2020 N. Central Avenue, Suite 230
Phoenix, Arizona 85004
P 602.229.2500
F 602.229.2555
AZRegents.edu

BOARD OF Regents ARIZONA'S PUBLIC UNIVERSITIES
EDUCATE · DISCOVER · IMPACT

June 18, 2018

Lindsey Perry
Auditor General
2910 N. 44th Street
Phoenix, AZ 85018

Dear Auditor General Perry:

On behalf of the Arizona Board of Regents, I am pleased to respond to the audit report, Arizona's Universities – Information Technology Security. First, let me thank you and your audit team for their utmost professionalism and integrity in reviewing our practices and in developing their findings. They are thoughtful and represent months of collaborative work.

The findings are agreed to and the audit recommendations will be implemented.

The regents will not only work to implement our findings, but will also monitor the implementation of the university specific findings. We are constantly looking for ways to improve and appreciate your help in that endeavor.

Sincerely,

John Arnold
Interim Managing Director

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1 – 1.5: Not applicable to ABOR.

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1 – 2.3: Not applicable to ABOR.

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1 – 3.3: Not applicable to ABOR.

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1 – 4.12: Not applicable to ABOR.

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: ABOR should work with the universities to develop and implement a comprehensive plan for expanding its governance and oversight of the universities' IT security practices. As part of expanding its efforts in this area, ABOR should consider implementing additional oversight practices recommended for governing boards, including:

Recommendation 5.1a: Requiring the universities to monitor and regularly report to ABOR on IT security program effectiveness;

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

Recommendation 5.1b: Requiring each university's annual audit plan to include an IT security component, such as audits of specific IT security controls or processes, including reporting audit results to ABOR; and

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

Recommendation 5.1c: Reviewing the results of the universities' IT risk assessments.

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

ARIZONA STATE UNIVERSITY

June 18, 2018

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

Dear Ms. Perry:

On behalf of Arizona State University (ASU), I am pleased to respond to the performance audit of Information Technology Security at ASU. We are in agreement with all of your findings and our responses to your recommendations are enclosed.

My staff and I wish to thank you and your staff for the professional manner in which this audit was performed. We are constantly looking for ways to improve our program and operations.

Sincerely,

Michael M. Crow
President

Enclosure

cc: Mark Searle, Executive Vice President and University Provost
Morgan R. Olsen, Executive Vice President and CFO

OFFICE OF THE PRESIDENT
FULTON CENTER 410, 300 E. UNIVERSITY DRIVE
PO BOX 877705 TEMPE, AZ 85287-7705
(480) 965-5253 FAX: (480) 965-0865
HTTP://PRESIDENT.ASU.EDU

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1: ASU should develop and implement written policies and procedures that:

Recommendation 1.1a: Specify roles and responsibilities for monitoring employee compliance with security awareness training;

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

Response explanation: ASU added the annual training requirement that was documented in the New Employee Orientation Guidance to our existing Information Security Policy and created a Security Awareness Compliance Procedure that includes roles and responsibilities for monitoring employee compliance with security awareness training. This was completed May 2018.

Recommendation 1.1b: Include a requirement for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so;

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

Response explanation: The security awareness training completion rate included in the report is as of March 2018 and represents an in-process training campaign. Security awareness training is tracked on an annual basis with training required to be complete by June 30, 2018. ASU created a Security Awareness Compliance Procedure that includes a requirement for regularly using the ASU training dashboard to review employees' completion and to report noncompliance to the Accountable Administrator. This was completed May 2018.

Recommendation 1.1c: Specify requirements for following up with employees who have not completed the required training; and

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

Response explanation: ASU created a Security Awareness Compliance Procedure that includes a requirement for following up with employees who have not completed the required training. This was completed May 2018.

Recommendation 1.1d: Identify potential consequences to employees for not completing required security awareness training within specified time frames, such as warnings and revoked access.

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

Response explanation: Potential consequences are included under the Violations and Enforcement section of the Information Security Policy. This was completed April 2018.

Recommendation 1.2 – 1.5: Not applicable to ASU.

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1: ASU should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

Recommendation 2.1a: Developing and implementing additional written policies and procedures for its vulnerability management process that include requirements and/or guidance for:

- Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual units are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;
- Sharing scan results across the university to help eliminate similar vulnerabilities in other IT systems;
- Conducting penetration testing at specified frequencies based on risk;
- Using its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and
- Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

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

Response explanation: ASU has a long-standing commitment to vulnerability remediation training, including a bi-weekly training session for vulnerability management, and will incorporate sharing remediation techniques for common vulnerabilities into this training agenda. ASU will update its existing Web Application Vulnerability Standard to address penetration testing. Additionally, ASU is creating a separate Network Vulnerability Standard that will include the network recommendations suggested by audit

to improve the regular scanning process of ASU's network. The expected completion date is July 2018.

Recommendation 2.1b: Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

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

Response explanation: ASU has a Server Security Standard and detailed endpoint security guidelines in place today and will supplement this documentation with additional detailed configuration best practices for network-attached devices. This documentation is scheduled to be reviewed and updated annually. ASU continues to investigate endpoint management tools to reduce further vulnerabilities stemming from inappropriate configurations. The expected completion date for new documentation is July 2018.

Recommendation 2.1c: Developing and implementing additional patch management policies and procedures to include guidance on how its staff should identify system flaws requiring patches and requirements for reporting those flaws to appropriate individuals for remediation.

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

Response explanation: ASU has a Patch Management Standard in place today. We will incorporate additional guidance in utilizing patching documentation available for reference in identifying known issues as part of the vulnerability management best practices. The expected completion date for new documentation is July 2018.

Recommendation 2.1d: Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Using secure coding standards when developing web applications;
- Requiring web application developers to be trained on developing secure software;
- Reviewing web application source code before web applications are released; and
- Performing security testing before web applications are released.

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: ASU currently requires these activities for all web applications with a criticality rating of High and Medium and recommends this activity for the Low criticality ratings. ASU will formalize its existing ad hoc training program in place today and implement a program to provide annual training for developers who administer web applications with a criticality rating of High or Medium. The expected availability for the new training is January 2019.

Recommendation 2.1e: Developing and implementing policies and procedures for protecting system logs from unauthorized access, modification, and deletion.

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

Response explanation: ASU has a System Audit Standard that currently requires logging to use a tamper-resistant mechanism. ASU will strengthen the language to clarify log management where separation of duties is a factor. In addition, ASU continues to recommend centralized logging via our enterprise logging solution that is currently available. The expected completion date for the revised standard is July 2018.

Recommendation 2.1f: Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

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

Response explanation: This spring ASU implemented a process to provide executive dashboard review with all Accountable Administrators. We have updated our risk assessment standard to document this new process. We also will continue to require expanded centralized logs for critical systems which allows visibility and stronger centralized oversight.

Recommendation 2.2 – 2.3: Not applicable to ASU.

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1 – 3.2: Not applicable to ASU.

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1: ASU should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified.

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: ASU's current Secure Development Standard requires a centralized inventory for High and Medium Criticality-rated systems. ASU will continue to centrally maintain this ASU-wide inventory and additionally recommend that departments and units include Low criticality systems. The inventory will include the required data elements – data classification, data owner and data description. During the ASU-wide annual review of High and Medium criticality systems, next scheduled January 2019, ASU will reinforce that departments must maintain their inventory. The revised standard is expected to be released by July 2018.

Recommendation 4.2: ASU should:

Recommendation 4.2a: Establish time frames and guidance for regularly reviewing and updating data inventories; and

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: See Recommendation 4.1 response.

Recommendation 4.2b: Develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: See Recommendation 4.1 response.

Recommendation 4.3 – 4.12: Not applicable to ASU.

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: Not applicable to ASU.

NORTHERN ARIZONA UNIVERSITY | Office of the President

nau.edu/president
presidentsofficesupport@nau.edu

928-523-3232 office
928-523-1848 fax
P.O. Box 4092
Flagstaff, AZ 86011

June 18, 2018

Lindsey Perry
Auditor General
Office of the Auditor General
2910 N. 44th Street, Suite 410
Phoenix, AZ 85018

RE: Response to Auditor General's Report on Arizona's public universities' information technology security

Dear Ms. Perry:

This letter provides Northern Arizona University's response to the Audit Report on the universities' information technology security.

Information security resources impact nearly every aspect of the NAU mission, vision, and values and as such, protection of those resources is important to NAU. This audit reaffirms the work NAU has already accomplished to develop and implement strong IT security policies, procedures, and practices. This audit also identifies opportunities where we can apply the same practices more specifically to other information security goal and objective areas. We appreciate this Office of the Auditor General feedback as we strive to further enhance our efforts to improve our information security posture, ensure our students' success, and help advance Arizona's educational attainment levels.

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1: Not applicable to NAU.

Recommendation 1.2: NAU should finish developing and implement its draft security awareness training policies and procedures, including adding requirements for regularly using an automated tracking system for analyzing all employees' security awareness training

completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its draft security awareness training policies and procedures.

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

Response explanation: NAU has completed the development and implementation of its security awareness training policy and procedures. This includes the requirements for tracking and reporting on completion, reporting (via email) noncompliance, and establishing time frames for compliance. This was completed in June 2018.

Recommendation 1.3: NAU should specify a time frame for new employees to complete initial security awareness training within its policies and procedures.

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

Response explanation: NAU specifies a time frame for new employees to complete initial security awareness training within its policy and procedures. The policy states new employees shall complete the training within sixty (60) days. This was completed in June 2018.

Recommendation 1.4 – 1.5: Not applicable to NAU.

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1: Not applicable to NAU.

Recommendation 2.2: NAU should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

Recommendation 2.2a: Finishing development of and implementing its draft policies and procedures establishing a vulnerability scanning process.

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

Response explanation: NAU will complete the development and implementation of its policies and procedures establishing a vulnerability scanning process.

Recommendation 2.2b: Developing and implementing additional written university-wide policies and procedures for penetration testing that include:

- Requirements for conducting penetration testing at specified frequencies based on risk.
- Guidance for its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for

conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and

- Guidance for helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all higher-risk web applications.

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

Response explanation: NAU will develop and implement written university-wide policies and procedures for penetration testing that includes industry best practices.

Recommendation 2.2c: Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

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

Response explanation: NAU will develop and implement revised configuration management policies and procedures that include IT standards and best practices.

Recommendation 2.2d: Revising its configuration management policies and procedures to indicate that they apply to all NAU IT systems.

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

Response explanation: NAU will revise configuration management policies and procedures to indicate that they apply to all NAU IT systems.

Recommendation 2.2e: Finishing development of and implementing its draft patch management policies and procedures.

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

Response explanation: NAU will complete the development and implementation of patch management policies and procedures.

Recommendation 2.2f: Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Gathering web application security requirements when developing web applications;

- Using secure coding standards when developing web applications;
- Requiring web application developers to be trained on developing secure software;
- Conducting threat modeling during web application development or security testing before releasing web applications to the live environment;
- Reviewing web application source code for web applications it develops internally before these web applications are released; and
- Performing security testing before web applications are released.

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

Response explanation: NAU will develop and implement additional web application development policies and procedures that include IT standards and best practices.

Recommendation 2.2g: Developing and implementing written log monitoring policies and procedures that:

- Describe the critical IT systems and functions within each IT system that should be logged;
- Specify how frequently each log should be monitored;
- Identify who is responsible for ensuring log events are captured and reviewing log events on a regular basis;
- Require analysis of security-related information generated by log monitoring across the university to determine any patterns that might indicate a potential attack;
- Outline standard response actions for specific types of detected events, including informing designated personnel of security risks to the university and to individual IT systems; and
- Include requirements for securely protecting the logs, including protecting them from unauthorized access, modification, and deletion, and time frames for how long to retain the logs before deleting them.

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

Response explanation: NAU will continue to develop and implement written log monitoring policies, standards, and procedures that align with industry best practices.

Recommendation 2.2h: Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including the development of corrective action plans, provision of training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

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

Response explanation: NAU will continue to develop and implement university-wide

policies and procedures for reporting, evaluating, and correcting instances of noncompliance with IT security policies and procedures.

Recommendation 2.3: Not applicable to NAU.

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1: NAU should:

Recommendation 3.1a: Finish developing and implement its draft IT security strategic plan including developing a mission, goals, and objectives aligned with NAU's overall strategic mission, and performance measures to assess progress toward achieving those objectives.

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

Response explanation: NAU will complete the development and implementation of the IT security strategic plan.

Recommendation 3.1b: Finish developing and implement its draft information security policy and draft information security program, including outlining how its policies and IT security controls should be communicated to those responsible for implementing them.

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

Response explanation: NAU will complete the development and implementation of the information security policy and information security program.

Recommendation 3.1c: Develop and implement policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

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

Response explanation: NAU will develop and implement policies and procedures for monitoring the effectiveness of the IT security practices and use monitoring results to help inform security policy and procedure revisions.

Recommendation 3.1d: Develop and implement policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security.

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

Response explanation: NAU will develop and implement policies and procedures to monitor and assess third parties' adherence to contractual agreement requirements as

related to IT security.

Recommendation 3.2: Not applicable to NAU.

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1 – 4.2: Not applicable to NAU.

Recommendation 4.3: NAU should revise its data classification policies and procedures to include a requirement to periodically review its classification of data to ensure the data is appropriately classified and to update its data inventory, as necessary.

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

Response explanation: NAU will revise the data classification policies and protocols to include a requirement to periodically review the classification of data.

Recommendation 4.4: NAU should develop a plan for implementing its data classification policies and procedures, including:

Recommendation 4.4a: Establishing a deadline by which all individual units must complete the data classification process and develop data inventories; and

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

Response explanation: NAU will establish a deadline by which all units must complete the data classification process.

Recommendation 4.4b: Following up with individual units to ensure they have completed the process.

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

Response explanation: NAU will follow up with units to ensure completion of the data classification process.

Recommendation 4.5 – 4.6: Not applicable to NAU.

Recommendation 4.7: NAU should develop and implement university-wide IT risk assessment policies and procedures for conducting IT risk assessments, compiling and evaluating the results, using the results to manage and address identified risks, such as by implementing controls to protect against identified risks, and reporting the results to NAU's leadership. Additionally, the policies and procedures should assign roles and responsibilities for conducting and completing these various requirements and procedures.

NAU Response: The finding of the Auditor General is agreed to and the audit

recommendation will be implemented.

Response explanation: NAU will develop and implement university-wide IT risk assessment policies and procedures for conducting IT risk assessments in alignment with best practices.

Recommendation 4.8 – 4.9: Not applicable to NAU.

Recommendation 4.10: NAU should continue its efforts to further align its incident response process with IT standards and best practices and ensure its incident response policies and procedures address training for incident response personnel and testing its incident response process, including establishing time frames for training and testing.

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

Response explanation: NAU will continue to further align the incident response process with IT standards and best practices.

Recommendation 4.11 – 4.12: Not applicable to NAU.

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: Not applicable to NAU.

NAU Response: This response will be provided by ABOR.

Sincerely,

Rita Hartung Cheng
President

THE UNIVERSITY OF ARIZONA
Executive Office of the President

1200 E. University Blvd. Rm. 200
P.O. Box 210021
Tucson, AZ 85721-0021

Off: 520-621-5511
Fax: 520-621-9323

president.arizona.edu

June 18, 2018

Lindsey Perry, Auditor General
State of Arizona - Office of the Auditor General
2910 N 44th Street- Suite #410
Phoenix, AZ 86018

Dear Ms. Perry,

I have reviewed the preliminary report of the ***Arizona's Universities - Information Technology Security*** performance audit. Thanks to you and your team for the work that has been put into the audit and for engaging us in a dialogue about how we can better secure our network, systems, and data. The report clearly values the work we have done at the University of Arizona by showing that UA has:

- Acted quickly to make information security improvements by appointing a CIO.
- A culture of security awareness as evidenced by the predominantly positive results of the audit social engineering tests.
- The ability to further improve our security posture by employing automated security tools, network segmentation, a risk assessment process, and other effective tools and processes.

The report highlights a number of areas where the University of Arizona can improve and expand its efforts. We agree with the findings overall, agree to the recommendations and moving forward with the work.

There are several campus leaders that worked hard throughout this process to make this report possible. They spent hours collecting and sharing key data and ensured that the University of Arizona responded to requests from your office in a timely manner. I would be remiss if I did not recognize that hard work, including the efforts of:

- Dr. Allison Vaillancourt, Vice President for Business Affairs and Human Resources, and Audit Coordinator
- Dr. Jeff Goldberg, Acting Provost
- Gregg Goldman, Senior Vice President, Business Affairs and CFO
- Karen Williams, Vice President for Information Strategy and University Libraries
- Barry Brummund, Chief Information Officer
- Lanita Collette, Chief Information Security Officer

This group will provide leadership as we move forward to address the recommendations outlined in the report.

Thank you once again for the thorough review of our information security efforts.

Sincerely,

Robert C. Robbins, MD
President

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1 – 1.3: Not applicable to UA.

Recommendation 1.4: UA should implement its security awareness training policy and develop and implement additional policies or procedures for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its security awareness training policy.

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

Recommendation 1.5: UA should revise its security awareness training policies and procedures to require existing employees to complete security awareness training annually, define the roles and responsibilities of staff who will develop and implement security awareness training materials, and include requirements for periodically evaluating and updating security awareness training materials.

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

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1 – 2.2: Not applicable to UA.

Recommendation 2.3: UA should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

Recommendation 2.3a: Developing and implementing revised policies and procedures for its vulnerability management process that include requirements and/or guidance for:

- Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual units are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;
- Analyzing scan results, including specifying time frames for conducting the reviews, and sharing these results across the university to help eliminate similar vulnerabilities in other IT systems;
- Conducting penetration testing at specified frequencies based on risk;
- Using a risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be

considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and

- Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

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

Recommendation 2.3b: Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems only provide essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

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

Recommendation 2.3c: Developing and implementing additional patch management policies and procedures that include the following:

- Identifying needed patches, reporting those patches to appropriate individuals responsible for remediation, and applying patches;
- Testing patches for effectiveness and potential side effects before installation; and
- Installing patches within required time frames.

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

Recommendation 2.3d: Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Requiring web application developers to be trained on developing secure software;
- Reviewing web application source code before web applications are released; and
- Performing security testing before web applications are released.

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

Recommendation 2.3e: Developing and implementing additional log monitoring policies and procedures that include the following requirements and guidance:

- Specifying how frequently each log should be monitored;

- Identifying who is responsible for ensuring log events are captured and reviewing log events on a regular basis;
- Analyzing security-related information generated by log monitoring across the university to determine any patterns that might indicate potential attack; and
- Including requirements for securely protecting the logs and time frames for how long to retain the logs before deleting them.

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

Recommendation 2.3f: Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

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

Recommendation 2.3g: Developing and implementing university-wide procedures aligned with best practices that all individual units must follow when developing policies and procedures to address the recommendations in this finding; or include sufficient guidance in its university-wide policies to help ensure its individual units develop procedures for implementing UA's policies that fully align with IT standards and best practices.

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

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1: Not applicable to UA.

Recommendation 3.2: UA should develop and implement:

Recommendation 3.2a: An IT security strategic plan that contains a mission, goals, and objectives aligned with UA's overall strategic mission and includes performance measures to assess progress toward achieving those objectives.

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

Recommendation 3.2b: IT security policies and guidance documents that explain how UA will guide the management and protection of its IT systems and the data contained in them,

such as developing an information security program that outlines its overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls and explains how it will communicate UA's policies and IT security controls to those responsible for implementing them.

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

Recommendation 3.2c: Policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

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

Recommendation 3.2d: Policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security.

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

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1 – 4.4: Not applicable to UA.

Recommendation 4.5: UA should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified, and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified.

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

Recommendation 4.6: UA should:

Recommendation 4.6a: Establish time frames and guidance for regularly reviewing and updating data inventories; and

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

Recommendation 4.6b: Develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.

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

Recommendation 4.7: Not applicable to UA.

Recommendation 4.8: UA should revise its IT risk assessment policies and procedures to include a requirement for managing and addressing identified risks, such as by implementing controls to protect against identified risks.

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

Recommendation 4.9: UA should fully implement its IT risk assessment process by:

Recommendation 4.9a: Conducting the IT risk assessment in all of its individual units;

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

Recommendation 4.9b: Compiling and analyzing the results of the IT risk assessment;

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

Recommendation 4.9c: Using these results to establish a university-wide IT risk profile; and

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

Recommendation 4.9d: Communicating the results to UA's leadership.

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

Recommendation 4.10: Not applicable to UA.

Recommendation 4.11: UA should develop and implement policies and procedures for training incident response personnel and for testing its incident response process, including establishing time frames for training and testing.

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

Recommendation 4.12: UA should develop procedures for assessing whether UA staff are complying with its incident response policies and procedures and take steps to help ensure identified instances of noncompliance are adequately addressed.

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

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: Not applicable to UA.