2022 PROJECT PROPOSAL CHECKLIST

2023-25 Biennium Four-year Higher Education Scoring Process

INSTITUTION	CAMPUS LOCATION
380 - Western Washington University	Bellingham
PROJECT TITLE	OFM/CBS Project #
Critical Safety, Access Control, and Fiber Optic Network Upgrades	30000604
PROJECT CATEGORY	FPMT UNIQUE FACILITY ID # (OR NA)
Replacement - Standalone	Click or tap here to enter text.
PROPOSAL IS	
New or Updated Proposal (for scoring)	Resubmitted Proposal (retain prior score)
☐ New proposal ☐ Resubmittal to be scored (more than 2 biennia old or significantly changed)	☐ Resubmittal from 2018 (2019-21 biennium) ☒ Resubmittal from 2020 (2021-23 biennium)
CONTACT	PHONE NUMBER
Brian A. Ross	360.650.6539

Proposal content

- ☒ Project Proposal Checklist: this form; one for each proposal
- ☒ Project Proposal Form: Specific to category/subcategory (10-page limit)
- ☒ Appendices: templates, forms, exhibits and supporting/supplemental documentation for scoring.

Institutional priority

- ☒ Institutional Priority Form. Sent separately (not in this packet).

Check the corresponding boxes below if the proposed project meets the minimum threshold or if the item listed is provided in the proposal submittal.

Minimum thresholds

- ☒ Project is not an exclusive enterprise function such as a bookstore, dormitory, or contract food service.
- ☒ Project meets LEED Silver Standard requirements.
- ☒ Institution has a greenhouse gas emissions reduction policy in place in accordance with RCW 70A.45.050 and vehicle emissions reduction policy in place per RCW 47.01.440 or RCW 43.160.020 as applicable.
- ☐ A complete predesign report was submitted to OFM by July 1, 2022 and approved.
- ☐ Growth proposals: Based on solid enrollment projections and is more cost-effectively providing enrollment access than alternatives such as university centers and distance learning.
- ☐ Renovation proposals: Project should cost between 60 – 80% of current replacement value and extend the useful life of the facility by at least 25 years.
- ☐ Acquisition proposals: Land acquisition is not related to a current facility funding request.
- ☒ Infrastructure proposals: Project is not a facility repair project.

2022 PROJECT PROPOSAL CHECKLIST

2023-25 Biennium Four-year Higher Education Scoring Process

☐ Stand-alone, infrastructure and acquisition proposals is a single project requesting funds for one biennium.

Required appendices

☒ Project cost estimate: Excel C-100

☐ Degree Totals and Targets template to indicate the number of Bachelors, High Demand and Advanced degrees expected to be awarded in 2023. (Required for Overarching Criteria scoring criteria for Major Growth, Renovation, Replacement and Research proposals).

☐ Availability of Space/Campus Utilization template for the campus where the project is located. (Required for all categories/subcategories except Infrastructure and Acquisition proposals).

☐ Assignable Square Feet template to indicate program-related space allocation. (Required for Growth, Renovation and Replacement proposals, all categories/subcategories).

Optional appendices

Attach supplemental and supporting project documentation, *limit to materials directly related to and needed for the evaluation criteria*, such as:

☐ Degree and enrollment growth projections

☒ Selected excerpts from institutional plans

☐ Data on instructional and/or research space utilization

☐ Additional documentation for selected cost comparables (acquisition)

☐ Selected materials on facility conditions

☐ Selected materials on code compliance

☐ Tables supporting calculation of program space allocations, weighted average facility age, etc.

☐ Evidence of consistency of proposed research projects with state, regional, or local economic development plans

☐ Evidence of availability of non-state matching funds

☒ Selected documentation of prior facility failures, high-cost maintenance, and/or system unreliability for infrastructure projects

☐ Documentation of professional assessment of costs for land acquisition, land cleanup, and infrastructure projects

☒ Selected documentation of engineering studies, site survey and recommendations, or opinion letters for infrastructure and land cleanup projects

☐ Other: Click or tap here to enter text.

I certify that the above checked items indicate either that the proposed project meets the minimum thresholds, or the corresponding items have been included in this submittal.

Name: Brian A. Ross Title: Associate Director, Capital Budget

Signature: Electronic Signature Date: 8.8.2022

INSTITUTION	CAMPUS
Western Washington University	**Bellingham**
PROJECT TITLE	
Critical Safety, Access Control, and Fiber Optic Network Upgrades	

SUMMARY NARRATIVE

- **Problem statement**

Western Washington University has two urgent and interrelated infrastructure needs that need to be solved in a single, consolidated effort. Western must replace and expand the campus fiber optic network, which has reached the end of its expected life and constrains growth in academic instruction; fire and life safety systems; business operations; and building automated control systems.

Most significantly, the current fiber network constrains Western's ability to make urgently needed changes to the campus electronic access control system. Existing manual and electronic locks are no longer adequate to meet campus efficiency, safety, and security obligations. In response to recent national active shooter events, the campus emergency management committee recommended two key improvements to campus security: expanding electronic access control capacity and installing manual classroom locks operable from the inside. This project proposes implementation of both recommendations.

Finally, the importance of having a uniform access control system across campus has been underscored by the demands of providing a safe workplace during the COVID pandemic, as handling physical keys requires personal contact which could be avoided.

- **Project description**

The project would replace the existing damaged and undersized fiber optic communications system between and within buildings and install electronic controls on exterior doors and designated high security internal doors of all major academic buildings. The project will also install new hardware on classroom doors to enable locking from the inside in the case of an active shooter emergency.

UPDATE: The project will also move the campus data center from Administrative Services Center (approximately 1/2 mile from the southern campus border) to the Communications Facility (on campus) in order to improve network reliability and make the access control more resilient.

Overall, these upgrades will enable Western to meet the continuing mission-critical communication and life safety needs of students, faculty, and staff. A unified electronic access control system will simplify and improve campus building access and security; provide improved integration with other security systems such as video monitoring and intrusion detection; and simplify dispatch functions during emergency responses. Manual classroom locks operable from the inside form a last line of defense should an active shooter incident ever occur.

This project is proposed to accomplish the following:

- Replace the existing campus fiber optic network, including improving efficiency by combining stand-alone switches and controllers to reduce space, power, and cooling needs.
- Upgrade power to network equipment closets to include emergency power and cooling.
- Bring affected data communication conduits and cable trays into electrical code compliance by

removing abandoned electrical cable and adding new trays where necessary.

- Reduce operating costs by reducing or eliminating the need for daily manual locking and opening of academic buildings and by consolidating existing dedicated networks, such as Building Automation Control, onto a common high-capacity backbone.
- Provide centralized lockdown functionality to facilitate more agile, appropriate, and effective response capabilities in the event of a campus emergency.
- Provide classrooms with internally lockable doors so that students and faculty can effectively take shelter under the "Run, Hide, Fight" response to an active shooter.

- **History of project or facility**

This project scope represents the convergence of several studies and plans completed over past biennia, as well as the opportunity for construction efficiencies as similar work can be accomplished within buildings in a single contract.

A 2017 Utilities Master Plan Update suggested that the existing fiber network supporting the Fire, Security Alarm, Access Control, and Building Automated Control systems are at capacity and should be replaced to maintain current service delivery and support future growth.

In the 2017-2019 biennium, Western received funding to separate its existing access control system from the fire alarm system. During the design stage of that project, the designer confirmed the recommendation in the Utilities Master Plan Update (in the Telecommunications Section), concluding that scattered damage to the existing 20-year-old fiber loop, the ever-increasing reliance of academic and business operations on web-based applications, and emerging technologies in building operating systems are stretching the fiber loop to its capacity. The section addressing the fiber loop is included in Appendix E.

Concurrently, in response to recent national active shooter events, the campus emergency management committee was charged with recommending strategies to improve campus safety and security. That committee identified the risks and operational shortcomings of relying on manual keying systems that are obsolete and failing or which do not provide the technical functionality required to safeguard buildings and facilities quickly and effectively. Lessons learned from active shooter events around the country pointed at two key improvements:

- Lockdown: The committee recommended expanding electronic access control capacity to improve safety and security across campus. Electronic access controls would be installed on exterior doors, sensitive areas, and selected high use labs. This would allow for immediate lockdown of campus, for securing buildings automatically on a schedule for non-working hours, and for providing an electronic record credentials used for access.
- Classroom Locks: The Final Report of the Sandy Hook Advisory Commission strongly recommended "a standard requiring classroom and other safe-haven areas to have doors that can be locked from the inside." The Commission's research indicated that "there has never been an event in which an active shooter breached a locked classroom door." Western's emergency management committee urged the adoption of that standard for campus classrooms.

More recently, the demands of the COVID pandemic have highlighted the mission-critical nature of data communications for all university services. The institution's resilience in the face of evolving and increasingly unpredictable challenges hinges on a robust data network.

UPDATE: In the 2021-23 biennium, Western received partial funding ($2.15 million) that will implement over 23,000 feet of fiber (of the approximately 155,000 total), 63 exterior access control locks (of the 290 total), and 100 classroom/lab lock upgrades. In 2023-25, Western is requesting the remainder of funding, for a total of $15 million. The $15 million includes the inflationary adjustments to finish the scope of work as well as moving the data center from Administrative Services Center (approximately 1/2 mile from the southern campus border) to the Communications Facility (on campus). During project design efforts over the past year, it was determined that moving the data center to the Communications Facility will reduce the

overall amount of fiber renewal/replacement associated with this project and improve network reliability across campus. Overall, the data center re-location will make access control more resilient.

- **University programs addressed or encompassed by the project**

A robust fiber optic network is crucial for virtually all the university's academic programs, administrative activities, and student services, beginning with the foundation of safe, accessible spaces and continuing to provide a technologically relevant, modern education, offering flexibility for changing conditions, supporting communications and learning opportunities, and allowing efficient administration. Expansion of electronic access controls, which is severely constrained without upgrading the fiber optic loop, will improve the security of campus buildings and enhance the safety of those who study and work in them.

GENERAL CATEGORY SCORING CRITERIA

1. Significant health, safety, and code issues

A. **While Western's facilities comply with current life safety codes, the completion of this project assures that conformance is not jeopardized by failing network equipment.** Life safety systems depend on efficient notification to the monitoring agency, which at Western is the University Police Department. The campus fiber optic network is the spine that provides this vital communication link.

B. **This project would improve consistency with the following standards and codes:**

Campus Safety and Security Guidelines: Western has determined that emergency lockdown capability during an active shooter event is of paramount importance. Recommendations from active shooter analyses across the country have concluded that locking, blocking, or otherwise obstructing access to a classroom is a highly effective deterrent to an active shooter – thus an important lifesaving functionality. This new lockdown functionality will complement Western's emergency preparedness and response plans, which include text, cell phone, and voice notification.

Energy Code Compliance: Operation and management of RCW required high efficiency building systems and system components requires a reliable fiber network for communications. Western constantly monitors the performance of HVAC systems through a data analytics tool directly connected to the Siemens operating system. The data is transmitted over the fiber optic line to a central station in the physical plant, where trained technicians evaluate the performance of all systems to reveal performance anomalies and identify areas of potential energy savings. Over the past three years, this process of real time data analysis has saved Western over $200,000 per year in energy.

Fire Code Compliance: All fire safety system monitoring, alarms, and notification rely on the fiber optic loop to communicate with the central monitoring station in the University Police Dispatch Center, as well as with the City of Bellingham first responders.

ADA Accessibility: Electronic and classroom locks will improve ADA compliance and accessibility through modification of existing hardware. As electronic entries are installed, existing traditional doorknobs will be replaced with ADA compliant openers. Newly installed classroom locks will also be fully compliant with both Fire Code and ADA requirements.

2. Evidence of increased repairs and/or service interruption

Recent studies and subsequent evaluation of the condition of the fiber optic network as work has been performed suggest the network is approaching the end of its useful service life. The

university has outgrown its network, which was primarily installed in 1999-2000, in several key places. Physical cable degradation is evident in the campus utility tunnels, threatening the foundation of all network services on campus. Replacement is required to avoid service interruption in the event of network failure.

In addition, the existing fiber network has several bottlenecks in which the number of available fiber strands has nearly run out, including:

- Direct fiber connections between the two network cores.
- Direct fiber connections between primary and secondary data centers.
- Direct fiber connections between the primary network core/data center and the emergency operations center.

These constraints limit our ability to implement critical electronic access control systems on the consolidated network. Without the fiber replacement and expansion access control need a separate fiber network, which would add substantial cost to the project and to university operations overall.

Once fiber optic upgrades are complete, this project proposes to expand the use of electronic credentialing across campus, reducing need for traditional brass keys. Four years ago, in response to a lost ring of master keys, Western accelerated an internal project to rekey all of campus. The monumental effort to issue new keys to thousands of students and staff highlighted the vulnerability of access control dependent on traditional keys and the routine maintenance costs involved in tracking and replacing keys.

3. Impact on institutional operations without the infrastructure project

The fiber optic data network is essential to the delivery of all aspects of the educational mission. Nearly all academic and administrative functions depend on a reliable fiber optic communications infrastructure. Emergency response capabilities will be enhanced by electronic credentialing and lockdown functionality. A fully capable electronic access system is a risk mitigation strategy. Access to a building or space can be immediately rescinded upon report of a lost credential, reducing or eliminating concerns of unauthorized access.

Under the current operating model, Western's academic buildings are locked and opened by a team of University Police Department student employees according to established building schedules. This process can be nearly eliminated through an automated electronic locking system, saving up to two FTE salaries per year. In addition, the lower operating costs of using electronic credentials is well established in the security industry.

4. Reasonable estimate

The post-escalation MACC ($10,451,316) and Equipment ($1,950,873) cost identified in the C100 is based on unit and equipment cost associated with recent access control and fiber optic upgrade projects. Those projects include the Access Control Project funded with State funds in the 2017-19 biennium and fiber optic and switchgear equipment associated with several recent major and minor capital projects. Those calculations are included in Appendix B (Cost Breakdown) and match the MACC and equipment costs in the C100 (Appendix A).

5. Engineering study

Western has commissioned several studies about safety and utility condition. The consensus is overwhelming that data communications and robust access control are central to university operations.

In 2017, Western completed a utilities master plan update which identified the need to replace the

existing fiber network to meet current and predicted requirements.

In 2013, Western contracted with TRUSYS, an operational security assessment company, to define a roadmap for conversion of our existing access control system. This capital request reflects the recommendations of that study, included in Appendix C.

6. Support by planning

A. **As Western plans for enrollment and program growth, an expanded and modernized fiber optic network will be essential for supporting an upgraded access control system, along with virtually all other campus functions.** Western's Comprehensive Campus Master Plan contains six guiding principles for future campus development. This project is fully aligned with Principle #3: "Provide convenient and safe access to and through the campus for the University's guests, faculty, staff and students."

B. **Western's 2018 Strategic Plan requires that the University "provide technological and other academic infrastructure to support curricular innovation, research, scholarship, and creative activity, civic engagement and social justice" and that it ensure the safety and security of students and staff.** The fiber optic infrastructure, on which nearly all academic and business functions rely, is essential to campus operations. The maintenance and improvement of Western's security infrastructure is fully aligned with strategic intent.

   The proposed project supports the standards and procedures of the campus Access Control Policy, included in Appendix D.

7. Resource efficiency and sustainability

Western will be able to continue energy conservation and monitoring efforts through a fully capable fiber optic infrastructure. The electronic access component will lower maintenance and labor costs associated with physical key security and provide indirect energy conservation opportunities with the enhanced ability to manage access control of buildings. By limiting unauthorized access to academic buildings, conservation of resources can be managed more efficiently and effectively. Building controls will be tied to building and room occupancy, enabling selective heating and ventilation rather than whole building measures. Alarms on exterior doors will reduce the potential or duration of propped open doors, conserving energy within the buildings.

8. Appendices: the following supporting documentation is included

A. Project Cost Summary/C100
B. MACC and Equipment Cost Breakdown
C. WWU Access Control Assessment Report prepared by TRUSYS
D. WWU Access Control Policy
E. WWU Utilities Master Plan Update, Telecommunications Section

Appendix A

STATE OF WASHINGTON
AGENCY / INSTITUTION PROJECT COST SUMMARY

Updated June 2022

Agency	Western Washington University
Project Name	Critical Safety, Access Control, and Fiber Optic Network Upgrades
OFM Project Number	30000604

Contact Information	
Name	Brian Ross
Phone Number	360.650.6539
Email	brian.ross@wwu.edu

Statistics			
Gross Square Feet		MACC per Gross Square Foot	
Usable Square Feet		Escalated MACC per Gross Square Foot	
Alt Gross Unit of Measure			
Space Efficiency		A/E Fee Class	B
Construction Type	Other Sch. B Projects	A/E Fee Percentage	10.98%
Remodel	Yes	Projected Life of Asset (Years)	50
Additional Project Details			
Procurement Approach	DBB	Art Requirement Applies	No
Inflation Rate	4.90%	Higher Ed Institution	No
Sales Tax Rate %	8.80%	Location Used for Tax Rate	
Contingency Rate	10%		
Base Month (Estimate Date)	July-22	OFM UFI# (from FPMT, if available)	
Project Administered By	Agency		

Schedule			
Predesign Start		Predesign End	
Design Start	October-21	Design End	October-23
Construction Start	January-23	Construction End	June-25
Construction Duration	29 Months		

Green cells must be filled in by user

Project Cost Estimate

Total Project	**$15,761,983**	Total Project Escalated	**$17,015,052**
		Rounded Escalated Total	**$17,015,000**

Cost Estimate Summary

Acquisition

Acquisition Subtotal	**$0**	**Acquisition Subtotal Escalated**	**$0**

Consultant Services			
Predesign Services	$0		
Design Phase Services	$802,463		
Extra Services	$171,000		
Other Services	$360,527		
Design Services Contingency	$133,399		
Consultant Services Subtotal	**$1,467,390**	**Consultant Services Subtotal Escalated**	**$1,521,353**

Construction			
Maximum Allowable Construction Cost (MACC)	$9,628,999	Maximum Allowable Construction Cost (MACC) Escalated	$10,451,316
DBB Risk Contingencies	$0		
DBB Management	$0		
Owner Construction Contingency	$962,900		$1,045,132
Non-Taxable Items	$0		$0
Sales Tax	$932,087	Sales Tax Escalated	$1,011,687
Construction Subtotal	**$11,523,986**	**Construction Subtotal Escalated**	**$12,508,135**

Equipment			
Equipment	$1,652,000		
Sales Tax	$145,376		
Non-Taxable Items	$0		
Equipment Subtotal	**$1,797,376**	**Equipment Subtotal Escalated**	**$1,950,873**

Artwork			
Artwork Subtotal	**$0**	**Artwork Subtotal Escalated**	**$0**

Agency Project Administration			
Agency Project Administration Subtotal	$618,232		
DES Additional Services Subtotal	$0		
Other Project Admin Costs	$0		
Project Administration Subtotal	**$618,232**	**Project Administration Subtotal Escalated**	**$671,029**

Other Costs			
Other Costs Subtotal	**$355,000**	**Other Costs Subtotal Escalated**	**$363,662**

Project Cost Estimate			
Total Project	**$15,761,983**	Total Project Escalated	**$17,015,052**
		Rounded Escalated Total	**$17,015,000**

Funding Summary

	Project Cost (Escalated)	Funded in Prior Biennia	New Approp Request 2023-2025	2025-2027	Out Years
Acquisition					
Acquisition Subtotal	$0				**$0**
Consultant Services					
Consultant Services Subtotal	$1,521,353	$393,528	$1,127,825		**$0**
Construction					
Construction Subtotal	$12,508,135	$1,490,872	$11,017,264		**$0**
Equipment					
Equipment Subtotal	$1,950,873		$1,950,873		**$0**
Artwork					
Artwork Subtotal	$0				**$0**
Agency Project Administration					
Project Administration Subtotal	$671,029	$80,600	$590,429		**$0**
Other Costs					
Other Costs Subtotal	$363,662	$50,000	$313,662		**$0**
Project Cost Estimate					
Total Project	**$17,015,052**	**$2,015,000**	**$15,000,053**	**$0**	**-$1**
	$17,015,000	**$2,015,000**	**$15,000,000**	**$0**	**$0**
	Percentage requested as a new appropriation		**88%**		

What is planned for the requested new appropriation? (*Ex. Acquisition and design, phase 1 construction, etc.*)
See scope of work in MACC worksheet
Insert Row Here

What has been completed or is underway with a previous appropriation?
See scope of work in MACC worksheet (highlighted in blue)
Insert Row Here

What is planned with a future appropriation?
Insert Row Here

Cost Estimate Details

Acquisition Costs					
Item	**Base Amount**		**Escalation Factor**	**Escalated Cost**	**Notes**
Purchase/Lease					
Appraisal and Closing					
Right of Way					
Demolition					
Pre-Site Development					
Other					
Insert Row Here					
ACQUISITION TOTAL	**$0**		**NA**	**$0**	

Green cells must be filled in by user

Cost Estimate Details

Consultant Services				
Item	**Base Amount**	**Escalation Factor**	**Escalated Cost**	**Notes**
1) Pre-Schematic Design Services				
Programming/Site Analysis				
Environmental Analysis				
Predesign Study				
Other				
Insert Row Here				
Sub TOTAL	**$0**	**1.0000**	**$0**	Escalated to Design Start
2) Construction Documents				
A/E Basic Design Services	$802,463			69% of A/E Basic Services
Other				
Insert Row Here				
Sub TOTAL	**$802,463**	**1.0121**	**$812,174**	Escalated to Mid-Design
3) Extra Services				
Civil Design (Above Basic Svcs)				
Geotechnical Investigation				
Commissioning				
Site Survey				
Testing				
LEED Services				
Voice/Data Consultant				
Value Engineering				
Constructability Review				
Environmental Mitigation (EIS)				
Landscape Consultant				
Electrical Engineering	$78,000			
Travel & Per Diem	$40,000			
Advertising	$3,000			
Site Surveying and Testing	$50,000			
Sub TOTAL	**$171,000**	**1.0121**	**$173,070**	Escalated to Mid-Design
4) Other Services				
Bid/Construction/Closeout	$360,527			31% of A/E Basic Services
HVAC Balancing				
Staffing				
Other				
Insert Row Here				
Sub TOTAL	**$360,527**	**1.0854**	**$391,317**	Escalated to Mid-Const.
5) Design Services Contingency				
Design Services Contingency	$133,399			
Other				

Insert Row Here				
Sub TOTAL	**$133,399**	**1.0854**	**$144,792**	Escalated to Mid-Const.
CONSULTANT SERVICES TOTAL	**$1,467,390**		**$1,521,353**	

Green cells must be filled in by user

Cost Estimate Details

Construction Contracts					
Item	**Base Amount**		**Escalation Factor**	**Escalated Cost**	**Notes**
1) Site Work					
G10 - Site Preparation					
G20 - Site Improvements					
G30 - Site Mechanical Utilities					
G40 - Site Electrical Utilities					
G60 - Other Site Construction					
Other					
Insert Row Here					
Sub TOTAL	**$0**		**1.0244**	**$0**	
2) Related Project Costs					
Offsite Improvements					
City Utilities Relocation					
Parking Mitigation					
Stormwater Retention/Detention					
Other					
Insert Row Here					
Sub TOTAL	**$0**		**1.0244**	**$0**	
3) Facility Construction					
A10 - Foundations					
A20 - Basement Construction					
B10 - Superstructure					
B20 - Exterior Closure					
B30 - Roofing					
C10 - Interior Construction					
C20 - Stairs					
C30 - Interior Finishes					
D10 - Conveying					
D20 - Plumbing Systems					
D30 - HVAC Systems					
D40 - Fire Protection Systems					
D50 - Electrical Systems					
F10 - Special Construction					
F20 - Selective Demolition					
General Conditions					
MACC per "MACC Breakdown" in Appendix of proposal	$9,628,999				
Insert Row Here					
Sub TOTAL	**$9,628,999**		**1.0854**	**$10,451,316**	
4) Maximum Allowable Construction Cost					
MACC Sub TOTAL	**$9,628,999**			**$10,451,316**	
	NA			*NA per 0*	

This Section is Intentionally Left Blank

7) Owner Construction Contingency				
Allowance for Change Orders	$962,900			
Other				
Insert Row Here				
Sub TOTAL	**$962,900**	**1.0854**	**$1,045,132**	
8) Non-Taxable Items				
Other				
Insert Row Here				
Sub TOTAL	**$0**	**1.0854**	**$0**	
9) Sales Tax				
Sub TOTAL	**$932,087**		**$1,011,687**	
CONSTRUCTION CONTRACTS TOTAL	**$11,523,986**		**$12,508,135**	

Green cells must be filled in by user

Cost Estimate Details

Equipment					
Item	**Base Amount**		**Escalation Factor**	**Escalated Cost**	**Notes**
1) Equipment					
E10 - Equipment	$1,652,000				
E20 - Furnishings					
F10 - Special Construction					
Other					
Insert Row Here					
Sub TOTAL	**$1,652,000**		**1.0854**	**$1,793,081**	
2) Non Taxable Items					
Other					
Insert Row Here					
Sub TOTAL	**$0**		**1.0854**	**$0**	
3) Sales Tax					
Sub TOTAL	**$145,376**			**$157,792**	
EQUIPMENT TOTAL	**$1,797,376**			**$1,950,873**	

Green cells must be filled in by user

Cost Estimate Details

Artwork					
Item	**Base Amount**		**Escalation Factor**	**Escalated Cost**	**Notes**
1) Artwork					
Project Artwork	$0				0.5% of total project cost for new construction
Higher Ed Artwork	$0				0.5% of total project cost for new and renewal construction
Other					
Insert Row Here					
ARTWORK TOTAL	**$0**		**NA**	**$0**	

Green cells must be filled in by user

Cost Estimate Details

Project Management					
Item	**Base Amount**		**Escalation Factor**	**Escalated Cost**	**Notes**
1) Agency Project Management					
Agency Project Management	$618,232				
Additional Services					
Other					
Insert Row Here					
Subtotal of Other	*$0*				
PROJECT MANAGEMENT TOTAL	**$618,232**		**1.0854**	**$671,029**	

Green cells must be filled in by user

Cost Estimate Details

Other Costs					
Item	**Base Amount**		**Escalation Factor**	**Escalated Cost**	**Notes**
Mitigation Costs					
Hazardous Material Remediation/Removal					
Historic and Archeological Mitigation					
Plan Review	$55,000				
In-Plant Services	$300,000				
OTHER COSTS TOTAL	**$355,000**		**1.0244**	**$363,662**	

Green cells must be filled in by user

Appendix B

MACC and Equipment Cost Breakdown

Summary Statistics (Represents July 2022 Costs):

Average access control cost per door leaf per PW728	$18,375
Average conversion cost per door per PW728	$10,500
Average cost per network Switch per PW733 & 746	$45,000
Average cost per linear feet of fiber (includes material, labor, testing, replacement of existing infrastructure)	$9.17

Scope Included in 2021-23 Appropriation

MACC Cost

Exterior Access Control and Associated Fiber at Academic Buildings

Bldg Name	Access Door Count	Associated Linear Feet of Fiber	MACC
Communications Facility	23	5357	$ 471,749
Morse Hall	12	6876	$ 283,553
Biology Building	14	6555	$ 317,359
Fine Arts	14	4403	$ 297,626
Ross Engineering	15	6800	$ 337,981
Performing Arts Center	40	5900	$ 789,103
Arts Annex	20	6300	$ 425,271
Canada House	7	5700	$ 180,894
College Hall	7	4900	$ 173,558
Commissary	10	6600	$ 244,272
Environmental Studies	22	6350	$ 462,480
Fairhaven Academic	3	3500	$ 87,220
Haggard Hall	17	7550	$ 381,609
High Street Hall	13	6000	$ 293,895
Humanities	16	7050	$ 358,649
Old Main	26	9850	$ 568,075
Steam Plant	7	6800	$ 190,981
Wilson Library	17	8950	$ 394,447
Fiber to prior converted buildings	7	44150	$ 533,481
Total	***290***	***159,591***	**$ 6,792,199**

Other

Scope	Cost/unit	# of Units/feet	MACC
Interior Doors under Access Control	$10,000/door	30 doors	$ 300,000
Classroom Locks	$1056/door	300 doors	$ 316,800
Lab wireless access locks	$2200/unit	100 Labs	$ 220,000
Data Center			$ 2,000,000
Total			**$ 2,836,800**

Pre-escalated MACC $ 9,628,999

Equipment Cost

Associated Equipment in the Buildings

Bldg Name	# of network switches	Cost
Fine Arts	1	$ 45,000
SMATE	2	$ 90,000
Ross Engineering	2	$ 90,000
Performing Arts Center	2	$ 90,000
Arts Annex	1	$ 45,000
Canada House	1	$ 45,000
College Hall	1	$ 45,000
Commissary	1	$ 45,000
Environmental Studies	2	$ 90,000
Fairhaven Academic	1	$ 45,000
Haggard Hall	2	$ 90,000
High Street Hall	2	$ 90,000
Humanities	2	$ 90,000
Old Main	2	$ 90,000
Steam Plant	1	$ 45,000
Wilson Library	2	$ 90,000
Bond Hall	4	$ 167,000
Academic Instruction Center	2	$ 90,000
Campus Services	2	$ 90,000
Fraser Hall	2	$ 90,000
Miller Hall	2	$ 90,000
Total Network Switches	**37**	

Total Equipment Cost $ 1,652,000

Appendix C

TRUSYS

WESTERN WASHINGTON UNIVERSITY

ACCESS CONTROL SYSTEM ROADMAP

Dave Miller, Principal, TRUSYS

March 15, 2013

CONTENTS

EXECUTIVE SUMMARY 4
ISSUE 4
RECOMMENDATION 4
ROADMAP 5
EXISTING SYSTEM 5
5-POINT ROADMAP 5
DEFINE REQUIREMENTS 5
ASSESS FEASIBILITY & COSTS 7
PLAN & DESIGN 7
PROCUREMENT & INSTALLATION 7
OPERATION 8
ALTERNATIVE 8
SUMMARY 8
BUDGETS 9
ACCESS CONTROL SYSTEM 9
INTRUSION DETECTION SYSTEM 10
VIDEO MANAGEMENT SYSTEM 11
OTHER SERVICES 11
ROADMAP PONTS 1 & 2 11
MANUFACTURER SELECTION PROCESS 11
BUDGETARY TIMELINE 12
PERSONNEL 12
DISPATCH 12
SYSTEM OPERATIONS 12
SUMMARY 14
APPENDIX A - EXISTING SYSTEM: EST-3 SYNERGY 15
CONFIGURATION & SOFTWARE 15
EXISTING IDS 15
CREDENTIAL SYSTEMS 16
INTEGRATION OF INTRUSION & VIDEO 16
SECURITY TECHNOLOGY PLAN 17
PERSONNEL & BUDGETS 17
APPENDIX B - SECURITY TECHNOLOGY IN THE MARKET TODAY 19
VIDEO MANAGEMENT SYSTEM (VMS) 19
ACCESS CONTROL BEST PRACTICES 19

CONCEPT....19
BEST PRACTICES RECOMMENDATION....21
INTERIM BEST PRACTICES....21
SYSTEM INTEGRATION....21
RECOMMENDATION....22
TECHNOLOGY RECOMMENDATIONS....22
EDGE TECHNOLOGY....23
CONTROL HARDWARE....23
ACS SOFTWARE....24
SUMMARY....25
INTEGRATED SYSTEMS VS. STAND-ALONE....25
APPENDIX C - SECURITY PLAN COMMENTS....27
BUILDING BLOCKS....27
TEAMS....28
TECHNIQUES....29
TECHNOLOGIES....29
TRAINING....29
ISSUES FOR CONSIDERATION IN A SECURITY PLAN....30
APPENDIX D - RESULTS OF REQUIRED VS. DESIRED ASSESSMENT....31
SUMMARY....33
BUDGETARY ESTIMATE FIGURE 1: TIMELINE (ENLARGED VIEW)....35

EXECUTIVE SUMMARY

Western Washington University (WWU) has contracted **TRUSYS** to provide a Roadmap detailing how to move forward with the implementation of the replacement for the Access Control System (ACS) at WWU.

ISSUE

The WWU process to date has created an impasse between two different approaches. The first approach advocates an immediate upgrade of the system due to funds being available in this biennium.

The other approach is to defer the replacement of the system as long as possible until it is no longer supported by the manufacturer. This approach is advocated by some within WWU so that badly needed capital dollars can be deferred for other projects as long as possible.

The need for replacing the ACS has been brought on by the following:

1. The need for distributed administrative control of the access control due to the inability to address it through staffing.
2. The pending "end of life" declaration that will be issued for the access control portion of the integrated EST system, and the future roll-out of the EST-4 which will make the access control portion of the system obsolete.

RECOMMENDATION

The key points to **TRUSYS**' recommendation are:

- Defer Replacement of the ACS for two to three years.
- Cease investment in current ACS
- Implement a 5-Point Roadmap for replacement of the Access Control System.

The 5-Points of the Roadmap are:

1. Define Requirements
2. Assess Feasibility & Costs
3. Plan and Design System Replacement
4. Procurement and Implementation
5. Operation of System

By following this Roadmap, WWU can achieve an access control system that can meet their growing needs and expectations, and that can be incorporated into their overall Security Plan.

ROADMAP

EXISTING SYSTEM

The existing ACS can continue to meet WWU's basic needs for the next two to three years. It is recommended that investment in customizing the EST ACS be stopped due to the following considerations:

- Creating the ACDB into a custom software application that is only understood by a limited number of people at WWU could be highly disruptive and expensive if WWU can no longer support the ACDB internally.
- Outside vendors may, or may not, be able to support a customized system.
- The cost in customization of ACDB would only bring it to what most ACS manufacturers offer today which makes the Return on Investment (ROI) questionable.

TRUSYS recommends that a moratorium be placed on any additions or modifications to the EST-3 Synergy access control system with the following exceptions:

1. New construction with exterior doors and audio/visual components that require monitoring. Where interior access control doors and intrusion detection are desired, a Risk Assessment should be provided to determine the risk associated, and the Assessment determines an immediate need for Security Technology. Infrastructure such as boxes, conduit stub-outs, conduit runs, and pull strings should be provided for the future devices.
2. Remodeled space that meets the criteria in Item 1 of this list.
3. Other spaces where a Risk Assessment determines an immediate need for Security Technology.

If more detailed information about the existing ACS is required, please refer to Appendix A.

5-POINT ROADMAP

TRUSYS recommends a 5-Point Roadmap to obtain an upgraded and operational access control system.

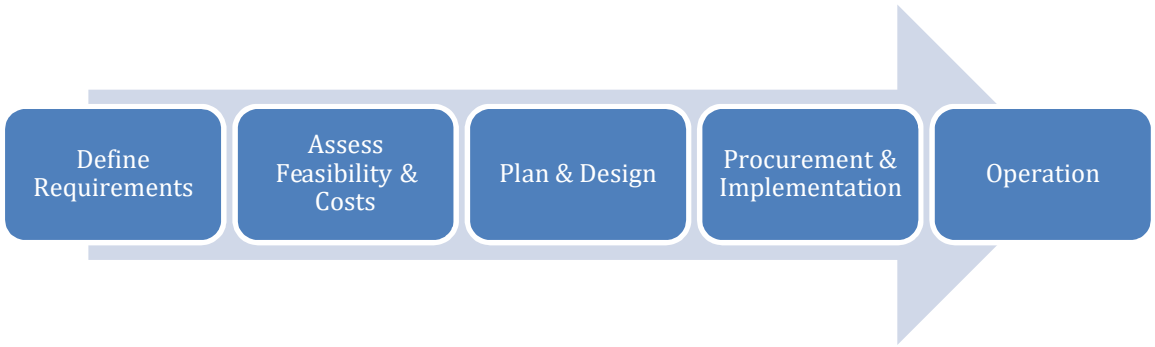


Figure 1 - 5-Point Roadmap

DEFINE REQUIREMENTS

The definition of requirements should be based on two levels:

1. The overall Security Plan and how the ACS will be integrated with other security technologies.
2. The technical requirements of the Access Control System.

SECURTY PLAN

A Security Plan that encompasses all aspects of security at WWU will be defined. It would assess key aspects such as:

Figure 2 - Security Plan

Commentary on a Security Plan can be found in Appendix C.

ACCESS CONTROL TECHNOLOGY

Technology issues that require definition for the new ACS are:

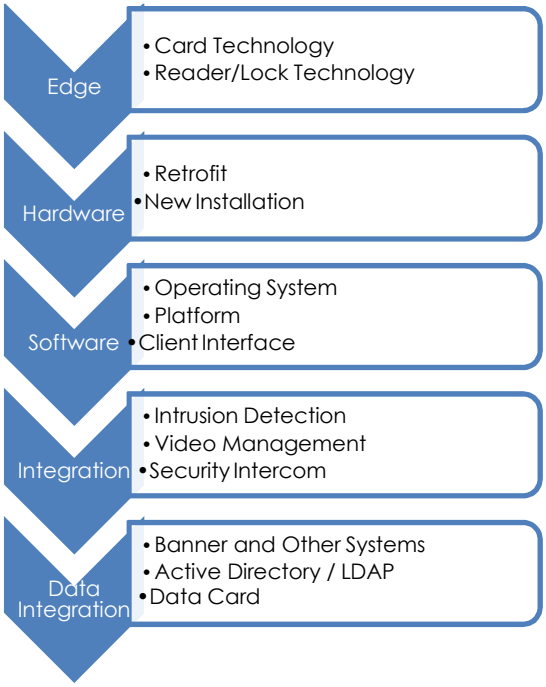


Figure 3 - Defining ACS Requirements

Commentary on current Security Technology can be found in Appendix B.

ASSESS FEASIBILITY & COSTS

Using the Requirements that are developed for the Security Plan and Access Control, the various avenues that are available for implementation should be evaluated for their feasibility and costs. Examples of these approaches include:

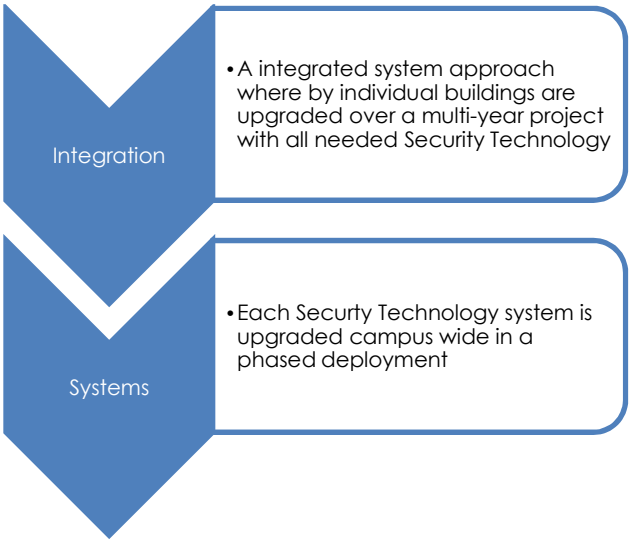


Figure 4 - Example Approaches

Each approach should be evaluated based on costs and impact to existing systems and operations.

PLAN & DESIGN

WWU should quantify the desired approach into a systematic plan that incorporates the defined requirements.

This stage will have deliverables such as:

Tasks	Tasks
Manufacturer Selection	Cards, Card Readers & Reader/Locks Control Hardware Software
System Plans	Detailed, Shop Drawing Level
Specifications	Specific to Project, Integrated with Plans
Budget Estimates	Detailed, Based on Specified System(s)

Figure 5 – Plan & Design

PROCUREMENT & INSTALLATION

Based upon the approach to be taken, the system(s) will be Procured and Implemented. Using accepted project management practices, the implementation process will be tightly controlled to ensure that the specified solution is installed.

System commissioning will be a major focus, which will lead to system acceptance by WWU.

OPERATION

Following system acceptance by WWU, the new technology will be used in a manner that supports the overall Security Plan for WWU.

ALTERNATIVE

If it is determined that the budgeted funds from the current biennium for the replacement of the Access Control System will be lost if no action is taken, then the following should be done:

1. Engage a consultant to specify and design a new ACS system which would include at a minimum:
   a. Determination of the optimum solution for smart card technology, readers and integrated reader/locks, or if the use of Proximity technologies be maintained.
   b. Determination of a hardware manufacturer that has the broadest range of ACS hardware that can support the chosen technologies.
   c. Qualify and select an ACS manufacturer who can provide the technology solution determined in Items 1 and 2 above.
2. Design and specify the system upgrade.
3. Receive quotations from authorized resellers of the ACS manufacturer selected in Item 1 above.

Development of a Security Plan including future Security Technology updates and integration should be done, following the recommended 5-Point Roadmap.

SUMMARY

By deferring for 24 to 36 months, the replacement of the Access Control System, Western Washington University can assure itself of enough time to implement the 5-Point Roadmap so that a cohesive and well thought out Security Plan and Security Technology Plan can be implemented.

BUDGETS

Both low and high budgets have been prepared and the Tables below summarize the differences and provide the assumptions that have been made.

The Consultant Design Fees quoted are based on a detailed design that would be created, and would effectively eliminate the need for shop drawings to be submitted by the contractor.

ACCESS CONTROL SYSTEM

Assumption	Low	High
Quantity of ACS Panels	32: Replaces only those panels that have existing ACS doors at this time.	59: Replaces all SAC-3 cards in existing FACP with new ACS control panel.
ACS Panel Location	Assumes that new ACS panel will be located in the same room as the existing EST panel.	Assumes that new ACS panel will be located in the same room as the existing EST panel.
Upgrades HID Prox to Smart Card Reader (Dual Tech)	212	212
Wireless Access Points	13: Provides wireless access points for conversion of 54 stand-alone reader/lock combinations.	13: Provides wireless access points for conversion of 54 stand-alone reader/lock combinations.
Upgrade of older style Stand-Alone reader/locks to Wireless	44	54
Convert AD-200 to AD-400	10	0
New RS-485 wiring for door modules	150' average per existing door.	300' average per existing door.
Software	1 Server License 320 Door Reader Licenses 2 Thick Client Stations 10 Concurrent Thin Client Stations 3 Data Base Integration Licenses	1 Server License 320 Door Reader Licenses 2 Thick Client Stations 10 Concurrent Thin Client Stations 3 Data Base Integration Licenses
System Budgetary Estimate:	$832,000	$1,143,000
Software Support	$6,000/year based on parameters indicated.	$6,667/year based on parameters indicated.
Consultant Design Fee	$149,640	$205,632

Budgetary Estimate Table 1: ACS

Savings can be obtained if it is determined that the existing RS-485 wiring can be used in lieu of providing new wiring.

INTRUSION DETECTION SYSTEM

Instead of trying to determine how much new wiring would be required from a single intrusion detection system (IDS) panel to the various devices and RCC-7s in each building, the approach of installing a minimum of one (1) IDS panel per building or 1 per RCC-7 where there are multiple locations in a building has been applied.

Assumption	Low	High
Quantity of IDS Panels	79: Assumes that where only 1 IDS point is indicated on the inventory, that it could be monitored by ACS.	88: When IDS devices are indicated, provides a minimum of one per building, or one per RCC-7 location.
IDS Panel Location	Typically RCC-7 location or central location such as MDF/IDF.	Typically RCC-7 location or central location such as MDF/IDF.
New wiring for devices & keypads	125' average per existing device or keypad.	200' average per existing device or keypad.
Software	1 Integration License per IDS Panel.	1 Integration License per IDS Panel.
Existing Devices	Assumes that all existing devices can be re-used.	Assumes that all existing devices can be re-used.
System Budgetary Estimate:	$510,645	$568,220
Consultant Design Fee	$91,916	$102,280

Budgetary Estimate Table 2: IDS

Savings can be obtained if it is determined that when a building has a small amount of devices, i.e. 1 to 10, that they can be re-wired to the ACS system controller which will have this capacity.

VIDEO MANAGEMENT SYSTEM

Assumption	Low	High
Quantity of Servers	2	2
Storage Capacity	24 TB	24 TB
Cameras	Use existing cameras with video encoders to convert analog to IP signal.	Install new IP cameras with new CAT 6 cabling to each camera.
Software Licensing	Assumes 1 license per camera for integration with ACS.	Assumes 2 licenses per camera (1 ACS/1 VMS) for integration with ACS.
System Budgetary Estimate:	$149,616	$321,660
Software Support	$1,870/year based on parameters indicated.	$4,194/year based on parameters indicated.
Consultant Design Fee	$26,931	$57,899

Budgetary Estimate Table 3: VMS

OTHER SERVICES

There are other recommended services that are not included with the Consultant Design Fees noted above.

ROADMAP PONTS 1 & 2

The above Consultant Design Fees do not include the first two points on the 5-Point Roadmap:

- Define Requirements
- Assess Feasibility & Costs

A budget range of $16,000 to $32,000 is suggested for this depending on the scope of services to be provided by a consultant. This does not include travel expenses which would likely run at 15% to 20% of the fee.

MANUFACTURER SELECTION PROCESS

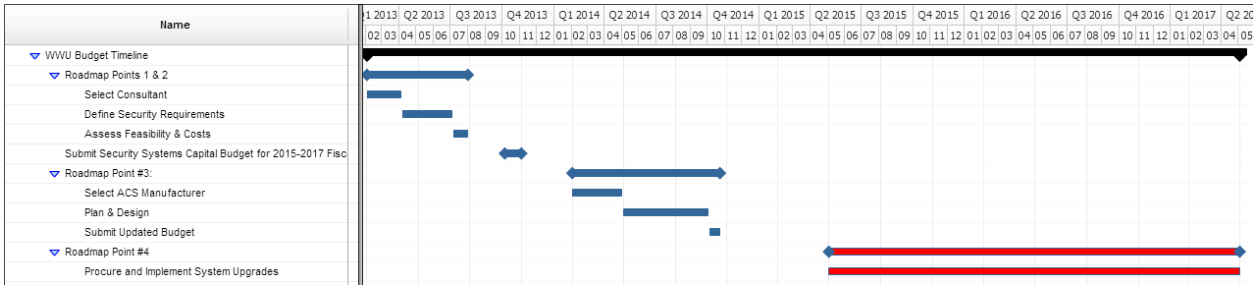
The detailed selection process for determining card technology, reader/lock technology, hardware, and system software is not included with the Consultant Design Fees noted above.

A budget range of $13,000 to $19,000 is suggested for this depending on the scope of services to be provided by a consultant. This does not include travel expenses which would likely run at 15% to 20% of the fee.

BUDGETARY TIMELINE

The following timeline is based upon the following assumptions:

1. That WWU will be able to find funding for Road Map Points 1 & 2, and Manufacturer Selection in 2013.
2. Funding for system design can occur in the 2nd half of 2014.
3. Funding for system replacements can occur in 2015/2017 biennium.



Budgetary Estimate Figure 1: Timeline

A larger view of this timeline is added at the end of the report.

PERSONNEL

TRUSYS has been asked to provide manpower recommendations for two aspects of the systems at WWU.

DISPATCH

Currently dispatch is operating with five (5) full time dispatchers for a 24/7 operation with no supervisor currently in place. The following, based on a discussion with Chief Randy Stegmeier, the following is considered the optimum personnel needed.

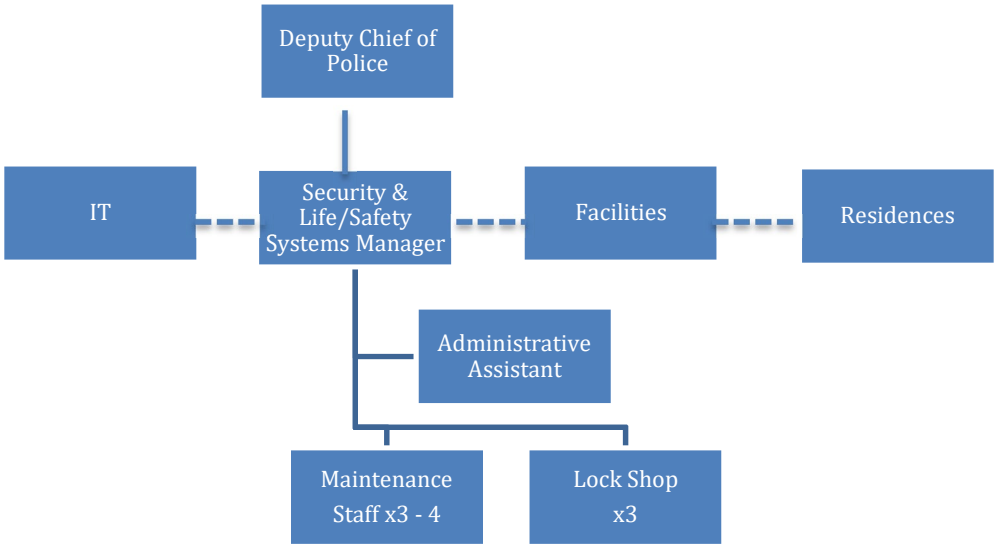
- 1 – Supervisor: The Supervisor will have the additional duties of covering sick or unexpectedly absent dispatchers, and to be the Terminal Agency Coordinator.
- 6 – Dispatchers: This will allow normal eight (8) hour shift coverage and minimize overtime. The Chief expressed a desire to have shifts maintained for a six (6) month duration, and then rotation can occur.
- 2 – Part Time Dispatchers: These are envisioned to be on call dispatchers to cover sickness and unexpected absences or short-term planned absences such as vacations. They are envisioned to be eligible for up to 16-hours per person per month, unless covering for a longer term duration such as a maternity leave.

SYSTEM OPERATIONS

Upon systems being installed, including fire alarm and mass notification, they become tools for dispatchers to be notified of conditions that affect the health, safety and welfare of the students, faculty and staff at WWU. Under this premise, it would make sense that the same entity that has authority over the dispatchers would have the ability to control the systems including their maintenance.

The Organizational Chart shown below has been provided with this in mind. The Systems Manager would have bilateral relationships with counterparts in IT, Facilities, and Residence Halls.

The Systems Manager would be the stakeholder representative for systems during capital project planning and implementation to ensure that collaboratively published system design requirements are adhered to, and that these systems are not compromised due to "value engineering".



Budgetary Estimate Figure 2: Systems Team

There are not to **TRUSYS**' knowledge, published standards or metrics for how many personnel are required for the maintenance and ongoing support of security systems.

SYSTEMS MAINTENANCE

The current maintenance of two (2) seems to be low, and does not allow for coverage of the campus should one of the two need to take an extended absence. WWU has begun to address this by training more personnel. The team should be able to be more efficient in maintaining the combined fire/life safety systems and security systems if one or two full time employees are added to this segment of the systems team.

LOCK SHOP

With the administration of the system moved to the System Manager and the Administrative Assistant, the Lock Shop should be able to fully focus on its purpose of lock maintenance and repair, issuing of "brass keys" and rekeying of locks.

The existing staff of three (3) should be sufficient for this task.

SUMMARY

The following are the budgetary estimates by system, and for the consultant cost by Roadmap point. Where we have felt that clarification was needed in the parts of the Roadmap Point, we have indicated the cost associated with the part.

System	Low	High
Access Control	$ 832,000	$1,143,000
Intrusion Detection	$ 510,645	$ 568,220
Video Management	$ 149,616	$ 321,660
Systems Costs Total	$1,492,261	$2,032,880

Budgetary Estimate Table 4: Systems Budget Summary

System	Low	High	Timeline
Roadmap Points 1 & 2 Define Requirements & Feasibility/Costs	$ 16,000	$ 32,000	April 2013 – Sept. 2013
Roadmap Point 3	$201,365	$291,358	April 2014 – Dec. 2014
Select ACS Manufacturer	$ 13,000	$ 19,000	April 2014 – June 2014
Design & Specification (All Systems)	$201,365	$272,358	July 2014 – Dec. 2014
Roadmap Point 4 (All Systems) Procurement & Implementation	$ 67,122	$ 91,453	July 2015 – June 2017
Total Consultant Budget	$284,487	$414,811	

Budgetary Estimate Table 5: Systems Budget Summary

Note: Consultant fee does not include travel expenses which typically be estimated at an average of 15% of the fee amount.

APPENDIX A - EXISTING SYSTEM: EST-3 SYNERGY

CONFIGURATION & SOFTWARE

The existing access control system (ACS) is an integrated component of the EST-3 fire alarm system. The security portion of the system, trade named as Synergy, has been in the market place since the early 2000's.

EST has gone through two (2) corporate buyouts, and since 2005 EST has been directed by corporate not to upgrade and improve the system technology as it is considered to be a competing product with several security product lines within GE and UTC.

- GE Security Purchases EST in 2005
- UTC Purchases GE Security in 2010

The ACDB while "state of the art" at the time of its release in the early 2000's has seen little development since its initial offering. The ACDB uses Delphi with JET engine as the data base language which is not commonly used in the development of data base applications today. Discussions have occurred between EST and WWU, where WWU would be given the source code for the ACDB, and have the ability to modify the ACDB for improvements that are deemed necessary. EST would be released from all liability associated with the source code being provided, and would only be obligated to support WWU should EST adopt any of the changes for their product offering. Based on previous history, it appears unlikely that EST would adopt these modifications.

EST has clearly stated that while a defined end-of-life date has not yet been published, that the ACS will in the near term of 2 to 3 years likely not be supported. The SAC-3 communications card and the CRC modules have been on the discontinued products price list for several years, but these parts are available with up to a two (2) week lead time.

The ACS is accessed and programmed via a separate ACDB server from the Fireworks stations. The Lock Shop manages card holders and credentials on the ACDB via a client station and communicates via modem to the respective panels.

The system panels are currently networked across a dedicated multi-mode fiber optic network. This network allows the EST-3 Synergy (fire alarm, mass notification, and security components) to be networked using TCP/IP. The "ring" topology of the fiber optic network makes it highly resilient.

Where ACS is currently installed within a building on the campus, the security system resides on the EST system using one of two formats:

- SAC-3 using RS-485: Keypads and Card Reader Controller (CRC)
- Addressable SLC: Security Devices; i.e. door contacts, motion sensors, audio/visual (A/V) alarms, via input modules

The CRC modules currently support HID Corporate 1000 Proximity technology card readers. With the exception of the CRC module all door devices and components could be retrofitted into a new system.

EXISTING IDS

The existing IDS is an integral part of the EST-3 Synergy system. The system is comprised of centrally located zone modules and distributed zone modules. In some cases, the

same area of the building might be served by both centrally located zones and distributed zones.

The centrally located zones located in RCC-7 enclosures in MDF and IDF rooms are relatively easily upgraded.

The field located security devices are not as easily upgraded to a new system infrastructure as they can reside on the same circuit as fire alarm devices.

Keypads will likely need to be rewired when the RS-485 circuit is taken over by the new access control system.

CREDENTIAL SYSTEMS

For the purpose of this report, a credential is any method that allows an authorized user access via a door into a building or space.

The vast majority of credentials issued at WWU are "brass keys". Keys are issued either via the Lock Shop which reports to the WWU Campus Police Chief or via the resident hall management system using their in-house developed "Keys" database.

When resident dormitory room keys have been lost, and not recovered within a predetermined time period, residence management notifies the Lock Shop of the need to rekey the affected door(s) and issue new keys.

Access control "cards" in the form of actual cards or fobs are issued on an as needed basis via the Lock Shop. WWU ID cards are not currently integrated with an access control card.

The "cards" are used to access three (3) different access control systems on the campus. The majority of card readers are on the EST-3 Synergy system with approximately 165 readers currently in use.

The other two systems are "stand-alone" door readers which must be programmed into a software program and then upload via a handheld device. The older stand-alone system is being phased out in lieu of the Schlage AD-200 system. The AD-200 integrated locksets have the capability to be upgraded from a stand-alone product to a 900 MHz wireless network product or to a Wiegand product using an RS-485 protocol. There are 46 stand-alone readers at WWU today.

INTEGRATION OF INTRUSION & VIDEO

The integration of intrusion detection system (IDS) is well integrated with the ACS on the EST-3 platform.

The integration of video is not well integrated with the EST-3 Synergy. Dispatch personnel were only able to identify five (5) cameras that could be viewed on alarm conditions from the EST-3 system.

The campus cameras are displayed on a single monitor in Dispatch. Dispatchers are not able to view camera thumbnails in full displayed view. In Dispatch there is no control of pan/tilt/zoom (PTZ) cameras on Campus.

Recorded video cannot be viewed from Dispatch.

SECURITY TECHNOLOGY PLAN

TRUSYS found that Security Technologies at WWU have been implemented as budgets and personnel have been available over the last 10-15 years and there has not been a Security Plan guiding implementation.

For example, there are numerous and disparate systems in Police Dispatch where the primary dispatcher's location has nine (9) "systems" that can provide "alarm" data and that requires observation or require interface by the dispatcher:

1. Emergency Phones
2. Web MSS (Runs license plates and driver licenses, but not the same system as in the officers' cars.)
3. ARMS – CAD and Incident Reporting
4. Voice Recording System
5. "Access Systems" for arming/disarming intrusion area when called on phone by occupant.
6. Aiphone – Audio/video system for access to the Campus Police building.
7. Fireworks – Fire and Security Annunciation of alarms.
8. HVAC Alarms – Operated for two weeks during summer leave period.
9. Video (CCTV) Camera Monitor (see notes above on integration)

In addition to the systems noted above, the dispatchers are tasked with answering the following audio systems or components:

1. Safe Phone (650-SAFE)
2. Primary Phone (3555 – non-emergency, 3911 – emergency)
3. Primary Phone (duplicate for when audio recording is required)
4. Emergency Call System Radio
5. Primary Police Radio desktop and portable
6. Parking Radio
7. Hard Line Phone (off campus)
8. TTY
9. Aiphone

Security Technology must work in a cohesive manner that allows the University's first responders to support those in need, and to create a document trail for incident response and reporting.

PERSONNEL & BUDGETS

The existing ACS is maintained by the "fire alarm shop". This two person team, David Holmwood and Lane Weaver, are exceptionally talented. They have developed capabilities on the EST-3 network that have been adopted by EST for the product line. This team reports to Facilities Management - Operations.

The Lock Shop is supervised by Kevin Conforti, and the administration of the card databases is performed by Ethan Van Diest. It reports directly to the WWU Chief of Police.

TRUSYS found three (3) common constraints during interviews with all stakeholders.

1. Funding is insufficient to support the work required to maintain the existing ACS.

2. There is uncertainty of the ability to obtain funding for a new and expanded ACS.
3. There is not a single person accountable and responsible for the maintenance and operation of the ACS; and who has the authority to make daily operational decisions using a prescribed standard of operation.

These opinions are not specific only to those personnel noted above, but was a general theme voiced by all that were interviewed.

APPENDIX B - SECURITY TECHNOLOGY IN THE MARKET TODAY

This section will provide a brief update on Video Management Systems (VMS), ACS Best Practices, and System Integration. These comments are based on **TRUSYS**' experience.

VIDEO MANAGEMENT SYSTEM (VMS)

VMS, formerly called CCTV, is the fastest growing area in the security industry. The use of megapixel IP-based cameras is driving this growth. Camera manufacturers are focused on creating better resolution by pairing higher quality lenses with ever increasing megapixel sensors.

To counter ever increasing resource demand on Network Video Recorder (NVR) processor bandwidth and storage requirements, the following trends have been identified:

- Movement to "Edge" processing of camera analytics. Cameras are now built with sufficient processing power to determine if there is a rules based need to have the video images recorded at the VMS and to alert monitoring personnel.
- Many cameras now have a built in ability to record video images to an SD card; thus allowing onboard storage for later upload to the VMS during off-peak transmission periods.
- Use of H.264 video format instead of MPEG and MPEG4.

There is a growing trend to use "purpose-built" servers and storage devices to run the VMS software and to store video. These manufacturers have partnered with VMS manufacturers to certify the manufacturers' VMS software on their purpose-built hardware solutions. **TRUSYS** recommends this approach as a best practice versus using commercial, off the shelf (COTS) solutions such as Dell, IBM and HP.

Two key areas that continue to require development are:

1. The ability to provide "backup" power to cameras and recording systems so that they can continue to operate during the loss of primary power.
2. The ability of high megapixel cameras to work in low and adverse light conditions.

ACCESS CONTROL BEST PRACTICES

CONCEPT

The best "Best Practice" that a client can implement is to create a Security Technology Plan (STP) that can be replicated. The STP should be part of the documented Security Plan, and should be made available to the contracted design team each time a new building or remodel is to be undertaken.

The use of an STP will minimize the cost of designing additions to the ACS, and provide savings for the maintenance of the system by minimizing the spare parts that should be maintained on site.

The SDS can minimize the impact of operating the system as well. A strong and resolute STP can ensure that items such as IDS keypads are included for areas where arming and disarming of the IDS is required, instead of allowing it to be "value engineered" (VE) out of the design. This VE has occurred at WWU, and areas are now armed & disarmed over the phone with the Campus Police Dispatch.

The STP should take into consideration the following:

1. Cost of Installation
2. Cost of Maintenance
3. Capabilities of Internal Resources
4. Capabilities of External Resource

By developing and adhering to a Security Technology Plan, each client can develop their own "best practices", because what is best for one owner may not work for the next owner.

Practical Application

TRUSYS has broken ACS Best Practices into two levels, Tactical and Strategic.

Tactical level best practices are those that can be ascribed to such issues as power supply configurations and mounting configurations of various door components. These are considerations that can be left to the design stage of the project.

Strategic level best practices are those that impact the overall operation of the system or dictate how the infrastructure will be placed within a building. It is these Strategic considerations that must be customized to each individual client's needs.

The best consensus in the industry today, is that there is no consensus. This can best be exemplified that for access control (and security in general) that unlike fire alarm systems, there are not Codes and Standards which dictate when to install these systems, and more importantly, how they shall be installed.

The following are examples of where accepted best practices are being challenged:

1. Centrally Located Control Hardware:
   A common practice has been to locate ACS control hardware and power supplies in a central location for an entire building, or for larger buildings in multiple locations. These configurations typically consisted of a custom enclosure for housing the ACS modules and power supplies for powering electronics and door locks. Often times a 4' x 8' space would have to be dedicated in the room where the equipment was to be located.
   New technology such as IP-based door controllers and integrated wireless and Wi-Fi reader/locks have begun to financially incentivize clients to move to a "distributed" technology format, and also minimize the centrally located space that is needed.
   In the case the one **TRUSYS** client, they chose to remain with a central configuration that required a very expensive two-door, 4' x 5' enclosure with redundant levels of power supplies and that required cooling fans due to heat generation. This was the best practice adopted by the client based on their risk and cost assessment.
2. Wire Exterior Doors
   It has been a commonly accepted practice since the inception of wireless communication technologies to only have wired doors on the exterior of a building. This was due to the long lag times for the wireless technology to achieve lockdown from a central command input.

   Advances in battery efficiency coupled with better technology now have wireless technology that can achieve lockdown in 10 seconds. Is the 10 second

window an acceptable risk to the client? Is the cost savings that can be achieved using this technology worth the potential risk of doors being delayed for locking on demand? The greater frequency of "handshake" between the wireless device and the system will have an impact on the device's battery life, thus an impact to operating cost.

WWU will likely continue to be challenged with budgets for the foreseeable future, and it is highly recommended that they review options like the above examples to determine their own best practices that balance cost vs. risk.

BEST PRACTICES RECOMMENDATION

TRUSYS recommends that WWU create a Security Plan with an integral component being the Security Technology Plan for the University. The process of creating an encompassing Security Plan will create the best practices that will be prescribed by WWU.

INTERIM BEST PRACTICES

What should WWU do with the wiring infrastructure where ACS and IDS have to be added to the EST system in the interim period while the Security Plan is created and the new ACS is selected and installed?

RECOMMENDATIONS

1. Wiring from the EST Panel to the door for the CRC module:
   - Use the required unshielded, twisted – low capacitance cable required for the SAC-3 RS-485 circuit.
   - Future Wiring:
     - Provide a shielded, twisted 4-conductor cable
     - Consider the option of "home-running" one or two CAT-6 cables from each CRC to the EST-3 panel or to an MDF/IDF as a "future or spare".
2. Place keypads on a separate extension of the SAC-3 RS-485.
3. Do not mix security monitor modules on the same addressable loop as fire alarm devices.
4. Home run all security field devices such as door contacts, motion sensors, glass break sensors, etc… back to the RCC-7 locations. Do not use field located monitor modules for security purposes.

SYSTEM INTEGRATION

In the market place today, Access Control System (ACS) is the system around which security system integration is achieved. Many ACS manufacturers realize that they do not have the ability to design, develop and manufacturer all the needed systems such as intrusion detection (IDS), video management (VMS), and security intercom (SIS). Instead they turn to manufacturers of these systems and create partnerships.

The primary method of integration between each of these systems and the ACS is via TCP/IP network technology. To ensure interoperability between these systems, many ACS manufacturers offer their partners certification programs; thereby ensuring that as new versions of software are rolled out, the systems will continue to operate.

When considering an integrated system, the selection of an ACS manufacturer who has multiple partners is highly desired.

RECOMMENDATION

The following are the Milestones that **TRUSYS** recommends for achieving the desired integration:

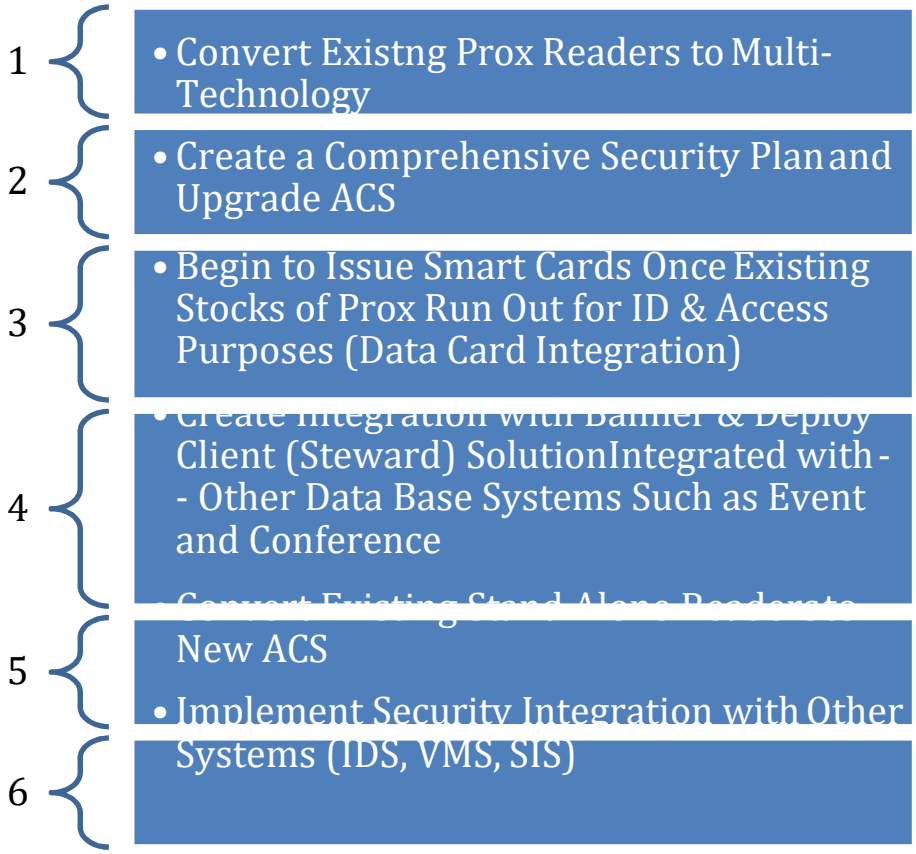


Figure 2: Recommended Milestones

Integration of the ACS with Banner, Data Card and the Event and Conference management systems can be accomplished using WWU's in-house resources, unless the ACS manufacturer has a "canned" integration that can be deployed effectively and efficiently.

TECHNOLOGY RECOMMENDATIONS

The following 3-step process should be adhered to regardless of whether the 5-Point Roadmap is used or the ACS is replaced immediately:

1. Determination of the optimum solution for smart card technology, readers and integrated reader/locks.
2. Determination of a hardware manufacturer that has the broadest range of ACS hardware that can support the chosen technologies.

3. Qualify and select an ACS manufacturer who can provide the technology solution determined in Items 1 and 2 above.

EDGE TECHNOLOGY

WWU should create a Request for Information to select the manufacturers who should be interviewed for their Smart Card and reader and integrated reader/lock technologies. Based on these interviews, a single source technology should be chosen for the Control Hardware selection.

CARD TECHNOLOGY

TRUSYS recommends that "Smart Card" technology be adopted at WWU. This will allow future upgrades of systems such as Dining, the Library, printing, etc… to leverage the existing Smart Card technology when they are migrated away from bar codes scanners and mag stripe readers. Most importantly, it will allow WWU to be proactive should WTA convert in the next few years to an ISO 14443 Compliant Application.

INTEGRATED READER/LOCK TECHNOLOGY

WWU should use Integrated Reader/Lock technology for the following applications:

- Exterior Doors where an ADA Door Operator will not be installed. These should be a wired, not a wireless or Wi-Fi configuration unless a delay in activation of a lock down is acceptable.
- Interior Doors as follows:
  - Doors behind which critical assets are maintained and managed or where instantaneous Lock Down is required: These should be a wired, not a wireless or Wi-Fi configuration unless a delay in activation of a lock down is acceptable.
  - All other interior doors: Wireless or Wi-Fi Configurations.

  Note: A Wi-Fi solution will be able to leverage WWU's existing Wi-Fi infrastructure if a VLAN can be created on that infrastructure and the system can be encrypted at 128-AES or higher to prevent hacking.

  A wireless solution of either 900 MHz or 2.4 GHz will require an additional infrastructure of wireless access points, but the technology is being directed to respond to a lock down signal within 10 seconds of activation. Faster response times are anticipated in the future.

CONTROL HARDWARE

WWU should select an ACS control hardware solution that works with the smart card reader and integrated smart card reader/lock technology chosen above.

The two primary "open" platforms for access control controller hardware are Mercury and HID VertX. Mercury appears, in the opinion of **TRUSYS**, to have a larger percentage of ACS system manufacturers who have chosen this hardware solution, and both primary manufacturers of integrated reader/locks have integrations with the Mercury hardware solution.

Issues that need to be addressed prior to the new system's installation are:

1. What is the ability of the new system to use the existing wiring infrastructure?

Note: The existing system uses a non-shielded, twisted pair for the RS-485 communications to the CRCs. RS-485 is a robust serial communications protocol that is often specified with a shielded, twisted pair cable. Per Mercury, the shield "drain" which is connected to the RS-485 terminal block is more for the purpose of creating a common ground reference than for electronic noise reduction. The common reference can be achieved by bonding all of the negative sides of the modules' power circuits (not lock power circuits) together and referencing them to ground.

The Mercury stated that they have run in house tests using unshielded CAT-5 cable, and using one of the conductors to create a ground reference at the power supply.

This approach assumes that the wiring is installed per the National Electrical Code (NEC) and that the cabling has not been simply laid along the top of ceiling areas where it can come into direct contact with fluorescent light ballast or other noise inducing components.

A two stage testing process to confirm this approach is recommended:
Stage 1: A lab test using the same cable that is currently installed
Stage 2: A single building installation that confirms operation prior to moving forward with a system wide replacement

2. Can the existing multi-mode fiber optic network be used for the TCP/IP communications for the new ACS?
   Note: This fiber network is extremely robust, and by using this network where the existing panels are located, it will help to minimize the installation cost of the new system by not requiring wiring runs between an MDF and/or IDF in the building.

   The decision can be made later whether or not to maintain the above practice or shift to an MDF/IDF model for buildings that have not yet had ACS installed.

3. Can the existing power supplies be used?
   Note: Should the power supplies provide any functions that are for the purpose of life safety, then new power supplies should be required for installation. If they are dedicated for the purposes of security, then it is highly likely that they could be reused.

ACS SOFTWARE

Once the card technology and associated readers and integrated reader/lock technology have been selected and the open control hardware platform selected, then ACS software manufacturers should be selected via an RFP for interview that can support the selected technologies.

Features that **TRUSYS** recommends focusing on during the RFP process are:

How does the ACS integrate with Banner and Data Card?

- How does the ACS software integrate with other 3rd Party Applications such as Event and Conference Management?

What Partners has the ACS manufacturer chosen for System Integration?

- How many VMS Partners have they Certified with their solution?
- How many IDS Partners have they Certified with their solution?
- Have they developed an alternative IDS solution such as using Mercury's keypad for IDS interface?

What is the software's ability to support "concurrent thin clients" and administrative functions needed at WWU?

What is the cost of ongoing licensing and software support agreements?

- Per individual or blocks of door reader licenses?
- Integration with 3rd Party data bases?
- Integration with Partner solutions such as IDS and VMS?
- Camera licensing, i.e. do they double charge?

Figure 3: ACS Software Issues

SUMMARY

WWU should select an ACS solution that meets their needs and expectations.

TRUSYS recommends that WWU develop a Security Plan before moving forward on any ACS Solution. Simply using a consultant to tell WWU how and what should be used for their ACS solution will lead to a short term, successful implementation, but will likely be a long term failure if a comprehensive Security Plan is not created and implemented.

INTEGRATED SYSTEMS VS. STAND-ALONE

TRUSYS recommends that an integrated systems approach be taken at WWU. The following path assumes that funds will be made available.

The following is Milestone 6 from Figure 2 above with more detail provided.

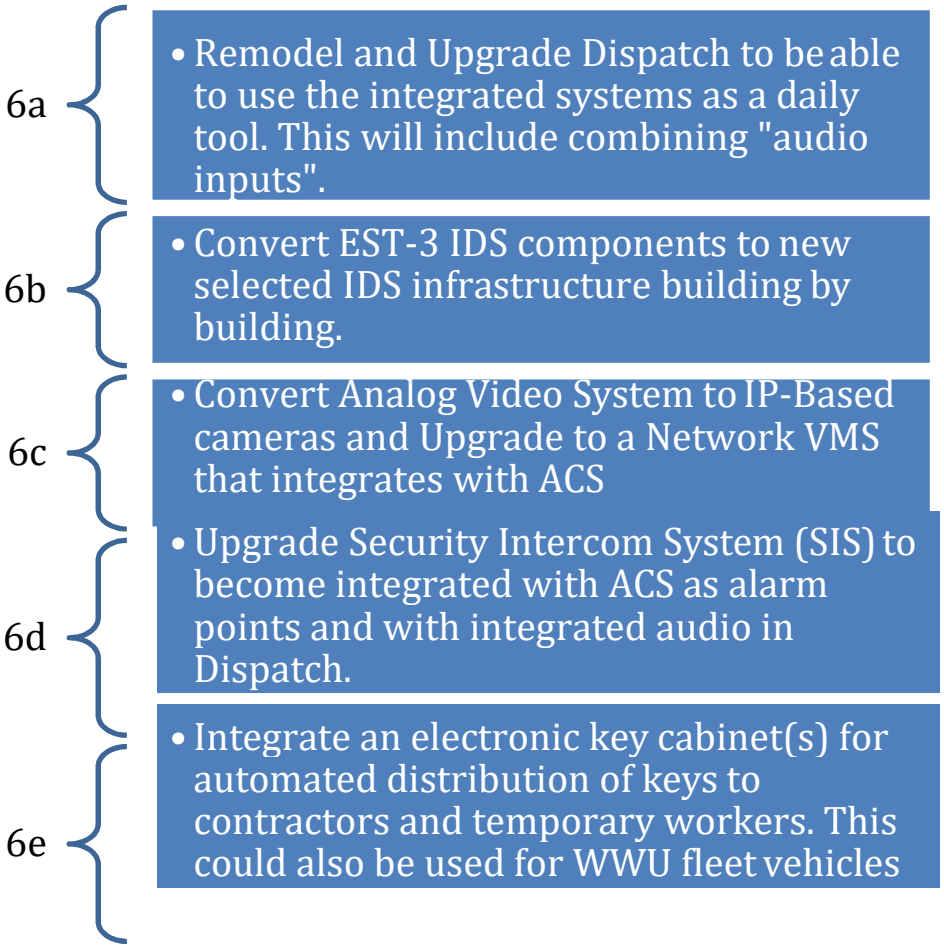


Figure 3: Recommended Milestones

APPENDIX C - SECURITY PLAN COMMENTS

A primary question that must be answered to create a Security Plan is what is the purpose or mission of security? Said in a different way, what is the role of security in supporting the mission of Western Washington University?

If Security Technology such as access control, video, audio communications, and intrusion detection cannot deter security events or be used as a tool to manage such an event it is likely to atrophy after its initial deployment.

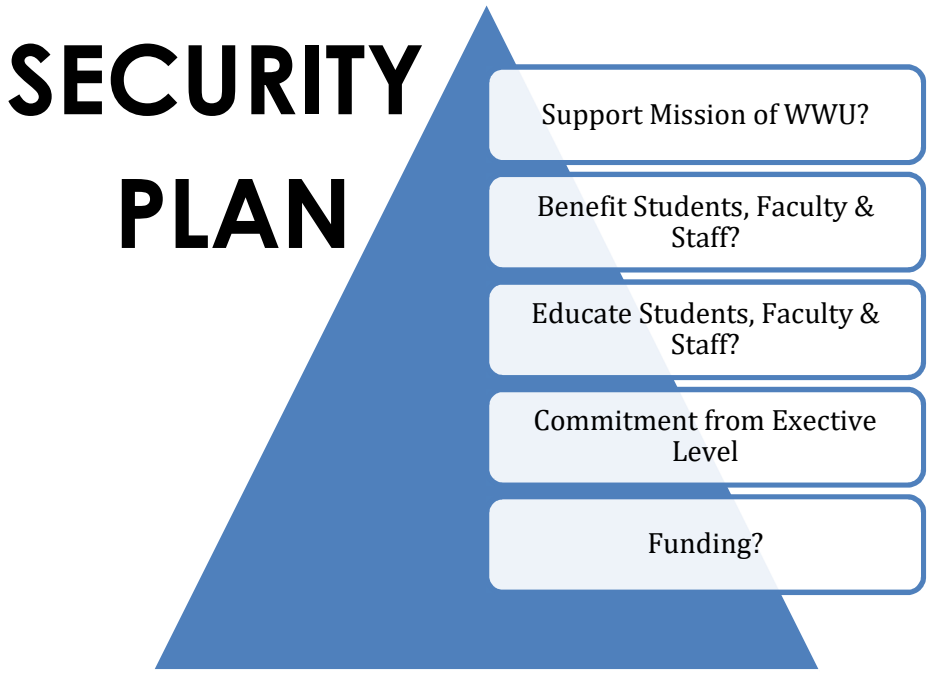


Figure 1: Critical Questions for Security Plan

The following are offered as key points for consideration in developing a Security Plan for WWU.

1. How will a Security Plan support the mission of WWU?
2. How will a Security Plan benefit students, faculty and staff at WWU?
3. How will students, faculty and staff be educated about the Security Plan at WWU; and how will that education process be appropriate for their status or position at WWU?
4. What is the commitment from the Executive level of WWU to a long term Security Plan?
5. What is the ability of WWU to fund a Security Plan?

BUILDING BLOCKS

The ability to build a resilient Security Plan will rest upon the ability of WWU to create key Building Blocks. **TRUSYS** has found that when the following building blocks are developed at functional, tactical and strategic levels that a resilient Security Plan can occur.

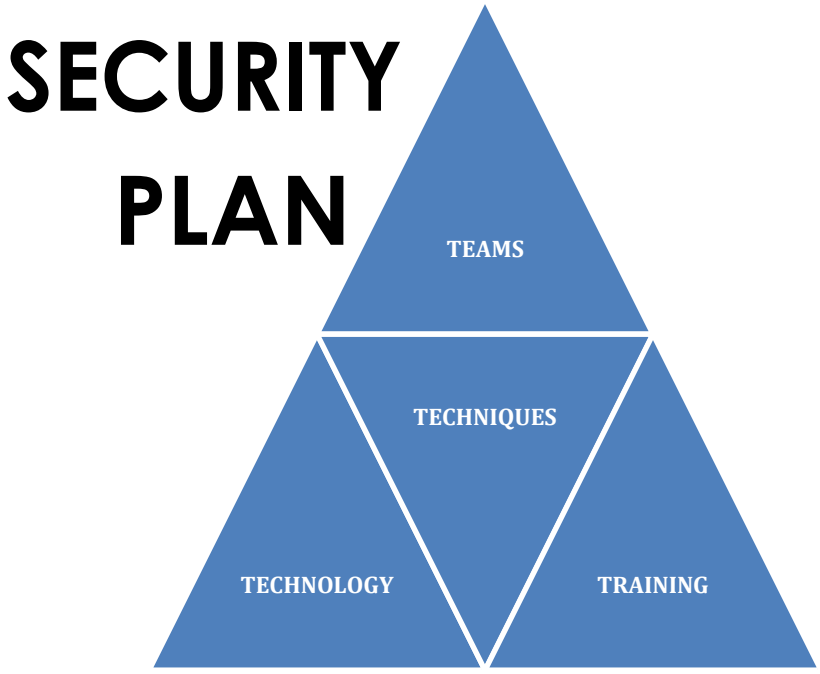


Figure 2: Building Blocks for Security Plan

1. Teams: People
2. Techniques: How to use Teams, Technology, and Training
3. Technology: Tools to assist and leverage the Security Plan
4. Training: The practical integration of Teams, Techniques, and Technology

TEAMS

Teams, Functional, Tactical, and Strategic, would be discerned during the planning and preparation of the Security Plan. The ability for the Security Plan to remain resilient and sustainable is based upon the collective strength of the employees, staff and stakeholders who comprise the various Teams.

There are several Functional Teams that are suggested to be formed and given operating parameters at WWU. They are:

1. Operations: This Team would be responsible for the daily operation and programming of the security technologies, including ACS. Note: As previously mentioned, it is highly desired to have a single management position that has accountability and responsibility for the daily operation of the Security Technology component, while still working within the Team environment. This should be considered as an "Exempt" position versus a "Classified" position at WWU.
2. Maintenance: This Team would likely be comprised of various trades from Facilities, IT, and the Lock Shop, and would have representation from the Operations Team.
3. Response: This would be primarily comprised of the Police Dispatch and Uniformed Officers.
4. Administrative: This would be comprised of all users with access to the client software, and who can assign privileges to card holders within their group and to

areas within their building(s). At the highest level this would include all areas including Residence Management, and could be comprised of smaller Teams that are based upon specific use areas/buildings on the campus or satellite areas.

Tactical Teams typically would be in response to a range of security events, with each Team appropriate to the level of the event.

There are two (2) apparent Strategic Teams that should be developed at WWU, with others that may be developed during the planning and preparation of the Security Plan.

1. Strategic Security Vision: This Team, similar to the Access Control Committee to whom this report is being submitted, would be responsible for the long range Security Plan. It would monitor the progress of the Security Plan to reach milestones and to audit its capabilities and effectiveness.

   Another primary task would be to secure funding for maintaining and operating the aspects of the Security Plan that are already in place, and to secure funding for upcoming milestones that are planned as enhancements or modifications to the Security Plan.

   All key stakeholders should be represented on this Team including a representative from the University President's or Provost's offices.

2. Strategic Response: This Team would function during security events where such things as press releases, press interviews, and notification to families arerequired.

TECHNIQUES

Teams must have Techniques based upon the task at hand, as well as on the structure of the organization, legislation, and stakeholder involvement. There can, of course, be different Techniques employed for different security events; however, at a minimum there are Assessment, Operational, and Compliance Techniques.

TECHNOLOGIES

In order to support the Teams and their Techniques, Technologies must be introduced based on strategies, how those strategies are employed, and the tasks that need to be accomplished. Technology must not drive the process; it must support the Teams and the Techniques that are employed to accomplish their mission.

TRAINING

Training is critical for implementing a successful Security Plan. Training must be continuous for all Teams, in all areas in which they are working. Without Training, the Teams will not be current in the Techniques or the Technologies they are using, or as new Techniques and Technologies emerge.

ISSUES FOR CONSIDERATION IN A SECURITY PLAN

The following are offered for consideration with this Roadmap approach.

1. Is there a commitment by WWU to develop a long term, comprehensive Security Plan?
2. Does WWU have the ability to provide the financial support for the following?
   a. Planning Phase
   b. Deployment of Initial Security Plan Technologies
   c. Cost of licensing and software support agreements needed for Security Technologies, and maintenance of said technology
   d. Funding for development and final planning of the identified milestones or those that will be identified as the Security Plan matures
3. Will satellite facilities such as Shannon Point Marine Center be included in the Security Plan? If yes, how many satellite locations are there, and what is the extent of their security needs?
4. Security Technology Considerations:
   a. What is the role of each specific Security Technology at WWU?
   b. What level of Security Technology integration is desired for WWU?
   c. What is the role of ACS for integrating other Security Technologies such as intrusion detection, video and audio emergency communications?
   d. What card and reader technology will be used at WWU?
      i. What are the policies and issues that need to be resolved for using this technology including the placement of pictures and personal information on the card?
      ii. What are the driving factors to move from Proximity technology to Smart Card technology such as WTA and other vendor type systems such as cafeteria, printing, and library?
   e. What are the specific needs for the transfer of data base information between systems such as Banner, Data Card, etc…?
   f. How will the integration of systems affect the ability of Campus Police Dispatch to efficiently work with the systems?
   g. Should advance training and remodel of Dispatch be considered as milestones for the Security Plan?

APPENDIX D - RESULTS OF REQUIRED VS. DESIRED ASSESSMENT

On January 28, 2013, TRUSYS facilitated an Access Control Stakeholder Meeting at WWU. It was attended by the members of the Access Control Replacement Committee and key stakeholders from WWU.

This meeting established that WWU does not have a clear and cohesive approach to which options and features/benefits should be incorporated either into the existing ACS or a new ACS.

The following are the results of a "Needs versus Wants" discussion regarding these new features for the WWU ACS:

Issue	Need	Want
Work with Existing Prox Readers		X
Work with WTA Now/Future	X	X
Logical Access Control	X	X
ISO 14443 Compliant Apps	X	X
Mag Stripe	X	
Bar Code	X	
NFC		X

Table 1: New Access Card

Several items, such as the new access card working with Whatcom Transit Authority (WTA), Logical Access Control and Compliance with ISO 14443 Apps are classified by the Stakeholders as being both Needs and Wants.

Issue	Need	Want
Desire to Continue with Existing Lock Hardware Manufacture?	X	X
Ability to Remotely Lockdown Exterior Doors?	X	
Ability to Remotely Lockdown Interior Doors?		X
Use of PoE Reader/Lock?	Cost	
Use of Wireless Reader/Lock?	Cost	
Use of Wi-Fi Reader/Lock?	Cost	

Table 2: New Reader/Lock Technology

Stakeholders were split on staying with the current Ingersoll Rand companies (Schlage and Von Duprin), with some advocating to maintain the relationship, and others expressing it as a Want.

Issue	Need	Want
Desire to Continue with Existing "Edge" (Distributed) Configuration?		X

Use of Low-Proprietary Hardware?	Cost
Use of High-Proprietary Hardware?	Cost
Use of Centralized, Wiegand?	Cost
Use of Distributed, Wiegand?	Cost
Use of Edge (Ethernet/PoE)?	Cost

Table 3: New ACS Hardware Configuration

When the subject of integrated reader/lock technology was broached, they were assessed to be a "Need" but cost is a principal driving issue.

The consensus of the group was that there is a desire to maintain the "distributed" configuration that exists with the system today. Again, the primary driving factor voiced by the group was, "What will the cost be?"

It is apparent from the responses, that a significant amount of the Stakeholders do not yet have a feel for how cost can be controlled with the use of some of the newer technology options that are available.

Issue	Answer
Desired Operating Software?	Linux
Desired Database?	Oracle
Desired Hardware (COTS, Appliance, VM)?	VMware
Client Stations?	1/Building Concurrent Licensing

Table 4: New ACS Software Configuration

The group was able to clearly articulate its preference for operating systems and data base engines.

Issue	Need	Want
3rd Party Integration w/IDS?	X	
3rd Party Integration w/VMS?	X	
3rd Party Integration w/SIS?	X	X
Incident Command System Integration?		X
Active Directory Integration?		X
Direct Banner Integration?		X
Banner Integration via Active Directory?		X
Direct Integration w/CollegeNet?		?
Direct Integration w/Event Management?		X
Direct Integration w/Conference Management?		X
Mobile Monitoring (handheld and/or laptop)?		X

Table 5: New ACS System & Data Integration

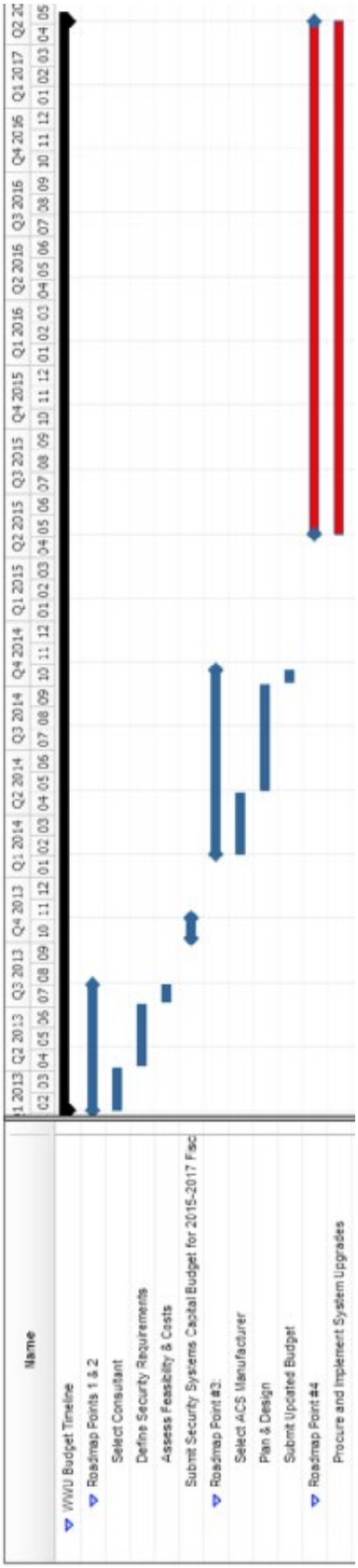
There is a "Need" to have an integrated system approach, and that the integration of data bases (Banner) and other scheduling systems (CollegeNet, Event Management, & Conference Management) with the ACS are highly desired.

SUMMARY

The repeated theme heard in the Stakeholders' Meeting and in individual interviews was that of cost, i.e. budget. Many Stakeholders are unclear on what the true cost of ownership will be for a new ACS, but general consensus is that an integrated system and data base approach is necessary and desired.

Figure 1: Uncertainty of Cost/Budget

BUDGETARY ESTIMATE FIGURE 1: TIMELINE (ENLARGED VIEW)



Appendix D

POLICY

Effective Date: September 1, 2015
Approved By: President Bruce Shepard

Authority: RCW 28B.35.120 SAAM Chapter 20
WAC 516-24-001

Cancels:	POL-U5610.01	Issuing and Using University Keys
See Also:	POL-U5346.03	Safeguarding University Assets
	POL-U5950.01	Health, Safety and Environmental Protection
	POL-U5400.01	Using University Resources
	POL-U5300.25	Reporting Loss of University Funds or Property

POL-U5710.01 MANAGING ACCESS TO UNIVERSITY FACILITIES

This policy applies to all faculty, staff, students, volunteers, guests or visitors who access University owned and leased facilities and space. Its purpose is to facilitate access to space and equipment by authorized individuals, to safeguard members of the Western Washington University community, and to minimize risk to both the University's property and the personal property of the individuals who work, study, and reside at Western.

Definitions:

Access Control – The means, methods and practices used to minimize risk to persons and property by regulating entry to buildings and spaces. Control activities may be preventative and/or detective.

Access Device – Any University-authorized device used to lock/unlock mechanical and electronic door hardware, including traditional metal keys, ID card, application and/or any other electronic means of access.

Area Access Manager – An Executive Officer, Chair, or Director of an academic or non-academic department designated to grant access privileges to individuals (i.e. faculty, staff, students, vendors and volunteers) for space over which they have been granted authority.

Access Control Administrator – A position designated to have operational oversight for access control to a defined grouping of buildings, facilities or spaces, and is responsible for determining operating hours.

Authorized Individual – An individual (i.e. University faculty, staff, student, volunteer or contractor) for whom certain access privileges have been granted by an Area Access Manager.

Departmental Key Controllers – Positions designated by an Area Access Manager to perform access administrative duties in accordance with University policies and procedures.

Sponsored Guest – A person who is present in a University building or space by way of an Authorized Individual.

POLICY

1. Vice President for Business and Financial Affairs Ensures an Appropriate and Effective Access Control Management Process is Established

The Vice President for Business and Financial Affairs (VP for BFA) will ensure physical access processes:

a) Are implemented and maintained,

b) Are compliant with other University policies, and

c) Minimize risk to the campus community and its property.

The VP for BFA appoints members of the Campus Access Control Committee (CACC) and approves its charter.

2. Campus Access Control Committee Oversees Access Control

The CACC is a standing committee with the responsibility to:

a) Designate Access Control Administrators (ACA) for campus spaces

b) Develop and maintain guiding documents;

c) Advise vice presidents on access control issues within their divisions

d) Advise ACAs in the development of processes for requesting and granting access devices within their areas of responsibility; and

e) Interpret this policy to resolve individual disputes and address questions pertaining to access control.

3. Area Control Authorities Define the Process for Requesting and Granting Access Devices

ACAs designate Area Access Managers (AAM) for areas and spaces assigned by the CACC.

The specific process for requesting, and the criteria used for granting access and access devices, is defined by the ACA in accordance with campus guiding documents and divisional guidance. The following underlying principles apply:

a) Employment status does not imply automatic authorization for access,

b) Access is granted at the lowest level of need, and

c) Granting access is to always favor safety and security of persons and property over the convenience of the requester.

AAMs may only grant access privileges within the parameters established by an ACA, and only for the areas assigned by the ACA.

4. Guiding Documents

Guiding documents are an extension of this policy. The CAAC, ACAs, AAMs, and Authorized Individuals are required to follow approved guidelines in order to effectively manage access to University facilities. Guiding documents will include, but are not limited to:

a) Guidelines for Issuing Access Devices - Describes levels of access and criteria for granting access privileges and access devices to authorized individuals.

b) Identification of ACAs and AAMs and departmental responsibilities for access control.

c) Access Control Measures - Describes risk and vulnerability considerations when determining the preventive and detective measures that will be used by the University for access to areas on campus.

5. Access to All University Owned and Leased Facilities and Space Is Limited to Authorized Individuals

a) During scheduled hours, academic and administrative buildings and spaces are open for general use by employees, students, and the public for educational, work related, and special event purposes.

b) Outside scheduled hours, access is restricted to authorized individuals. Sponsored guests must be accompanied at all times by an authorized individual.

c) During all hours:

i. Access to certain University areas is limited to authorized individuals only. For example:

1) Operational facilities and spaces (e.g. steam plant and mechanical rooms).

2) Higher-risk facilities and spaces (e.g. laboratories, hazardous materials storage areas, and performance venues).

ii. Access to residential facilities is limited to authorized:

1) Students,

2) Guests of students,

3) Employees,

4) Visitors (e.g. pre-authorized conference attendees), and

5) Contractors.

6. Visitors, Students and Employees Must Comply with University Conduct Regulations

In addition to employees and students, guests, contractors and visitors on University property are expected to comply with all University policies and state and federal regulations related to:

a) Access to and use of University buildings and spaces, and

b) Appropriate conduct as described in WAC 516-24.

7. All Access Devices Are the Property of Western Washington University

a) Access devices and privileges are assigned to authorized individuals on a temporary basis only,

b) Authorized individuals must sign for the access device, indicating they understand and will comply with individual rules and responsibilities for access devices,

c) Supervisors of authorized individuals must ensure access devices are promptly returned or relinquished to the original issuer:

i. When no longer needed for any reason,

ii. Before departing the University or transferring to another department, or

iii. Upon request for any reason at any time by an Executive Officer, Access Control Administrator, Area Access Manager, Supervisor, or Director of Public Safety.

d) Failure to return access devices by an authorized individual may result in one or more of the following:

i. Administrative action by the University, up to and including legal action, and/or,

ii. Assessment of charges for expenses incurred by the University to return access control to the same level that it was before it was compromised by the individual's failure to return the access device.

e) Lost, stolen, or damaged access devices shall be reported immediately to the:

i. Appropriate Access Control Administrator,

ii. Area Access Manager, and

iii. University Police Department.

The *Reporting Loss of University Funds or Property* (POL-U5300.25) policy is to be followed when any known or suspected loss resulting in the unauthorized taking of University public or non-public funds or property or other illegal activity.

8. Authorized Individuals Responsible for Safekeeping Access Devices and Appropriate Use of Spaces

Authorized individuals who are assigned an access device are prohibited from:

a) Loaning access devices to others,

b) Transferring access devices to others,

c) Duplicating access devices,

d) Altering access devices or access control mechanisms,

e) Damaging, tampering, or vandalizing any University access control mechanism,

f) Propping locked doors open, and

g) Admitting unauthorized individual(s) into an access controlled space.

9. Director of Public Safety Ensures Audits of Issued Access Control Devices

The Director of Public Safety may independently conduct periodic audits of issued access control devices or may request that Access Control Administrators and Area Access Managers conduct audits of the area(s) for which they have oversight.

Appendix E

TELECOMMUNICATIONS

(APPENDIX F in original document)

F.1 Existing System

F.1.1 Description

Data, telephony, and CATV communications are delivered on campus via fiber optic and copper cable plants both within and between buildings. Bond Hall is the primary demarcation point for all internet, telephone, and CATV service to campus from outside providers. Fiber optic cabling between buildings on campus is both single-mode and multi-mode (62.5 micron) fiber. The majority of buildings on campus are wired with a mix of Cat5e and Cat6 copper cabling, though some buildings still contain Cat5 or Cat3 wiring.

Data network service is delivered to all users by Cisco routing, switching, wireless, and security systems. Analog telephone service is delivered to approximately 4000 users (including elevators, emergency phones, fax machines, and other services/facilities) via a Nortel PBX located in Bond Hall, and three fiber remotes in AC, CF, and the Commissary. IP telephony is delivered to approximately 400 users over the data network infrastructure using Microsoft Skype4Business; it interfaces with analog gateways in Bond Hall and AC to connect to both the PBX and the wider PSTN. CATV services are delivered to campus from a Comcast head-end in Bond Hall via a series of transmitters, fiber nodes, and amplifiers across campus. The CATV network includes a return path to Comcast to allow campus to broadcast programming on a community channel in greater Whatcom County.

The wired and wireless data network is divided into academic and residential sections. The academic data network is architected in an active-passive redundant core design with multiple failover points between the two legs. The data network is logically arrayed in three tiers—the redundant core provides routing between the different nodes in the distribution layer (routers and switches that service individual buildings or groups of buildings on campus), and the distribution layer distributes traffic to the access layer devices (switches that service the endpoints—computers, servers, printers, wireless, etc.). The residential network also uses a three-tiered logical design, with a single core router attached to the redundant core routers of the academic network.

Western maintains telecommunications services to several remote sites, such as Shannon Point Marine Center, Lakewood Watersports Facility, the Technology Development Center, the Small Business Development Center, and Alumni/Foundation offices in downtown Seattle and the Bellingham Herald Building. We also maintain colocation services with Portland State University, site-to-site Virtual Private Network connections to Microsoft Azure and St. Joseph's Hospital, and direct fiber connectivity to the Whatcom County Courthouse.

All services and remote site connections pass through Bond Hall—no endpoint on campus can access CATV, internet, or the PSTN without going through Bond Hall to do so. In addition to being the demarcation point for internet, PSTN, and CATV service,

Bond Hall serves as the primary datacenter for the campus. The secondary datacenter is located on the second floor of AC, with fiber optic cable on above-ground utility poles connecting AC to the campus network. Internet service is provided via a 10Gbs circuit from the primary provider, and a 1Gbs circuit from the secondary/backup provider. From Bond Hall, Comcast and CenturyLink also maintain their own network demarcations to provide services directly to endpoints on our campus, such as contractors or vendors.

F.2 Existing Conditions Evaluation

- Overall Concerns
  - Lack of direct fiber paths from each building to each core – several buildings have to be patched one or more times through another building to reach a core, which introduces potential points of failure.
  - Multiple instances of chokepoints in our copper cable pathways: daisychained connections over multiple 110 blocks, CAT5 jumpers on crossconnects between Cat5e or Cat6 cables, Cat5 or Cat5e hydra cables connected to Cat6 station cables, etc.
  - Most of the network equipment is end-of-life or end-of-support, or will be by 2020. No operating dollars are allocated for upgrading network infrastructure. Most of the hardware and cabling was funded as part of two capital projects (in 2000 and 2010), or as part of other construction projects (Buchanan Towers East, Miller Hall, Carver, etc.), rather than operationalized for regular replacement.
  - The primary and secondary internet connections for campus share a demarcation point in Bond Hall. In the event of a facilities emergency in Bond Hall, there is no second path to the internet for campus.
  - Lack of insight and input into the design of other networks (building automation and control, fire and life safety, etc.) from our engineers can result in both security and performance issues for those networks, as well and technical issues for the academic network in places where the networks are bridged (i.e. Shannon Point Marine Center)
  - High risk of failure for existing PBX
  - Aging CATV system, lack of training and support for maintenance, lack of funding for equipment replacement, and lack of clear roadmap for the future of CATV (converged with data network vs maintained as a separate physical network).
  - Current wireless network is deployed “ad-hoc”, rather than designed strategically to ensure appropriate coverage and density across campus. As a result, the current wireless network infrastructure is inadequate to meet student needs and operational demands.
- Datacenter and Distributor Room Concerns
  - Lighting in all MDF/IDFs may not meet spec (BICSI TIA-569 Spec.)
  - Temp and Humidity in MDF/IDFs may not meet spec (ASHRAE Class 3 Spec.)
  - Several MDF/IDFs have become “shared spaces” over time, where our equipment competes for space with other departments’ equipment (ladders, custodial supplies, etc.). Lack of strong access controls in these spaces (brass key access only) leaves critical equipment at risk, and the confined space makes it difficult for people to work. Storage of some equipment (such as fluorescent lamps) is precarious, which is a safety concern for people working in the space.
  - MDF/IDF are becoming overcrowded with equipment from BAC, Fire and Life Safety equipment, CCTV hardware, etc. Rack and wall space are become tight, and work space becomes limited. Additional equipment also pushes up the temperature, requiring additional cooling systems to meet spec.
  - The second network core location (Arntzen Hall basement) is a hightraffic corridor for FM personnel to access fire control, electrical equipment, and other equipment. For a

network core, this space is inadequately secured and puts south campus network connectivity at risk. The space allocated for the network core doesn't have room for expansion.
    - Lack of clarity around electrical codes—can network equipment be operated on the same circuits as emergency lighting systems? If not, how do we provide a separate emergency power circuit for these systems to stay up during power failures (especially if they are supporting VOIP telephones over POE)?
    - High risk / low utilization of AC datacenter facility—the AC datacenter is vulnerable to service breaks due to above-ground utility service. Growth of services in the AC datacenter is constrained by diminished fiber capacity between the facility and campus, which is prohibitively expensive to expand. The facility itself is massively overbuilt in terms of both its physical space and power/cooling systems, relative to the shrinking physical footprint of modern datacenters (due to virtualization and migration to SaaS platforms).
    - Access to some MDFs/IDFs (for example, Rec Center and Old Main) are frequently limited because they are only accessible from within another occupied room (training room, group counseling room, cash-counting room, etc.).
- Capacity Concerns
    - Overall fiber capacity between buildings is insufficient in places.
    - Fiber capacity to AC from campus is insufficient and cost-prohibitive to expand.
    - Single-mode fiber capacity for direct connections between cores (AH and BH) does not meet future growth needs
    - Copper pathway capacity in some buildings is insufficient—cable trays are over-packed in places, and the changing specifications around Power-over-Ethernet will require fewer cables to be packed together in order to meet spec.
    - Switch port capacity at the access layer of select buildings is insufficient.
    - Available bandwidth of secondary ISP circuit is insufficient to accommodate normal campus bandwidth consumption during business hours—in the event of a primary ISP failure during a weekday, we will not have sufficient bandwidth on the backup connection to provide internet service to campus.

F.3 Future Conditions Evaluation

- Increased adoption of SaaS solutions, virtualization of servers, increases in storage density, and the shift from a large PBX to a small PBX+VOIP services will further decrease the size of the datacenter footprint required to support services on campus.
- Shifts to hosted solutions and the convergence of services onto the data network will push demand beyond what our network infrastructure can currently support.
- Resilience and flexibility of Azure computation and storage resources will eliminate the need for maintaining two datacenters on campus as a business continuity/disaster recovery solution—one datacenter plus "cloud" backups and a small secondary on-campus site for business-critical services will suffice.
- Movement toward the adoption of IPTV as a delivery mechanism for CATV service would allow us to converge data and CATV services on the data network, reducing or eliminating the need to maintain separate CATV hardware and cable plant.
- Increased use of wireless devices by both students and staff, including the adoption of mobile network devices in university operations (i.e. Asset Works) and instruction (i.e. audience response systems) will drive the need for increased coverage and density of wireless networks, which will in turn drive an increased need for access layer capacity, more Cat6 cable, more fiber, more Power-over- Ethernet switches, and upgrades to 208v power in more closets. These increased needs will also be driven by the

proliferation of IP-enabled devices on the wired/wireless network (the “Internet of Things”).
- Not all MDF/IDFs have the physical space to house the additional hardware needed to support the need for more access-layer port capacity.
- Rapidly evolving cable specification standards and accelerating hardware performance options may require the copper cable plant to be upgraded more frequently than in decades past. In lieu of adequate funding to upgrade entire buildings at once, the problem of ad-hoc upgrades and connections patched with mismatched cables could proliferate, making the MDF/IDFs more difficult to physically manage and diminishing overall network performance.

F.4 Recommendations

- Operationalize the costs of network equipment maintenance and replacement, WWU UTMP F-6 June 2017 and establish a fully-funded strategic plan for the cyclical replacement and expansion of core-, distribution-, and access-layer network devices, including a continued expansion of the wireless network and accompanying access-layer port capacity.
- Expand fiber capacity between buildings, including upgrading fiber to recommended latest spec.
- Run new fiber optic cables to ensure direct fiber paths exist from each building to each of the two cores, plus additional capacity directly connecting the cores to each other.
- Evaluate more secure/resilient locations on south campus for the second network core, such as Campus Services or Commissary, and relocate the core infrastructure there.
- Bring additional fiber to a new campus location (such as a new network core) to serve as a secondary ISP circuit, physically separating the two ISP connections into separate facilities.
- Consolidate datacenter services in Bond Hall, with a smaller redundant location on campus for business continuity of critical services only. Use cost savings from vacating the AC datacenter to move disaster recovery functions to cloud-hosted platforms.
- Devote time and resources to further investigating Passive Optical Networks (PON) as an alternative to copper cabling in new/remodeled buildings.
- Incorporate central networking/telecommunications team in the planning, configuration, security, and maintenance of data networks other than just academic and residential (i.e. BAC, lighting control, etc.).
- Fully fund the migration of PBX telephone users to IP telephony services, and replace the existing PBX with a smaller PBX to provide telephony to non-IP telephony compatible services only (elevators, fax machines, etc.).
- Fund and strategically plan for the upgrade of all MDF/IDFs on campus to 208v power. Bring humidity/temperature and lighting up to industry specifications. Upgrade and standardize all 110-block termination fields to new campus standard (current standard is Commscope Visipatch system), and upgrade all hydra cables to current communication cable specifications, subject to the study and analysis of PON systems.
- Fund and strategically plan for the upgrade of all horizontal cable systems to latest specification, subject to the study and analysis of PON systems.

F.5 Conclusions

Campus telecommunications is at a critical point in its lifecycle. The data network is resilient, but nearing the end of its supported life with no active plan for upgrade. The analog telephone network is at critical risk, with transition to newer services stymied by lack of funding and lack of clear institutional prioritization and direction. The CATV network is in a state of transition, where institutional leadership has sent mixed signals by investing in both an IP-based distribution for the residence halls and in production/broadcast facilities that rely on non-IP based distribution for academic programs.

The challenges and opportunities facing Western's telecommunications services and infrastructure are not unique; others have weathered these storms before, and we can do so as well with adequate funding, coordination, and commitment from the university to a strategic vision for the future.