doing so, they should assess whether they internally have the resources needed to develop and implement their programs, or whether they need to develop a request for additional funding.	**Implemented at 12 Months**

Recommendation	Status/Additional Explanation
d. Continue to develop and implement plans for monitoring information security program compliance.	**Implementation in Process** According to UA, it will monitor compliance with the information security program through the use of risk assessments and network vulnerability, and Web application scanning. UA has developed and implemented a risk assessment process; however, it is still developing and implementing network vulnerability and Web application scanning.
e. Work with the Board's Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.	**Implemented at 12 Months**
2.2 Not applicable to UA.	
2.3 UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by.	
a. Improving its university-wide data classification procedures to require that classifications be regularly reviewed and updated, and then approving and implementing the procedures.	**Implemented at 12 Months**
b. Continuing its efforts to develop and implement risk assessment procedures that are in line with IT standards and best practices	**Implemented at 18 Months**
c. Ensuring that its incident handling documents include all key requirements outlined in IT standards and best practices, and that the information within these documents is consistent.	**Implemented at 12 Months**
2.4 Not applicable to UA.	