Colorado Mesa University
Network Security and Resiliency Project
Initial Funding Year FY2021-22
Quarterly Update, August 19, 2023

1. **Which elements of the project are currently underway? Which elements have been completed since the department last updated the JTC? Is the Project on schedule with initial plans?**

All elements of CMU's Network Security and Resiliency Project are complete. Since the May 2023 JTC update, CMU has completed the main campus local area network (LAN) backbone to 10 GbE with redundant building links. This project has been a huge success and extremely beneficial to the University and the students that CMU supports. Thank you.

CMU's Network Security and Resiliency Project had three main elements:

I. Upgrade the core network switch and add redundant top-of-rack 40 Gigabit Ethernet (GbE) switches to increase connectivity to virtualized server environments. –**Complete**

A pair of Aruba VSX core network switches have been installed in the primary and secondary data centers. Redundant 40 GbE links have been configured between the core network switches and they are actively handling network traffic. The core networks switches have 10 GbE ports for building local area network (LAN) backbone connections. A pair of high-performance 40 GbE top-of-rack switches have been installed in each data center, and they are actively handling traffic between the VSX core switches, virtualized servers, and mobility controllers.

The top-of-rack switches are configured with redundant 40 GbE uplink connections to the VSX core network switches and redundant 10 GbE connections to servers and mobility controllers to support the university's wired and wireless infrastructure. Each pair of top-of-rack switches have been configured to use Aruba's resilient switch stacking technology to provide redundancy and to handle heavy data traffic loads between systems and building networks, significantly increasing the university's network performance and resiliency.

II. Upgrade the main campus local area network (LAN) backbone to 10 GbE with redundant links to most buildings. –**Complete**

New Aruba CX network switches have been installed and the LAN backbone has been upgraded to 10 GbE. To add redundant network connections to each building, additional interconnect fiber had to be terminated between the primary data center and the data center building's entrance facility. All the interconnect fiber has been terminated for the project.

By deploying Aruba CX network switches with advanced security features, CMU implemented zero-touch switch configuration protocols for deploying network switches. This approach allows a new switch to be connected to the network where it is automatically configured using Aruba's auto-stacking feature. Adding or replacing a switch in a building is now simply performed by taking a new Aruba CX switch out of the box, registering its MAC address, and connecting it to a building's network switch stack where the switch automatically receives firmware updates and downloads a building configuration from the Aruba mobility controller. Further, network policy changes and device-specific configurations are pushed from the centrally managed mobility controller. Zero-touch switch configuration dramatically reduces the possibility of network configuration errors and ultimately prevents security holes.

III. Upgrade edge switches in residence halls to upgrade all device ports to 1 GbE with advanced features to support dynamic port segmentation for increased personal device security. – **Complete**

All residence hall network switches have been upgraded to provide 1 GbE device ports and improve security for student devices connecting wired or wirelessly. Each residence hall LAN backbone connection was also upgraded to redundant 10 GbE connections as described above.

With the upgrade of residence hall network switches, CMU implemented Aruba's advanced security feature, dynamic port segmentation, to provide complete visibility of what and who is on the university network and allow access to the network according to network security policy. The technology collects information about each device connecting to the network, such as device type and operating system, to proactively protect the network. Dynamic port segmentation allows device traffic to be tunneled from the network edge to the mobility controllers—network security appliances—in the data center and eliminates possible points of unauthorized access to the network through a centrally managed, unified, role-based network security policy. The mobility controllers automatically segment the device traffic to help ensure device and application security. For example, CMU registered, Internet of things (IoT), untrusted, and guest devices are dynamically segmented by virtual LAN to protect systems, applications, and other devices on the university's network from being affected by a compromised device part of a malicious attack.

2. **How much money has been obligated and spent at this point? Please break down amounts spent separately.**

CMU spent a total of $2,446,065.65 of the $2,472,417 total project funding.

	Capital Construction (CCF)	Cash Funds (CF)-9%	Total Funds
Budget	$ 2,249,898.00	$ 222,519.00	$ 2,472,417.00
Network Equipment/Cabling	$ 2,180,730.30	$ 215,676.62	$ 2,396,406.92
Professional Services	$ 45,189.44	$ 4,469.29	$ 49,658.73
Total Expenditures	$ 2,225,919.74	$ 220,145.91	$ 2,446,065.65
		Remaining Funds:	$ 26,351.35

Professional Services expenditures for fiber interconnect work performed by contractor.

3. **What is anticipated to be completed by the next quarterly update?**

Project is complete.

4. **When does the department/institution anticipate that the project will be complete?**

CMU has completed its Network Security and Resiliency Project.

5. **Are there any important concerns or updates you wish to share with the committee?**
   None

6. **For multi-phase projects, has there been any insight gained through this phase of the project that will cause changes in the next requested phase of the project?**
   N/A