Letter to the Senate with Resolution
Report for Senate on the UITS Cloud and Centralization Plans Proposed by the CIO

SUBJECT: UITS-suggested Mega-migration assessment

This document is a request for clarification of the proposed UITS mega-migration to cloud-based data processing and mega-centralization. This memo offers initial faculty assistance to President Robbins and the Faculty Senate to initiate a due diligence assessment of the proposed UITS mega-migration.

In March 2023, the CIO stated to the Faculty Senate that the proposed mega-migration to cloud-based data processing and extreme centralization changes to UITS were a response to the 2018 Arizona Auditor General performance audit. The facts do not seem to support this claim.

- The CIO has not proposed an extreme centralization plan and did not make a statement to that end in Faculty Senate in March 2023.
- The UArizona ASITS (Accelerating Secure Information Technology Services) program was established as a result of a follow up audit in spring 2022 when three campus units were found to be deficient in vulnerability management, configuration management and logging and monitoring.
- The results demonstrated campus units were still not compliant with 2018 audit recommendations. UITS successfully passes audits on an annual basis.
- The focus is on providing UITS managed services to address college/division information security audit findings, not centralization.

In 2018, the Arizona Auditor General conducted a performance audit, simulating a computer security attack of the UA, ASU, NAU, and the Board of Regents. They found that *"security controls slowed simulated attacks, but vulnerabilities allowed unauthorized access."* The Arizona Auditor General made 85 recommendations, 23 to UA, returning for follow up reviews in 2000 and 2022, respectively. Specifically, the UA was asked to improve its IT risk assessment processes and implement them university-wide, continue to improve and develop its security governance, including policies and procedures. https://www.azauditor.gov/sites/default/files/18-104_Report.pdf.

Four years later, the Arizona Auditor General reported that ABOR, NAU, and ASU implemented or were implementing all of their 62 recommendations. In contrast, the UA had implemented only 5 of its 23 recommendations, with 12 in progress and 6 still not addressed. The Arizona Auditor General states that the UA refused to provide the Auditor General with an *"outline a plan or estimated time frame for implementing these 6 recommendations."* The Arizona Auditor General concluded that *"we do not see further benefit in continuing to follow up with UA. Therefore, unless otherwise directed by the Joint Legislative Audit Committee, this report concludes our follow-up work on the Universities' efforts to implement the recommendations from the June 2018 report."*

- The UArizona did not refuse to provide the Arizona Auditor General with a plan or estimated time frame. The federated org design of IT at the University requires a collaborative approach. Arizona Auditor General recommendations were communicated to colleges/divisions. In 2022, the Arizona Auditor General tested compliance with recommendations in three units and found those units to not be in

compliance with their recommendations. UITS successfully passes audits on an annual basis.

- The Arizona Auditor General and the ABOR want the UA to address security deficiencies in all colleges and divisions. The first step in the UA ASITS program is to develop plans in each College/Division, for each College/Division, to address findings at the College/Division level. The services developed by UITS as part of the ASITS program will help colleges and divisions to address current infrastructure security issues.
- Offering these services broadly to the University is critical because the Arizona Auditor General wants their recommendations implemented for ALL University systems, not just UITS systems. Many colleges/divisions are not staffed sufficiently today to handle this large amount of work.

The Arizona Auditor General's recommendations made no reference to total IT centralization (including all research units), moving to a predominantly cloud-based data processing, hiring an outside company to run IT, or a concern about saving money. These four elements are the core of the UITS proposal as presented by the CIO to the Senate. They apparently were never spelled out by the Arizona Auditor General .

- The UArizona has not proposed total IT centralization.
- The UArizona has not proposed to have an outside company run IT.
- Minimizing the cost of implementing these requirements is one of many considerations and is part of all UITS proposals.

The failure to implement the 23 security risks at UA outlined by the Arizona Auditor General led ABOR to task President Robbins with solving the problem. (Note, that the Arizona Auditor General's concern for unaddressed system vulnerability remains.) The ABOR set performance incentives for President Robbins were:

- ● *"By June 30, 2023, develop, adopt and communicate a plan to centralize responsibility and balance local authority in the university-wide administrative functional areas of Information Technology and Financial and Business Services. The plan should include appropriate transfers of budgetary, financial, hiring and operational accountability to maximize service, effectiveness, and efficiency."*
- ● *"Implement and document an Information Technology security governance framework that includes: an IT security strategic plan, articulated roles and responsibilities, policies and guidance, training across the university in security awareness, and processes for monitoring and evaluating the effectiveness of institutional IT security practices."*

The above statements refer to the *centralization of responsibility in functional areas of IT and Financial and Business Service* but NOT to technical/hardware/software centralization, as applied to research and academic activities.

Because of the foregoing we pose the following questions to the CIO:

1) Of the Arizona Auditor General's 85 recommendations to ASU, NAU, The Regents, and the UA, why was UA the ONLY campus to fail to complete its list (in over 4 years), therefore exposing the Regents, UA President and UA to legislative scrutiny?

- UArizona UITS services are in compliance with 2018 Arizona Auditor General requirements. UArizona college/division services are not all in compliance with 2018 Arizona Auditor General requirements.
- UArizona college/division IT services/staff are different than college/division services/staff at NAU and ASU. Information technology services/staff at NAU are fully centralized. Information technology services/staff at ASU have substantially more IT capacity (employees/budget) per student and per contract/grant.

2) Why was President Robbins then tasked with fixing the security IT risks, as opposed to the CIO and staff?[1]

- Cybersecurity risk is a university risk, not just a UITS/CIO risk, as UArizona college/division IT services/staff are not all centralized and do not all report to the CIO.

3) Why was UA the ONLY university that did not offer *"Response explanations"* of how to implement the recommendations in the response to the audit report *"Arizona's Universities – Information Technology Security"* from 06/18/2018, but only offers the following standard response to ALL recommendations: *"The finding of the Auditor General is agreed to and the audit recommendation will be implemented."*? Why is the "how" never spelled out?

- UArizona responses are consistent with responses from ASU, NAU, and the ABOR.

4) Why was the noncompliance of the CIO not made known to the UA faculty and staff, the stakeholders, but instead was disguised by distracting the entire campus into an unrelated, expensive, and harmful centralization and cloud-computing mandate that was, despite insistence to the Senate, not the focus of the Arizona Auditor General 2018 audit?

- There have been a substantial number of communications and meetings focused on information security and the importance of remediating the 2018 Arizona Auditor General findings. Communications were distributed to many audiences, including Dean/VPs and IT leaders. Guidance and consultation, a risk assessment web application, information security awareness training, secure development training, and a number of other services are offered by the Information Security Office to assist departments in securing information resources.

Assessment

This assessment reveals that the AZ Auditor General did not request the currently proposed massive centralization with outside companies and cloud-based framework. The faculty, staff, and students have been misinformed. The UA IT security effort, led by the CIO, failed the university by not fixing all the items outlined by the Arizona Auditor General over a four year period, in utter contrast to ASU and NAU. The current proposed mega-centralization to "fix" the IT security is inappropriate, entirely out- of-scale, and destructive to the university's mission. It must stop now.

PROPOSED MOTION

As such we move to:

1. Suspend all further IT integration/centralization until the issues above are properly addressed, and until a full risk assessment of any proposed mega-centralization and cloud migration framework is conducted.

- Information security is an urgent priority for the University requiring immediate action in colleges/divisions – current efforts to remediate Auditor General findings/risks should continue. Pausing remediation efforts will likely expose the University to additional cybersecurity risks.
- Centralization of college/division IT staff has not been proposed; therefore it does not need to be suspended.
- A mix of on premise equipment and elastic cloud equipment is optimal to manage the University's IT infrastructure. Both options should be considered by each college/division for each college/division information security remediation plan.

2. Form immediately a UITS Technical Oversight Committee composed principally of knowledgeable faculty who are true stakeholders in IT efforts (for example, those with scientific instruments that require computers), chosen from the affected colleges, mostly non-UITS IT-personnel (Colleges/units), who will devise a plan on a short time scale (i.e., before Fall Semester 2023) for campus IT security that addresses all remaining security issues to the satisfaction of the AZ Auditor General and the UITS Technical Oversight Committee.

- UArizona encourages faculty engagement in IT services supporting academic and educational activities and IT services supporting matters related to faculty personnel. Further, UArizona encourages faculty engagement in IT services supporting research.
- The UArizona ASITS program is currently working with IT liaisons in every college/division (liaisons appointed by each Dean/VP). College/Division information security remediation plans are being developed by each college/division, for each college/division.
- UArizona encourages the implementation of the best plan possible to address college/division information security findings, recognizes that faculty and staff in all units have a stake in addressing cybersecurity risks in their unit, and encourages faculty and staff to engage with their college/division Dean/VP and IT Liaison as they develop their plans.
- UArizona information technology services are presently federated. The current proposal to remediate college/division information security findings preserves the standing federated organizational design. The focus is on providing UITS managed services to address college/division information security audit findings, not centralization.
- The UA ASITS program is partnering with faculty and IT experts from RII and the College of Science to develop solutions to support research requiring specialized scientific equipment. More information about this partnership and these solutions will be shared as it evolves.

[1] Robbin's ABOR assignments.

Links to the respective audits:

https://www.azauditor.gov/system/tdf/18-104_48-Mth_Followup.pdf?file=1&type=node&id=10061&force=0 for details of 6 non-implemented recommendations.

https://www.azauditor.gov/system/tdf/18-104_Responses.pdf?file=1&type=node&id=10061&force=0

Note, that UA is the ONLY university that does not offer "Response explanations" of how to implement the recommendations, but only offers the following standard response to ALL recommendations: "The finding of the Auditor General is agreed to and the audit recommendation will be implemented." Why is the "how" never spelled out?