

Fiscal Year 2016-17 Information Technology Request

University of Northern Colorado *Wireless and Network Infrastructure Upgrade*

PROGRAM PLAN STATUS and OIT BEST PRACTICES

2017-019

Approved Program Plan? Date Approved:

The university states that this project and network design align with industry best practices for network operation, including end user policies, authenticated access, and encryption. The project will follow Project Management Institute project implementation strategies.

PRIORITY NUMBERS

| Prioritized By | Priority | |
|----------------|----------|--|
| DeptInst | 1 of 1 | |
| CCHE | 25 of 31 | |
| OSPB | 37 of 46 | Not prioritized. Not recommended for funding |

PRIOR APPROPRIATION AND REQUEST INFORMATION

| Fund Source | Prior Approp. | FY 2016-17 | FY 2017-18 | Future Requests | Total Cost |
|--------------|---------------|--------------------|------------|-----------------|--------------------|
| CCF | \$0 | \$3,123,300 | \$0 | \$0 | \$3,123,300 |
| Total | \$0 | \$3,123,300 | \$0 | \$0 | \$3,123,300 |

ITEMIZED COST INFORMATION

| Cost Item | Prior Approp. | FY 2016-17 | FY 2017-18 | Future Requests | Total Cost |
|-----------------------|---------------|--------------------|------------|-----------------|--------------------|
| Land Acquisition | \$0 | \$0 | \$0 | \$0 | \$0 |
| Professional Services | \$0 | \$52,500 | \$0 | \$0 | \$52,500 |
| Construction | \$0 | \$0 | \$0 | \$0 | \$0 |
| Equipment | \$0 | \$2,970,800 | \$0 | \$0 | \$2,970,800 |
| Miscellaneous | \$0 | \$0 | \$0 | \$0 | \$0 |
| Contingency | \$0 | \$100,000 | \$0 | \$0 | \$100,000 |
| Software Acquisition | \$0 | \$0 | \$0 | \$0 | \$0 |
| Total | \$0 | \$3,123,300 | \$0 | \$0 | \$3,123,300 |

PROJECT STATUS

This is a new, never-before requested project.

PROJECT DESCRIPTION / SCOPE OF WORK

The University of Northern Colorado (UNC) is requesting state funds to replace its wireless and network infrastructure, including controllers, wireless access points, switches, and cabling, over the course of nine to ten months. The university says that it has prepared for the upgrade by making investments in bandwidth, border network devices, intrusion prevention, power upgrades, and staffing. The project goals include:

- replacing aging and failing equipment;
- increasing wireless coverage and bandwidth in academic and residential buildings;
- meeting student and faculty bandwidth expectations;
- providing power over Ethernet (PoE) for new wireless access points and other network devices;

Fiscal Year 2016-17 Information Technology Request

University of Northern Colorado

Wireless and Network Infrastructure Upgrade

- allowing greater integration between building automation and life safety systems;
- preventing surges, brownouts, and power losses to network equipment; and
- increasing overall campus network security.

The university states that this upgrade will bring UNC technology up to current needs and standards and provide five to seven years of service without the need for further upgrades.

PROJECT JUSTIFICATION

According to UNC, its current wireless and network infrastructure is approximately seven to eight years old. The university contends that the existing wireless technology is failing and has reached the end of its useful life. Specifically, UNC indicates that the two Cisco wireless services modules' (WiSMs) hardware and software support agreements are nearing expiration and the university is over capacity on licensing with no redundancy if one or both WiSMs fail. Additionally, 15 network switches failed during the 2014-15 academic year, with another three failing since July 1, 2015.

The university says that students in a modern educational environment use multiple computing devices and require additional bandwidth for high definition media use. Additionally, building automation (e.g., thermostats and door locks) and life safety (e.g., fire alarms and security cameras) use wireless technology. The university hopes to utilize PoE to provide greater bandwidth to students and better integrate building and life safety functions.

PROGRAM INFORMATION AND IMPLEMENTATION PLAN

UNC employs several different IT-specific project managers and will assign one to this project to review the original scope. The university plans to hold a kickoff meeting, which stakeholders and technical staff will attend where project policies and procedures will be reviewed, including the change management procedure. Network closets will be built in parallel and switched over during well-defined network maintenance windows. According to the university, access point installations will be scheduled with building coordinators and communicated through the change management process. Training will be provided through online sessions with Cisco. The university has an IT governance group that includes academic, student, and administrative units, which will play a key role in the implementation and change management processes.

COST SAVINGS / IMPROVED PERFORMANCE OUTCOMES

The university was unable to quantify cost savings attributable to the project and did not perform a cost benefit analysis. It discussed a number of project alternatives, including taking no action, using multiple vendors or a single vendor other than Cisco to find the best price on equipment, and implementing the project slowly over several phases, but rejected these alternatives.

SECURITY AND BACKUP / DISASTER RECOVERY

The university explains that this project will allow it to build a redundant and robust network infrastructure that will allow for the integration of life safety and security devices across campus. The increased capabilities, which include higher levels of encryption and security features, will allow for cameras and other devices to be installed where power might not have been previously available.

BUSINESS PROCESS ANALYSIS

The university says that the inadequacies of the existing wireless and network infrastructure were identified through the campus project process and discussions with key leaders at the university. Students signed a petition asking for more bandwidth and better wireless coverage. Upon being alerted to the students' concerns, the university began studying technology requirements and identifying equipment that had reached the end of its useful life. The conclusion reached by this study was to work with Cisco on a two-part implementation. To that end, the university has already increased bandwidth, border router capabilities, and reliability of power. UNC indicates that it talked to several public private institutions about alternatives and decided that an all-at-once approach to the second part of

Fiscal Year 2016-17 Information Technology Request

University of Northern Colorado

Wireless and Network Infrastructure Upgrade

the implementation plan was appropriate in order to take advantage of opportunities for bulk purchasing discounts.

PROJECT SCHEDULE

| | Start Date | Completion Date |
|---------------------------|------------|-----------------|
| Contracting | May 2016 | July 2016 |
| Design and Implementation | May 2016 | January 2017 |
| Completion | | February 2017 |

OPERATING BUDGET

UNC currently has the appropriate staff needed to support this project and the associated ongoing maintenance. The upgrade would require an additional \$40,000 per year in maintenance agreements for new networking gear. The university intends to absorb this additional cost moving forward.

STAFF QUESTIONS AND ISSUES

1. Has the current wireless network failed during the 2014-15 academic year? If so, how many times or what percentage of time has it been down?

The UNC wireless system as a whole has not failed during the 2014-2015, however we have had 17 wireless access points fail.

2. Please explain the current power capacity and its inability to power modern wireless access points and other IT equipment.

Our current Cisco 3750 Power of Ethernet (PoE) switches have a power capacity of 540Watts. Below is a list of general network devices powered by our edge network:

Cisco IP Phones 7911, 7936, 7937, 7940, 7941, 7942, 7945, 7960, 7961, 7965, 8831, 9951, 9971 use between 6.3Watts – 13.5Watts

Axis IP Cameras – 15.4Watts

Cisco Wireless Access points – 15.4Watts

GAI-Tronics SIP phones – 15.4Watts

UNC's enterprise environment utilizes one network drop for both computer and phone service per person and often we run into power consumption issues at the edge level given number PoE device per 48 port switch. UNC is already behind in wireless deployment for modern wireless technology 802.11ac. Wireless AC requires PoE + capable switches as well as increased power consumption of 16.1Watts.

3. What equipment is currently failing and in need of replacement?

Our two WiSM's are end of life on hardware and software support. We are currently over capacity on licensing (150 access points per WiSM) with no redundancy if one or both WiSM's fail. We have also had 15 Cisco 3750 switches fail over the 2014-2015 academic year which we were fortunate to replace via SmartNet RMA until 7-1-15 when all Cisco 3750 switches became End of Life. As of 7-1-15 we have already had 3 Cisco 3750 switches fail with no support for replacement.

4. What are the life safety and security devices that the network relies upon?

Our campus utilizes our edge switch environment to power a total 3,400 VoIP phones, 84 of which are for Area of Shelter and Refuge locations as well as 29 emergency pole phones for campus emergency notifications and 911. We also support building automation systems such as fire alarms and HVAC alarms for our data centers via the edge

Fiscal Year 2016-17 Information Technology Request

University of Northern Colorado

Wireless and Network Infrastructure Upgrade

network. As for campus security we have 405 network IP cameras in various buildings and outdoor spaces.

5. Please explain the current levels and features of UNC's network security.

The UNC infrastructure includes the following security systems:

Unified Threat management -

Intrusion Prevention

Intrusion Detection

Data Leak Prevention

Web Application Controls

Anti-Malware inspection

Network Architecture and Analysis Tools -

Firewalls

Device by Device ACL's

Traffic Shaping

Penetration and Vulnerability Scans

Proxy Servers

Security Information Event Management (SEIM)

Log Analysis and Aggregation Tools