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 Northern Arizona University (NAU) 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:

- 12 have been implemented, and
- 1 is substantially implemented.

Unless otherwise directed by the Joint Legislative Audit Committee, this concludes our follow-up work on NAU'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
MJ McMahon, Executive Vice President and Interim Vice President, Administration/Finance, Northern Arizona University
Fred Estrella, Chief Information Technology Officer, Northern Arizona University

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

ARIZONA'S UNIVERSITIES—
INFORMATION TECHNOLOGY SECURITY
For Northern Arizona University
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.

Implemented at 12 Months

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.

Implemented at 12 Months

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.	**Implemented at 6 Months**
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 6 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, although not mandatory, NAU enrolls all students in a technology class that addresses security awareness.
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 6 Months**
d. Continue to develop and implement plans for monitoring information security program	**Implemented at 18 Months**

Recommendation	Status/Additional Explanation
compliance.	
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 NAU.	
2.3 Not applicable to NAU.	
2.4 NAU should continue with its efforts to implement an information security program that is in line with IT standards and best practices by.	
a. Developing and implementing a documented university-wide data classification process in line with IT standards and best practices, such as protecting the information based on confidentiality, and developing an inventory of its data classification that is updated regularly.	**Implemented at 12 Months**
b. Developing and implementing university-wide risk assessment procedures in line with IT standards and best practices.	**Implemented at 12 Months**
c. Approving and implementing its incident response policy, guidelines, and flowcharts.	**Implemented at 12 Months**