UTAH SYSTEM OF HIGHER EDUCATION
Building a Stronger State of Minds

State Board of Regents
Board of Regents Building, The Gateway
60 South 400 West
Salt Lake City, Utah 84101-1284

Phone 801.321.7101
Fax 801.321.7199
TDD 801.321.7130
www.higheredutah.org

May 8, 2019

MEMORANDUM

TO: State Board of Regents

FROM: David L. Buhler

SUBJECT: USHE – Cybersecurity Funding

Issue

In both 2018 and 2019 the Board of Regents included cybersecurity in its budget request to the state legislature. In 2019 the legislature approved intent language that a portion of the Board's cybersecurity request is funded with unallocated performance-based funding. Although this is helpful it leaves other critical cybersecurity measures still unfunded. The Commissioner has consulted with the presidents and is recommending a significant portion of these identified needs be funded through internal institutional resources. Institutions will report back to the Board on a funding plan to address their cybersecurity needs.

Background

Student information, institutional financial data, hospital records, proprietary research, and employment records require safekeeping. The Board of Regents and USHE institutions take information security seriously. Over the past few years, the Board of Regents and USHE institutions proactively took a number of steps to protect against cyber threats, including:

- *Biennial IT Security Audits*. The Regent Audit Subcommittee of the Board began requiring biennial IT security audits of each USHE institution several years ago, which they review annually.
- *Multi-Factor Authentication*. As required by the Board, over the last year institutions have implemented two-factor authentication.[1]
- *Data Breach Insurance*. The Board created policy to require each institution to purchase insurance to cover a "loss or breach of Personally Identifiable Information."[2]

As demonstrated in the IT security audits, institutions have made significant strides to protect themselves from cyber threats; however, cybersecurity remains a top system and institutional risk. The Regent Audit Subcommittee and institutional audit committees continue to rank IT security among the highest risks in the system.

In July 2018, the Board of Regents received a briefing in closed session on cybersecurity by Steve Hess,

[1] See Regent policy R432-4.1.3
[2] Regent policy R432-8

CIO for the system as well as the University of Utah. Recognizing the need to protect the system, institutions, and students from aggressive global cybersecurity threats, and to replace aging USHE IT infrastructure, the Regents prioritized $7,150,000 for cybersecurity in the 2019 legislative budget request. This included the following items:

- $500,000 to purchase, install, and maintain next-generation network firewalls
- $750,000 to purchase, install, and maintain advanced malware endpoint protection
- $4,900,000 to update edge network equipment to access control and security standards
- $1,000,000 for salaries, wages, and benefits for IT security personnel

The state legislature recognized the importance of USHE cybersecurity by adopting intent language but did not fund the request (nor have they funded similar system requests in the past). The legislature authorized the Board of Regents to use any unallocated performance funding for cybersecurity needs and left the remainder to be funded from within existing appropriations.

The Commissioner recommends that, as per the legislative intent language, $1,005,800 in unallocated performance funding for FY 2019-20 be used toward the unfunded cybersecurity request on an ongoing basis for next-generation network firewalls and advanced malware endpoint protection. Institutions do not all currently have this type of comprehensive protection, and the new funding will bring them up to the same standard.

The Commissioner further recommends, after consultation with the Council of Presidents, that each institution create a funding plan to submit to the Board of Regents on how they will allocate internal funds to cover the ongoing replacement of edge network equipment. The network is the first layer of defense against cybersecurity threats, but the USHE wireless and network edge components are dated and cannot maintain newer advanced network security protocols. The components and devices must be replaced on a recurring lifecycle. Institutions identified replacement needs for the edge network as follows and will provide the Commissioner's Office with a plan for funding of these needs by July 1, 2019:

• University of Utah	$1,620,000
• Utah State University	$ 604,000
• Weber State University	$ 770,000
• Southern Utah University	$ 161,000
• Snow College	$ 140,000
• Dixie State University	$ 216,000
• Utah Valley University	$ 548,000
• Salt Lake Community College	$ 807,000

These two recommendations will substantially address all but the $1,000,000 in the USHE budget request for salaries, wages, and benefits of IT security personnel. The Commissioner encourages institutions to consider, where feasible, how to fund these positions, but does not require them to be part of the institutional plans required above.

Commissioner's Recommendation

The Commissioner recommends that the Board approve the $1,005,800 unallocated portion of performance funding for cybersecurity needs in the system and require USHE institutions to submit a plan to the Commissioner's Office by July 1, 2019, describing how they will address unfunded ongoing cybersecurity needs for the edge network.

_____

David L. Buhler
Commissioner of Higher Education

DLB/KLH/RPA