MEMORANDUM

TAB R

September 4, 2019

USHE - Cybersecurity Funding Update

During the 2019 Legislative session, the Board of Regents requested from the legislature, $7,150,000 for cybersecurity needs. While not funded, the Legislature adopted intent language allowing for $1,005,800 of the Board's request to be funded with unallocated performance-based funding.

During the May 2019 Regents meeting, the Board approved using $1,005,800 of unallocated performance funding for cybersecurity needs including next-generation firewalls, advanced malware endpoint protection, and wireless upgrades. The Board also recommended institutions fund a significant portion, totaling $4,345,000, with internal institutional resources, and submit plans to the Commissioner's office describing how they will address unfunded ongoing cybersecurity needs for the edge network using internal allocations. The attached document describes these plans.

Commissioner's Recommendations

This is a discussion item only; no action is required.

Attachment

Cybersecurity Total USHE: $5,350,800

This initiative supports the purchase of next-generation network firewalls, advanced malware endpoint protection, wireless upgrades, and edge network equipment. These upgrades will help protect student information, financial data, hospital records, proprietary research, and employment records. Institutions have created the following funding plans using internal allocations.

University of Utah $1,620,000

Regents' Strategic Priorities – Information technology is essential to achieve the strategic goals for higher education of affordability, completion and innovation. IT eliminates paper, streamlines processes, provides relevant data and analytics for critical decisions and provides library, counseling, and instruction to students anywhere at any time. It increases productivity of faculty, staff and students, helping students toward faster completion. The baseline of IT that makes these benefits possible is the IT network and secure access to rich online resources and data. The loss of personal private data is damaging and costly to the reputation of a university or college. Staff, faculty and students expect 24 X 7 connectivity and security for their personal data. A network outage and security breach can have significant impact on job productivity. It can also cut essential network connected services such as building, access, HVAC control, fire alarms, security cameras, utility meters, instructional materials, accounting reports, payroll and emergency alerts. IT security and networks have been underfunded for years. Compared to other colleges and universities around the country, Utah institutions of higher education are 1.5% below the norm in IT spending, particularly with security and networks. The requests listed below will catch up Utah colleges and universities on secure network equipment.

Description – The network is the first layer of defense against cyber security threats, but Utah school's dated wireless and network edge components can't maintain the newer advanced network security protocols. These devices must be replaced on a recurring lifecycle in order to have the latest manufacturers' upgrades, which provide the best cyber security protection possible, or Utah schools face a high probability of a cyber-security breach.

USHE CIOs have completed a comprehensive network edge inventory, looking at the cost to maintain an industry recommended ten-year replacement for all building network switches and network components and a five-year replacement for all wireless network components and software to meet minimum security standards and network demand.

Justification – The top cyber security threats facing higher education are phishing attacks, malware and ransomware, encryption blind spots, cloud access, Internet of Things (IoT), vulnerability management, third-party risk management, and user actions. This is not an issue unique to Utah: 35% of all security breaches take place in higher education. Additionally, the critical importance of quality high-speed internet connectivity to higher education and research is an inarguable certainty. Today's core college and university knowledge and administrative functions are intertwined with innovative software, powerful hardware, and interconnected

services. Core functions of campus buildings are also tied to the internet through the network edge.

The demand for greater in-building networking capability has dwarfed the resources available to keep up with the requirements of the network, network edge, and security standards. Updating and maintaining this equipment, as well as ensuring the equipment meets minimum security standards to allow for better security monitoring across campuses, is crucial for Utah's colleges and universities to function – as crucial as maintaining building HVAC, plumbing, electric, and infrastructure has always been.

Outcomes – This funding will bring the University of Utah networks up-to-date with network industry standard replacement schedules. Many network devices are too out-of-date to receive manufacturer updates and are no longer meeting the minimum-security standards *or* user demand, something that has accelerated exponentially in the past three years as more and more devices show up on campuses.

Assessment – Network Edge Replacement: Network replacement schedules and new security features will be reviewed in quarterly USHE CIO meetings and update reports shared with the Regents' audit committee and the legislature. The reports will include replacement schedules, progress on installation to insure accountability on completion, and activation of security features made available with the new equipment.

Budgetary Plan – The $4.9M dollar USHE request is to update and replace edge network equipment, wireless access points, controllers and software. The University of Utah's annual cost for network access controls is $1,620,000.

Utah State University $604,000

Budgetary Plan – Support full on-going legislative allocation beginning FY21. To address interim cybersecurity network infrastructure initiatives needs for FY20, USU will identify and utilize a combination of internal unit chargeback/fee and central funding sources. USU IT will apply this funding to identify and replace infrastructure based on age and scope of impact.

Weber State University $110,000

R*egents' Strategic Priorities* – Information technology is essential to achieve the strategic goals for higher education of affordability, completion and innovation. IT eliminates paper, streamlines processes, provides relevant data and analytics for critical decisions and provides library, counseling, and instruction to students anywhere at any time. It increases productivity of faculty, staff and students, helping students toward faster completion. The baseline of IT that makes these benefits possible is the IT network and secure access to rich online resources and data. The loss of personal private data is damaging and costly to the reputation of a university or college. Staff, faculty and students expect 24 X 7 connectivity and security for their personal data. A network outage or security breach can have significant impact on job productivity. It can also affect essential network connected services such as building

automation, access control, HVAC control, fire alarms, security cameras, utility meters, instructional materials, accounting reports, payroll and emergency alerts. IT security and networks have been underfunded for years. Compared to other colleges and universities around the country, Utah institutions of higher education are 1.5% below the norm in IT spending, particularly with security and networks.

Description – With more one-to-one initiatives in K-12 we are seeing a stronger desire to use the wireless when these students reach our campus. The money would be used to fund wireless density increases, additional backend equipment to keep up with increased usage of the wireless. Keep up with the latest wireless standards and fund backend and closet infrastructure needed to support these new more dense wireless installs. A few buildings are in need of closet upgrades to support more wireless in the buildings and allow for other classroom technology use.

The network is the first layer of defense against cyber security threats, but Utah school's dated wireless and network edge components can't maintain the newer advanced network security protocols. These devices must be replaced on a recurring lifecycle in order to have the latest manufacturers' upgrades, which provide the best cyber security protection possible, or Utah schools face a high probability of a cyber-security breach.

Justification – The top cyber security threats facing higher education are phishing attacks, malware and ransomware, encryption blind spots, cloud access, Internet of Things (IoT), vulnerability management, third-party risk management, and user actions. This is not an issue unique to Utah: 35% of all security breaches take place in higher education. Additionally, the critical important of quality high-speed internet connectivity to higher education and research is an inarguable certainty. Today's core college and university knowledge and administrative functions are intertwined with innovative software, powerful hardware, and interconnected services. Core functions of campus buildings are also tied to the internet through the network edge.

The demand for greater in-building networking capability has dwarfed the resources available to keep up with the requirements of the network, network edge, and security standards. Updating and maintaining this equipment, as well as ensuring the equipment meets minimum security standards to allow for better security monitoring across campuses, is crucial for the University to function – as crucial as maintaining building HVAC, plumbing, electric, and infrastructure has always been.

Outcomes – Updated network underpinnings in older facilities as well as density increases as needed in newer and older facilities.

This funding will bring all colleges and universities networks up-to-date with network industry standard replacement schedules and network security tools. Many network devices are too out-of-date to receive manufacturer updates and are no longer meeting the minimum-security standards *or* user demand, something that has accelerated exponentially in the past three years as more and more devices show up on campuses.

Assessment – Network Edge Replacement: Network replacement schedules and new security features will be reviewed in quarterly USHE CIO meetings and update reports shared with the regents audit committee and the legislature. The reports will include replacement schedules, progress on installation to insure accountability on completion, and activation of security features made available with the new equipment.

Budgetary Plan – Originally, this request was for $770,000 in lump sum funds. To meet the needs of the University and to create a sustainable program for repairs and replacement of the wireless network, the request was updated to reflect an annual base operating expense increase of $110,000.

Southern Utah University $300,000

Next General Firewalls

Regents' Strategic Priorities – Completion: In today's security landscape, it is becoming ever more apparent the need for institutions to implement industry best practices in protecting the personal information of their constituents. As students entrust us with their personal data, we need to ensure that proper controls are in place to help reduce the risk of unauthorized access to that information, which may result in an impact to the institution's ability to fulfill its core mission of providing educational services.

Description – One of the core controls in any information security program is effectively controlling network traffic into and out of the network. This is primarily done through the use of firewalls. Firewalls were one of the first security technologies implemented and stateful firewalls have become a critical component for a successful information security program. New capabilities have been added to the traditional stateful firewalls, leading to a technology dubbed as a next generation firewall. This moniker refers to a firewall that has added functionality, such as deep packet inspection, intrusion detection capabilities, URL filtering, and application inspection, among others. These added capabilities not only control the authorized flow of traffic, but also inspect the traffic to better detect anomalous behavior and potential malicious activity.

This request is for two next generation firewalls, that can be configured in a high availability pair, including the yearly subscriptions that provide additional capabilities.

Justification – The need for better security controls is readily apparent as the number of organizations in the news due to a security incident is steadily on the rise. A truly effective security program subscribes to the defense-in-depth approach to security. This simply means that no single security control can prevent data breaches, but rather, a complementary suite of controls is needed to effectively reduce the overall risk to an organization. These controls may include next generation firewalls, intrusion detection systems, endpoint protection solutions, network monitoring, log management, security information and event management systems, centralized log management, privileged access management, etc. The challenge that universities face is that they have similar data protection needs and requirements as commercial entities, yet can be limited in the financial resources available to acquire some of

these technologies. Simply put, security tools can be very expensive and often out of the financial reach of a university. Yet, the institution still has a responsibility to provide adequate data protection. Southern Utah University has already invested in endpoint protection, and has made significant use of open-source technologies to address some of the other layers. However, some security controls are best implemented with a commercial offering. This request is to secure funding to help provide for one of those core data security controls, namely, next generation firewalls, which is one of those technologies best provided by a commercial solution.

Outcomes – Funding would allow SUU to acquire two next generation firewalls to be configured in a high availability pair. Funding would also include the yearly maintenance costs to maintain the subscriptions to provide added functionality. This would result in an overall risk reduction to the university as this core preventive/detective control is strengthened.

Assessment – Success will be measured by the number of incidents prevented/detected by the technology. With traditional stateful firewalls, the number of denies to unauthorized destinations is tracked. With the implementation of a next generation firewall, that same metric can be tracked, but additionally, other preventive and detective metrics can be measured and monitored to reflect the new capabilities. Thus, detections that would have gone unseen with a traditional firewall, are now visible and measurable, helping to show the risk reduction realized with the implementation of the next generation firewall.

Budgetary Plan –	One-time Capital Acquisition Costs	$230,000
	On-going Operating Expenses	$ 70,000
	Total Annual Operating Expenses	$300,000

Snow College $140,000

Snow College has put together the following information that specifically outlines the Cybersecurity steps that have been taken during this past fiscal year, and what the plans are moving forward.

"Edge Networking" has been defined in many ways, with that said, we would like to define what we believe the terms "Edge Networking components" and "Wireless" are so that the reader will understand Snow's approach to securing these respectively. Simply put, Edge computing allows data from the IoT (internet of things) devices to be analyzed for security concerns at the "Edge" of the network before being allowed to access the data center.

As one part of this strategy to more tightly secure access to mission critical systems and the data contained therein, Snow has recently acquired 4 "Fortinet, Fortigate Next Generation Firewalls" model 3000D. Two of the devices are configured at our Ephraim data center, and two are configured at our Richfield data center, as part of the "Edge" gateway.

These Fortigate firewalls will be on a 5-year refresh cycles based on the manufactures statements. Snow will continue to do what it's done in the past and make our systems last as

long as possible, as long as doing so does not compromise our ability to continue to protect the schools information and it's students.

Since the "IoT" relies heavily on "Wireless" access, Snow has collaborated with Fortinet and has been testing their latest wireless AP's (Access Points). Snow's current wireless AP's are very dated and no longer support the new security protocols needed to secure the network. Some of these access points are 16 years old. The current aged AP's are manufactured by Cisco, and updating these will be very costly. Snow's Information Technology team is currently working with Fortinet to perform thorough testing and analysis of their AP technology compared to Cisco. Snow's current direction is to migrate away from the Cisco AP's, and to standardize on Fortinet's next gen AP's across both campus's.

Snow has many old Cisco switches as part of it's network that are overdue to be replaced. IT is currently working on exploring a way of leveraging Fortinet's next Gen Firewalls ability to perform some key switching functions. If successful, IT will be able to replace the older and much more costly Cisco switches with less expense switches, which will provide a net cost savings of approx. 250k. These savings can then be used to refresh other IT equipment such as the aged AP's.

Fortinet has recently acquired Bradford networks, which was a factor in our decision to go with them as our "Next Gen. Firewall" partner. Snow rolled out Bradford networks a couple years ago to further control endpoint access to its networks. Fortinet's vision is to integrate Bradford's functionality within the suite of Fortinet's Security solutions.

Cybersecurity is of paramount importance to Snow College. Snow will continue to improve upon what it has built as a good security foundation, and will continue to evolve as technology changes, and as budgets allow.

Dixie State University $216,000

Regents' Strategic Priorities – This initiative supports the Regents' strategic priority of strengthening IT security across the USHE system.

Description – This funding will enable DSU to implement a regular replacement cycle for edge network equipment, including network switches and wireless access points.

Justification – Since specific requests for IT security funding have not been prioritized by the state legislature, DSU has identified alternate funding as recommended by USHE.

Outcomes – Current network equipment is significantly outdated due to the lack of a consistent funding source. The institutional goal is a 10-year replacement cycle for switches and a 5-year replacement cycle for access points, although it will take several years to reach this status. DSU will begin by replacing the oldest and most vulnerable equipment first.

Assessment – Success will be measured by reaching institutional replacement cycle targets for edge network equipment.

Budgetary Plan – DSU plans to fund $216,000 in FY20 with $107,800 ongoing funds from performance funding and $108,200 from one-time institutional reserves. The $108,200 portion will be converted from one-time to ongoing funding in FY21 using funds from anticipated enrollment growth.

Utah Valley University $548,000

Regents' Strategic Priorities – Student Growth & Capacity

Description – Protect UVU and its students from aggressive global cybersecurity threats and replace aging IT infrastructure by updating edge network equipment to access control and security standards.

Justification – The network is the first layer of defense against cybersecurity threats. Dated wireless and network edge components cannot maintain newer advanced network security protocols.

Outcomes – Updated wireless switch, controllers, and network edge components in accordance with lifecycle

Assessment – All wireless switch, controllers, and network edge components at end of lifecycle in 2019-20 will be updated.

Budgetary Plan – Utah Valley University has allocated one-time funds from additional dedicated credit revenue of $515,000 and reallocation of existing IT budget of $33,000, totaling $548,000 to pay for end of lifecycle replacement of wireless switches, controllers, and network edge components for 2019-20. Identifying ongoing funding for lifecycle replacement will be a focus during UVU's FY21 budget process.

In addition to providing one-time funds outlined above, ongoing funds of $278,944 were allocated from FY20 Performance Funding—Education Funds to fund a full-time security analyst $113,944, next generation firewall expansion $70,000, and advanced endpoint protection $95,000.

Salt Lake Community College $807,000

Regents' Strategic Priorities – This initiative supports the Regents' strategic priority of strengthening IT security across the USHE system.

Description – The USHE 2019-20 Cyber Security Operating Budget Request included a $7.1 million ongoing base fund request for Information Security. Of that amount, SLCC's share was $800,000. This request was not funded; however, SLCC has continued to set one-time dollars to cover these costs. The funding amount is the cost to replace network infrastructure at 10 of our campus sites around Salt Lake County.

Justification – Network infrastructure equipment needs to be replaced as it ages and should be on a standard replacement cycle determined by the particular equipment. This ensures that SLCC infrastructure supports the growth and scalability for students, faculty and staff as technology dictates. The College has used strategic planning to cover the annual costs with one-time funds, but as other needs arise, it creates an increased demand for ongoing base funds.

Outcomes – These upgrades ensure that SLCC's infrastructure will continue to support the growth and scalability of the network while providing the college a solid foundation for their Cybersecurity posture. Students, faculty, and staff need the infrastructure to perform their academic and work duties while also providing cybersecurity protection.

Assessment – We will continue to measure how students, faculty and staff access the network and monitor usability as well as provide safe data infrastructure.

Budgetary Plan – The funding for the network infrastructure will come from institutional one-time funding and not new tax funds. The institution has set aside $801,000 funds to cover this need for at least the next 3 years; however, we would support and benefit from base dollars system-wide.

State Board of Regents $1,005,800

Regents' Strategic Priorities – Investment in this area will advance the Regents' strategic priority of affordable access by reducing the liability associated with cybersecurity breaches.

Description –The state legislature authorized the Board of Regents to use any unallocated performance funding for one-time cybersecurity needs. While institutional cybersecurity needs require ongoing funding, this allocation will provide one-time funds to help institutions acquire two elements of IT security recommended by internal IT security auditors and the Center for Internet Security. The first element is the purchase and installation advanced malware end point protection. Malware often called malicious software is any program or file that is harmful to a computer user. Types of malware include computer viruses, worms, trojan horses and spyware. The second element that institutions will use these funds to support is the purchase and installation of next generation network firewalls. A firewall is part of a computer network which is designed to block unauthorized access while permitting outward communication. Our institutions have improved their network firewalls and additional funding will provide the latest next generation firewalls which are essential in the prevention of computer and network breaches. Institutions will receive a portion of the funds based on budget-related student FTE.

Justification – Student information, institutional financial data, hospital records, proprietary research, and employment records require safekeeping. 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, multi-factor authentication, and data breach insurance. 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.

Outcomes – The strategic use of these funds will provide institutions an initial investment in an ongoing effort to secure and protect institutional data and information from cybersecurity threats. The one-time nature of the funds will require institutions to identify and prioritize internal revenue sources and future funding to continue and expand the effort in this critical area. Ultimately the funds will improve institutional cybersecurity.

Assessment – Annual IT security audits will continue to provide the Regent Audit Committee assessment information on institutional cybersecurity strengths, opportunities, weaknesses, and threats.

Budgetary Plan – These funds contribute to the purchase of endpoint protection, firewalls, security information event management, and core security-related IT infrastructure.

Equipment/Software	$1,005,800
Total	$1,005,800