ASU
ARIZONA STATE UNIVERSITY

June 11, 2008

Debbie Davenport
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

On behalf of Arizona State University (ASU), I am pleased to respond to the performance audit regarding the Information Technology Security Program at ASU. ASU is in agreement with your recommendations and responses specific to your recommendations are enclosed. The report represents a thoughtful analysis of the ASU Information Technology Security Program.

ASU is very appreciative of the professional manner in which the audit was performed. We are always seeking to identify new and better ways to improve our programs and operations. The implementation of your recommendations will meaningfully enhance the Information Technology Security Program at ASU.

Sincerely,

Michael M. Crow
President

MMC:dq
/c

Enclosure

c: Adrian Sannier, Vice President, University Technology Officer
Carol Campbell, Executive Vice President and CFO

Response From Arizona State University

To the Auditor General's Report on

Information Technology Security

FINDING 1

1. ASU, UA, and NAU should:

   a) Develop and implement a plan for conducting regular security assessments of their Web-based applications.

   RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

   STATUS: ASU is actively developing a comprehensive strategy for assessing Web-based applications. In addition to collaborating with NAU and UA to deploy a common assessment tool set, ASU is leveraging industry standard methodologies for assessment around Web development and development in general practices and procedures.

   b) Enhance or develop and implement University-wide standards or procedures for updating and maintaining their Web servers.

   RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

   STATUS: ASU has created standards and procedures based on its Web-based applications. Implementation of these standards will be done in conjunction with training around secure coding practices. ASU's approach is to first create standards on the Operating System (OS), all Web browsers, and application servers, to be followed by development and maintenance standards for its Web applications and Java 2 Platform Enterprise Edition (J2EE) Web applications. To update and maintain Web servers, ASU and UTO will create procedures on best practices to support the recommendation.

   c) Establish and implement a set of University-wide standards for developing secure Web-based applications. These standards should encompass all phases of development.

   RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

   STATUS: ASU is implementing standards for Secure Software Development Lifecycles (SDLC) that will address all Web-based applications. ASU is focusing its initial implementation on its most critical enterprise systems. ASU will then apply these same standards University-wide.

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.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: As part of ASU awareness and training, ASU is identifying mandatory training collateral that will be useful in training its Web-developer community. This material will be generally available beginning in Fall 09.

e) Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU has and will continue to work with the Arizona Board of Regents Technology Oversight Committee to report on all of its technology activities, including those related to information security.

FINDING 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.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU continues to articulate the role of the ISO through its various committees and counsels and the role and responsibilities of the ISO across the University.

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.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU has defined and is preparing to implement a University-wide awareness and training program. The “Get Protected” campaign is interactive and includes user-specific, mandatory courses on training and awareness education.

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.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU initially specified (3) FTEs and has currently filled one of these positions. ASU has also defined a budget for FY09 for resources, systems, applications, and awareness and will begin to track and manage expenditures for security program efforts.

d) Continue to develop and implement plans for monitoring information security program compliance.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU’s Information Security Office is engaged with ASU’s Internal Audit team to develop and implement a program compliance plan. Over time, this responsibility will reside within the ISO’s Office.

e) Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

RESPONSE: ASU agrees with this finding of the Auditor General and is taking steps to implement it.

STATUS: ASU has and will continue to work with the Arizona Board of Regents Technology Oversight Committee to report on all of its technology activities, including those related to information security.

2. ASU should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by:

a) Obtaining approval for its Information Security Policy and Information Security and Privacy Strategic plan, and then disseminating and communicating this policy to all appropriate individuals.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU is currently working with various committees and entities within the University to obtain approval for its draft Information Security Policy and Privacy Strategic plan.

b) Improving and implementing University-wide data classification procedures that are in line with IT standards and best practices, such as creating an inventory.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU has begun a data classification investigation that will identify what types of data exist within the University systems and help focus security efforts on the most sensitive areas. In addition, there is an overall standard for data classification and management that is currently under review, as well as a set of best practices and procedures for protecting data of various classifications.

c) Obtaining approval for its risk assessment standard and continuing with its plans to develop and implement a risk assessment process standard.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU has completed its initial risk assessment and has developed a schedule and plan for future assessments. ASU's ISO will leverage the Internal Auditing group to provide the initial functionality until the Information Security Office has established its own capability.

d) Approving and implementing its incident response plan.

RESPONSE: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

STATUS: ASU has created and corrected issues within its Incident Response Plan and is working to ensure that it is maintained, updated, and evaluated on a consistent level.

THE UNIVERSITY OF ARIZONA®

Office of the President

Administration Building, Room 712
1401 E. University Boulevard
P.O. Box 210066
Tucson, AZ 85721-0066
Tel: (520) 621-5511
Fax: (520) 621-9323

June 13, 2008

FEDEX AIRBILL NUMBER 7920 7072 2217

Debra K. Davenport, CPA
Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Re: The University of Arizona

Dear Ms. Davenport:

Thank you for the opportunity to respond to the report issued in connection with the performance audit of information technology security at The University of Arizona (UA). We appreciate the professional approach of the auditors during their review. The purpose of this letter is to forward UA's written responses to the report.

UA's five-year information technology strategic plan identifies information technology security as a priority. Many improvements have been implemented. We welcomed the Auditor General's review as a means to enhance and refine our efforts.

UA agrees with the findings in the report and has implemented or plans to implement the recommendations as described in the accompanying report.

Sincerely,

Robert N. Shelton
President

RNS/slh

c: Michele Norin, Chief Information Officer and
Executive Officer for University Information Technology Services
Floyd Roman, Assistant Comptroller, Financial Management,
Financial Services Office
Sylvia Johnson, University Information Security Officer

THE UNIVERSITY OF ARIZONA RESPONSE TO INFORMATION TECHNOLOGY SECURITY PERFORMANCE AUDIT REPORT

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

Finding 1, Recommendation 1a:

UA should develop and implement a plan for conducting regular security assessments of its 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.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

UA's plan for conducting regular security assessments of Web-based applications is as follows:

- UA will inventory Web-based applications and the data processed and determine their criticality as part of UA's risk assessment process at least every three years.
- UA, ASU and NAU are in the process of acquiring Web application and network vulnerability scanning tools.
- UA central security staff will attend vendor-provided training covering all aspects of the scanning tools.
- Following completion of the vendor training, central security staff will begin training UA system administrators.
- Following completion of the vendor training, UA central security and UA IT staff will begin use of the tools to identify Web servers and assess security of Web-based applications.
- UA will develop and implement a procedure for regular security reviews and remediation of identified problems.

Finding 1, Recommendation 1b:

UA should enhance or develop and implement university-wide standards or procedures for updating and maintaining its 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.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

UA will use network vulnerability tools to identify Web server vulnerabilities on an ongoing basis.

UA will develop and implement a procedure that reinforces its Server Security Standard by identifying a method for identifying relevant, widely known Web server vulnerabilities, creating a timeline for reacting to notifications of newly discovered Web server vulnerabilities, and describing a process for determining whether to apply a software update, establish a compensating control, or accept the risk of not updating the software.

.

Finding 1, Recommendation 1c:

UA should 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.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

UA will establish and implement a set of university-wide standards for developing secure Web-based applications.

Finding 1, Recommendation 1d:

UA should provide guidance and training to Web developers on secure Web-based development practices as part of a wider security awareness education and training effort.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

The Information Security Office will continue to enhance the information for application developers currently available on its website.

UA will provide training for a number of its Web developers. Following completion of the training, trained Web developers will develop a sustainable training program for other UA Web developers.

Finding 1, Recommendation 1e:

UA should work with the Arizona Board of Regents' Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report its implementation efforts.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Finding 2 – Universities need to develop comprehensive IT security programs

Finding 2, Recommendation 1a:

UA should seek additional opportunities while implementing its information security program to ensure that its ISO's authority is communicated and understood university-wide.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

In addition to steps already being taken, UA's ISO will:

- Establish an information security advisory committee, as required by the ABOR Information Security Policy, and periodically report to the Faculty Senate Executive Committee.
- Seek additional opportunities to meet with a variety of UA organizations.

Finding 2, Recommendation 1b:

UA should 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.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

The Information Security Office will continue to identify needs for training. Current efforts include:

- Planning the Information Security Office's sixth annual awareness event, with tracks for all types of users
- Development of new employee and refresher training to meet the mandate of UA's Standard on Management Responsibilities for Information Security
- Presentation of internal firewall implementation and management training sessions geared toward system administrators in May 2008, with the video version available on the Information Security Office website by July 2008
- Delivery of awareness education to over 6,000 incoming freshmen through new student orientation
- Delivery of awareness presentations to classes attended by one-third of UA's freshman class

Finding 2, Recommendation 1c:

UA should determine its resource needs for implementing a formal information security program. In doing so, it should assess whether it internally has the resources needed to develop and implement its program, or whether it needs to develop a request for additional funding.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

UA will determine whether it has the internal resources needed to develop and implement its program over the next six months and, if it determines that it does not, will develop a request for additional funding. In making such a determination, UA will take into consideration the timelines developed in conjunction with the Arizona Board of Regents' Technology Oversight Committee, as described below.

Thereafter, any additional need for funding will be articulated in the information security program plan submitted annually to ABOR in accordance with the ABOR Information Security Policy.

Finding 2, Recommendation 1d:

UA should continue to develop and implement plans for monitoring information security program compliance.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Compliance will be monitored as part of the risk assessment process and by means of network vulnerability and Web application scanning.

Finding 2, Recommendation 1e:

UA should work with the Arizona Board of Regents' Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report its implementation efforts.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Finding 2, Recommendation 3a:

UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by improving its university-wide data classification procedures to require that classifications be regularly reviewed and updated, and then approving and implementing the procedures.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

The data classification procedures will be revised by December 2008 to require the regular review and update of classifications. Approval of the procedures will be sought immediately after their revision.

Finding 2, Recommendation 3b:

UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by continuing its efforts to develop and implement risk assessment procedures that are in line with IT standards and best practices.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

The Information Security Office will continue efforts to develop and implement university-wide risk assessment procedures in line with IT standards and best practices by July 2009.

Finding 2, Recommendation 3c:

UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by 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.

UA Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

The Incident Handling Standard and the Incident Handling Guideline have been implemented and have been available on UA's website since May 2006. Since their publication, the reporting of incidents at UA has increased significantly. UA will continue its efforts to raise awareness of information security matters, including the Incident Handling Standard and the Incident Handling Guideline.

UA's incident handling documents will be revised by December 2008 to:

- Ensure consistency
- Identify roles and responsibilities
- Incorporate additional detail on how to investigate or contain and recover from or follow up on incidents

NORTHERN
ARIZONA
UNIVERSITY

Office of the President

Northern Arizona University
PO Box 4092
Flagstaff, AZ 86011-4092

928-523-3232
928-523-1848 fax
nau.edu/president

June 11, 2008

Ms. Debra Davenport
Auditor General
State of Arizona
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

We have received the Auditor General's report on information technology security at the three state universities. Northern Arizona University has no significant issues or concerns with the report.

Attached is Northern Arizona University's response. The audit recommendations will be implemented.

Sincerely,

John D. Haeger
President

Northern Arizona University
Auditor General's Performance Audit
Information Technology Security
June 2008

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

Recommendation a.

Develop and implement a plan for conducting regular security assessments of their Web-based applications

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. One of the primary responsibilities of the Information Security Analyst, Sr. position is to manage the security assessment program at NAU. Additionally, the Arizona Board of Regents Technology Oversight Committee approved funding for a suite of software applications to be used in the regular assessment of Web-based applications.

Recommendation b.

Enhance or develop and implement university-wide standards or procedures for updating and maintaining their Web servers.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. A university-wide standard or procedures for updating and maintaining web-servers will be developed and implemented.

Recommendation c.

Establish and implement a set of university-wide standards for developing secure Web-based applications.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. Information Technology Services has begun prototyping and testing a software development lifecycle standard. As this prototype matures it will be tested by others responsible for developing web-based applications on the campus. After it has been thoroughly reviewed it will be distributed as a university-wide standard.

Recommendation 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.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

The first training for secure web-based development practices was held on May 20-May 23. This training was attended by twenty core web-application developers. The core developers receiving this training will be used in a train-the-trainer type effort to structure future training opportunities for the campus.

Additionally, on-going guidance will be developed and distributed to campus-wide web-application developers based on the standards developed in response to Recommendation c and updates to best practices in web-application development.

Recommendation e.

Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The NAU Director of Information Security will work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and providing progress reports.

Finding 2 - Universities need to develop comprehensive IT security programs

Recommendation 1a.

Seek additional opportunities while implementing their information security programs to ensure that their ISO's authority is communicated and understood university-wide.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The Director of Information Security will work with the NAU Information Security Committee to identify campus organizations for targeted awareness efforts to this effect.

Recommendation 1b.

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.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Work has begun in coordination with the Director of Human Resources and the NAU Training Coordinator to gain approval for a suite of mandatory training for faculty, staff, and students at NAU.

An annual schedule for training and awareness has been developed and presented to the NAU Information Security Committee. The first monthly training was held on April 23 and awareness articles were included in the ITS newsletter.

The Information Security Awareness coordinator at the University of Arizona has been contacted to begin arranging for the purchase of professional security awareness materials to be distributed at NAU.

Recommendation 1c.

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.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The approved NAU Information Security Program calls for an annual risk assessment to be conducted. One aspect of the risk analysis is an assessment of resources needed to mitigate risks. This assessment will be completed this fall per the Program, and will assess whether there are enough internal resources to develop and implement the program, or whether a request for additional funding is required.

Recommendation 1d.

Continue to develop and implement plans for monitoring information security program compliance.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. A plan for monitoring compliance with the information security program will be developed and implemented.

Recommendation 1e.

Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The NAU Director of Information Security will work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and providing progress reports.

Recommendation 4.

NAU should continue its efforts to implement an information security program that is in line with IT standards and best practices by:

Recommendation 4a.

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.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. A university-wide data classification process will be developed and implemented.

Recommendation 4b.

Developing and implementing university-wide risk assessment procedures in line with IT standards and best practices.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. An initial inventory and assessment was conducted in 2007. Part of that assessment lead to the approval of the NAU Information Security Program. The Program calls for an annual risk assessment to be completed each fall. A draft risk assessment strategy has been developed and will provide the foundation for these assessments.

Recommendation 4c.

Approving and implementing its incident response policy, guidelines, and flowcharts.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The incident response policy, guidelines, and flowcharts are being reviewed and approval will be sought for their campus-wide implementation.

ARIZONA
BOARD OF
Regents

Arizona Board of Regents
2020 North Central Avenue, Suite 230
Phoenix, AZ 85004-4593
602-229-2500
Fax 602-229-2555
www.azregents.edu

Arizona State University ***Northern Arizona University*** ***University of Arizona***

June 13, 2008

Ms. Debra Davenport
Auditor General
State of Arizona
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

Thank you for the opportunity to review the revised preliminary performance audit report of information technology security at the Arizona public universities.

We appreciate the professionalism of your staff and their responsiveness to our earlier comments.

While the report does not include any specific recommendations directed to the Arizona Board of Regents, we will work with the Board and the universities to ensure progress in implementing the recommendations directed to the universities.

Sincerely,

Joel Sideman
Executive Director

c:
Regent Fred Boice
Art Ashton
Rick Gfeller