Institution
Western Washington University
Project Title
Critical Safety, Access Control, and Fiber Optic Network Upgrades
Project Location (City)
Bellingham

1. Problem Statement (short description of the project – the needs and the benefits)

Western Washington University has an immediate and urgent need to replace and/or upgrade the campus fiber optic network. This communications fiber supports academic instruction, fire & life safety systems, business operations, and building automated control systems. Western has also determined that the existing manual locks and internal classroom locks are not adequate to meet campus efficiency, safety, and security objectives and obligations.

2. Project Description

The project would replace the existing 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.

Overall, these upgrades will enable Western to meet the continuing communication and life safety needs of students and faculty. The electronic and classroom locks will 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.

This project is proposed to accomplish the following:

1. Replace the existing damaged and undersized campus fiber optic network between and within major academic buildings. This includes combining (for efficiency) stand-alone switches and controllers to reduce space, power, and cooling needs.
2. Provide centralized lock down functionality to facilitate more agile, appropriate, and effective response capabilities in the event of a campus emergency. This will be accomplished through expansion of electronic control to all exterior doors of major academic buildings and designated high security internal doors within those buildings.
3. Provide classrooms with internally lockable doors so in the event of an emergency, students and faculty are able to effectively take shelter under the “Run, Hide, Fight” response to an active shooter.
4. Upgrade power to equipment closets to include emergency power and cooling.
5. Bring utility conduits and trays into electrical code compliance by removing abandoned electrical cable and adding new trays where necessary.
6. Reduce operating costs by reducing or eliminating the need for manual locking and opening of academic buildings on a daily basis.

3. History of the project or facility

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

A 2017 Utility 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 in order to maintain current service delivery.

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 Utility Master Plan Update, concluding that the occasional damage to the existing 17 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.

Concurrently, in response to recent 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 quickly and effectively safeguard buildings and facilities. Lessons learned from active shooter events around the country pointed at two key improvements:

a) Lockdown: The committee recommended that the expansion of the campus electronic access control capacity will improve its ability to protect the safety and security of people and buildings. Electronic access would become the predominant means of accessing certain spaces, not replacing traditional brass keys entirely, but becoming the “norm” for exterior doors, general use classrooms, and selected high use labs. Operationally, this will provide a reliable method for immediate lockdown of campus, secure buildings during non-working hours, and provide an electronic record of whose credentials have been used for access.
b) Classroom Locks: The Final Report of the Sandy Hook Advisory Commission strongly recommends “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 strongly recommended adaption of that standard for WWU classrooms.
c) (http://www.shac.ct.gov/SHAC_Final_Report_3-6-2015.pdf)

4. University programs addressed or encompassed by the project

This project supports virtually all of the university’s academic programs, administrative activities, and student services. The updated fiber optic loop, once completed, will provide a faster and more reliable means for campus academic and business units to accomplish their respective missions. Fiber cable connects all buildings on Western’s campus, and runs within most of them. Without it, there would be no email, internet accessibility, access to student records, etc. As today’s students arrive on campus, they want to know that Western has the technology and infrastructure that allow them to capably complete their education. Similarly, as more and more university business processes rely on internet accessibility and high speed data transmission, the new and more capable fiber will enable Western to meet future demands.

All programs on the Western campus are operated out of and depend on safe, reliable, and fully functioning buildings. Expansion of electronic access controls, which relies on a dependable fiber network, will help improve the security of our buildings as well as the safety of the students and staff who need those spaces in nearly every academic activity.

5. Significant Health, Safety, and Code Issues

There are several operational activities with code compliance implications that directly or indirectly rely on a fully functioning fiber optic communications loop. These activities enable Western to operate in accordance with various laws and codes:

Clery Act: The Clery Act of 1998 is a federal law requiring institutions of higher education that receive federal funding to collect and publish statistics about reports of certain crimes that occur on or adjacent to campus. In order to comply with the requirements, the university is also required to have in place security policies, procedures, and infrastructure to protect and safeguard the Western community. 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 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 year alone, this process of real time data analysis has saved Western over $100,000 in energy. All of Western's buildings are monitored through a central station located in the Physical Plant building.

Fire Code Compliance: All fire alarm 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 we install electronic entries, we will also replace (where necessary) existing traditional door knobs with ADA compliant openers. Similarly, classroom locks will be fully compliant with both Fire Code and ADA requirements.

6. Evidence of increased repairs and/or service interruption

Building Access Issues. This project proposes to expand the use of electronic credentialing across campus, thus reduce the use of and need for traditional brass keys. Three years ago, in response to a lost master key, Western accelerated an internal project to rekey all of campus. The "service interruption" caused by the loss of the key and subsequent monumental effort to issue new keys to thousands of students and staff is a maintenance activity that can be nearly eliminated through the use of electronic technology.

Fiber Capacity Issues: Our campus has numerous bottlenecks in which the number of available fiber strands has nearly run out, including:

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

In addition to our strand count capacity issues, we are experiencing several bandwidth bottlenecks in key areas of our campus, resulting in poor network performance during peak hours. This congestion could be alleviated with additional fiber and upgrades to our core and distribution network equipment. These bottlenecks include:

- Traffic on our campus wireless network.
- Traffic to and from our Science, Math, and Technology Education (SMATE) facility.
- Traffic to and from 12 single-network-closet facilities (including six teaching facilities and our campus police department/health center/emergency operations center).

7. Impact on Institutional Operations without the Infrastructure Project

Much of the impact to the operation of campus systems is articulated elsewhere in this proposal. Nearly all academic and administrative functions depend on a reliable fiber optic communications infrastructure. Emergency response capabilities and functionalities will be enhanced by a more capable electronic credentialing and lockdown functionality.

In addition to those impacts is the anticipated savings in recurring labor and materials costs that are inherent in operating a traditional brass key system.

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 per year.

It is well established within the security and safety industry that the use of electronic credentials has a lower life cycle cost than traditional brass keys. By eliminating the need to rekey a lock when a brass key is lost, all the hard costs of new keys will be avoided by (literally) several key strokes in the electronic system.

A fully capable electronic access system is also 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.

8. Reasonable Estimate

The cost estimates for electronic access control are based on actual costs seen in recent campus work. During FY13, Western completed a minor works capital funded project that brought electronic access control into two campus buildings. During the 15-17 biennium, a major renovation project provided additional baseline information on installation costs. Two major public works projects in the 17-19 biennium – one in multiple academic & auxiliary buildings, and one in a residence hall provided recent market information for similar work.

The cost estimate for the fiber optic installation portion of the project is also based on actual cost seen in small projects throughout campus.

See Appendix A for specifics associated with the budget breakdown.

9. Engineering Study

In 2017, Western completed a utility master plan update which identified the need to replace the existing fiber network in order 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. See Appendix E.

10. Supports Facilities Plan

In order to provide the opportunity for Washington's residents to complete a post-secondary education program (Results Washington Goal 1), we must first provide a learning environment that is attractive to prospective students and parents, conducive to learning once those students are on campus, and always provide a sense of personal well-being and safety (Results Washington Goal 4) to everyone on campus. See Appendix C.

Western's 2018 Strategic Plan specifically declares the need to "provide technological and other academic infrastructure to support curricular innovation, research, scholarship, and creative activity, civic engagement and social justice". The fiber optic infrastructure, upon which nearly all academic and business functions rely, is essential to campus operations. Elsewhere in the Strategic Plan, the safety and security of students and staff is expressed as a paramount concern. The improvement of Western's physical security capabilities as well as the maintenance of current safety capabilities is fully aligned with our strategic intent.

Western's institutional master planning, while focused on long range development zoning and relationships with surrounding neighbors, also contains six guiding principles for that 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." See Appendix C.

As stated earlier, all academic and research programs on the Western campus are operated out of and depend on safe, reliable, and fully functioning buildings. As stewards of state resources Western is expected and required to provide a safe learning and working environment. Highly qualified faculty, motivated students, and expert staff all inherently depend on fully functioning, highly capable infrastructure systems.

The proposed project supports the campus Access Control Policy (Appendix D) as well as that policy's supporting standards and procedures.

11. Resource Efficiency and Sustainability

Western will be able to continue its energy conservation and monitoring efforts through a fully capable fiber optic infrastructure.

The electronic access component provides 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.

Access Control Security & Infrastructure Upgrades

Appendix Contents

Appendix A

OFM

380 - Western Washington University
Capital Project Request

2019-21 Biennium

*

Version: SV 2019-21 Capital Budget Request

Report Number: CBS002
Date Run: 7/31/2018 2:20PM

Project Number: **30000604**
Project Title: **Access Control Security Upgrades**

Description

Starting Fiscal Year: 2020
Project Class: Program
Agency Priority: 8

Project Summary

We are proposing to change the project title to "Critical Safety, Access Control, and Fiber Optic Network Upgrades". This project would replace the existing fiber optic communications loop 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.

Project Description

Western has an immediate and urgent need to replace and/or upgrade the campus fiber optic network. This communications fiber supports academic instruction, fire and life safety systems, business operations, and building automated control systems. Additionally, the University has determined that the existing electronic locks and internal classroom locks are not adequate to meet efficiency, safety, and security objectives.

This is a multi-phased project, which began in February 2018 and would end by June 2023. The project would accomplish the following:

1. Replace the existing damaged and undersized fiber optic network between and within major academic buildings. This includes combining stand-alone switches and controllers to reduce space, power and cooling needs.
2. Provide centralized lock down functionality to facilitate appropriate and effective response capabilities in the event of a campus emergency.
3. Provide classrooms with internally lockable doors, enabling students and faculty to effectively take shelter, in the event of an active shooter on campus.
4. Upgrade power to equipment closets to include emergency power and cooling.
5. Bring utility conduits and trays into electrical code compliance by removing abandoned electrical cable and adding new trays where necessary.
6. Reduce operating costs through elimination of manual locking/opening of academic facilities.

In the 2017-19 biennium, Western received $1.5 million in State 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 Utility Master Plan Update, concluding that the occasional damage to the existing 17 year old fiber loop, along with the increased reliance on web-based applications campus-wide, and emerging technologies in building operating systems are stretching the fiber loop to its capacity. The proposed funding will remedy the issues associated with the fiber loop as well as complete construction of the Access Control.

In addition to the State funds, the project also received approximately $600,000 in University auxiliary resources to cover the portion associated with the connection of the Access Control to residential and recreation facilities.

Nearly all academic and administrative functions depend on a reliable fiber optic communications infrastructure. Western's 2018 Strategic Plan specifically declares the need to "provide technological and other academic infrastructure to support curricular innovation, research, scholarship, and creative activity, civic engagement and social justice".

In providing electronic access control, this project aligns perfectly with Principle no. 3 of Western's institutional master plan "provide convenient and safe access to and through the campus for the University's guests, faculty, staff and students." Electronic access control will limit unauthorized access to academic buildings. In addition to providing safety to building occupants, electronic access control will better control energy consumption. 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 and duration of propped open doors and conserve energy within buildings.

Western constantly monitors the performance of HVAC systems through a data analytics tool directly connected the Siemens operating system. The data is transmitted over the fiber optic line to the physical plant technicians who can evaluate

Project Number: 30000604
Project Title: Access Control Security Upgrades

Description

performance anomalies and identify areas of potential energy savings. Over the past year alone, this real-time data analysis has saved Western over $100,000 in energy costs.

Location

City: Bellingham **County:** Whatcom **Legislative District:** 040

Project Type

Infrastructure (Major Projects)

New Facility: No

Funding

			Expenditures		2019-21 Fiscal Period	
Acct Code	Account Title	Estimated Total	Prior Biennium	Current Biennium	Reapprops	New Approps
057-1	State Bldg Constr-State	13,600,000				6,700,000
065-1	WWU Capital Projects-State	1,500,000		1,500,000		
	Total	**15,100,000**	**0**	**1,500,000**	**0**	**6,700,000**

		Future Fiscal Periods			
		2021-23	2023-25	2025-27	2027-29
057-1	State Bldg Constr-State	6,900,000			
065-1	WWU Capital Projects-State				
	Total	**6,900,000**	**0**	**0**	**0**

Operating Impacts

No Operating Impact

STATE OF WASHINGTON

AGENCY / INSTITUTION PROJECT COST SUMMARY

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

Contact Information

Name	Rick Benner, FAIA
Phone Number	(360) 650-3550
Email	rick.benner@wwu.edu

Statistics

Gross Square Feet		MACC per Square Foot	
Usable Square Feet		Escalated MACC per Square Foot	
Space Efficiency		A/E Fee Class	B
Construction Type	Other Sch. B Projects	A/E Fee Percentage	11.17%
Remodel	Yes	Projected Life of Asset (Years)	50

Additional Project Details

Alternative Public Works Project	No	Art Requirement Applies	No
Inflation Rate	3.12%	Higher Ed Institution	No
Sales Tax Rate %	8.70%	Location Used for Tax Rate	
Contingency Rate	10%		
Base Month	June-18		
Project Administered By	Agency		

Schedule

Predesign Start		Predesign End	
Design Start	February-18	Design End	May-22
Construction Start	November-18	Construction End	April-23
Construction Duration	53 Months		

Green cells must be filled in by user

Project Cost Estimate

Total Project	**$13,972,009**	Total Project Escalated	**$15,099,900**
		Rounded Escalated Total	**$15,100,000**

STATE OF WASHINGTON

AGENCY / INSTITUTION PROJECT COST SUMMARY

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

Cost Estimate Summary

Acquisition

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

Consultant Services

Predesign Services	$0		
A/E Basic Design Services	$687,017		
Extra Services	$113,000		
Other Services	$308,660		
Design Services Contingency	$110,868		
Consultant Services Subtotal	**$1,219,545**	**Consultant Services Subtotal Escalated**	**$1,300,191**

Construction

Construction Contingencies	$810,350	Construction Contingencies Escalated	$878,501
Maximum Allowable Construction Cost (MACC)	$8,103,500	Maximum Allowable Construction Cost (MACC) Escalated	$8,785,005
Sales Tax	$775,505	Sales Tax Escalated	$840,726
Construction Subtotal	**$9,689,355**	**Construction Subtotal Escalated**	**$10,504,232**

Equipment

Equipment	$2,089,000		
Sales Tax	$181,743		
Non-Taxable Items	$0		
Equipment Subtotal	**$2,270,743**	**Equipment Subtotal Escalated**	**$2,461,713**

Artwork

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

Agency Project Administration

Agency Project Administration Subtotal	$437,366		
DES Additional Services Subtotal	$0		
Other Project Admin Costs	$0		
Project Administration Subtotal	**$437,366**	**Project Administation Subtotal Escalated**	**$474,149**

Other Costs

Other Costs Subtotal	**$355,000**	**Other Costs Subtotal Escalated**	**$359,615**

Project Cost Estimate

Total Project	**$13,972,009**	Total Project Escalated	**$15,099,900**
		Rounded Escalated Total	**$15,100,000**

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	$687,017				69% of A/E Basic Services
Other					
Insert Row Here					
Sub TOTAL	**$687,017**		**1.0567**	**$725,972**	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	$66,000				
Travel & Per Diem	$40,000				
Advertising	$3,500				
Document Reproduction	$3,500				
Sub TOTAL	**$113,000**		**1.0567**	**$119,408**	Escalated to Mid-Design
4) Other Services					
Bid/Construction/Closeout	$308,660				31% of A/E Basic Services
HVAC Balancing					
Staffing					
Other					
Insert Row Here					
Sub TOTAL	**$308,660**		**1.0841**	**$334,619**	Escalated to Mid-Const.
5) Design Services Contingency					
Design Services Contingency	$110,868				
Other					
Insert Row Here					
Sub TOTAL	**$110,868**		**1.0841**	**$120,192**	Escalated to Mid-Const.
CONSULTANT SERVICES TOTAL	**$1,219,545**			**$1,300,191**	

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**		**1.0130**	**$0**	
2) Related Project Costs					
Offsite Improvements					
City Utilities Relocation					
Parking Mitigation					
Stormwater Retention/Detention					
Other					
Insert Row Here					
Sub TOTAL	**$0**		**1.0130**	**$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	$8,103,500				
Insert Row Here					
Sub TOTAL	**$8,103,500**		**1.0841**	**$8,785,005**	
4) Maximum Allowable Construction Cost					
MACC Sub TOTAL	**$8,103,500**			**$8,785,005**	

This Section is Intentionally Left Blank

7) Construction Contingency				
Allowance for Change Orders	$810,350			
Other				
Insert Row Here				
Sub TOTAL	**$810,350**	**1.0841**	**$878,501**	
8) Non-Taxable Items				
Other				
Insert Row Here				
Sub TOTAL	**$0**	**1.0841**	**$0**	
Sales Tax				
Sub TOTAL	**$775,505**		**$840,726**	
CONSTRUCTION CONTRACTS TOTAL	**$9,689,355**		**$10,504,232**	

Green cells must be filled in by user

Cost Estimate Details

Equipment					
Item	Base Amount		Escalation Factor	Escalated Cost	Notes
E10 - Equipment	$2,089,000				
E20 - Furnishings					
F10 - Special Construction					
Other					
Insert Row Here					
Sub TOTAL	**$2,089,000**		**1.0841**	**$2,264,685**	
1) Non Taxable Items					
Other					
Insert Row Here					
Sub TOTAL	**$0**		**1.0841**	**$0**	
Sales Tax					
Sub TOTAL	**$181,743**			**$197,028**	
EQUIPMENT TOTAL	**$2,270,743**			**$2,461,713**	

Green cells must be filled in by user

Cost Estimate Details

Artwork					
Item	Base Amount		Escalation Factor	Escalated Cost	Notes
Project Artwork	$0				0.5% of Escalated MACC for new construction
Higher Ed Artwork	$0				0.5% of Escalated MACC 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
Agency Project Management	$437,366				
Additional Services					
Other					
Insert Row Here					
PROJECT MANAGEMENT TOTAL	**$437,366**		**1.0841**	**$474,149**	

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**		**1.0130**	**$359,615**	

Green cells must be filled in by user

Appendix B

JAY INSLEE
Governor

Policy Brief
September 2013

By setting clear goals and continually tracking results, the state will be better equipped to engage its employees, partners and the public in building a healthier, better-educated and more prosperous Washington.

World-Class Education

Prosperous Economy

Sustainable Energy and a Clean Environment

Healthy and Safe Communities

Efficient, Effective and Accountable Government

www.results.wa.gov

Results Washington: A more efficient, effective and transparent state government

Any organization functions better — and gets better results — when its decisions and actions are guided by solid data. Washington has seen this firsthand. Over the past decade, for example, our data-driven "Target Zero" traffic safety program has helped reduce the state's fatality accident rate to record lows. Intensive data-gathering has helped us speed up our response to reports of child abuse and streamline delivery of government services, from water permit approvals to vehicle registration renewals. Now we're taking it to a new level.

Governor Inslee believes we can do more to ensure a faster, smarter and more accountable state government — a government focused on key goals that will help strengthen our economy, improve our schools and make Washington an ideal place to live and do business. By setting clear goals and continually tracking results, the state will be better equipped to engage its employees, partners and the public in building a healthier, better-educated and more prosperous Washington. Indeed, the Governor is delivering on his inaugural address promise that "We will provide efficiency, effectiveness and transparency."

RESULTS WASHINGTON

Washington has long been a national leader in adapting proven private-sector methods and tools to measure and improve state government performance. For the past eight years, tools such as the Government Management Accountability and Performance (GMAP) program and Lean process improvement tools and techniques have been used to improve individual state agency performance.

The state is now poised to launch Results Washington, a new system combining the best aspects of GMAP with a significantly expanded Lean initiative that involves all state agencies. Results Washington will use the latest technology to routinely gather, review and display performance data which will make it easier for citizens to see for themselves how well state government and its many partners — such as school districts, local governments and community organizations — are delivering services and meeting key performance goals.

An innovative and data-driven approach to governing

Governor Inslee started this effort by identifying the vision, mission and top goal areas of his administration:

- World-Class Education
- Prosperous Economy
- Sustainable Energy and a Clean Environment
- Healthy and Safe Communities
- Efficient, Effective and Accountable Government

These goals tie into his "Building a Working Washington" agenda and encompass everything from transportation and education to health care and a clean environment. Goal councils, composed of agency directors, representatives from the Governor's budget and policy offices and the Results Washington team, were established for each goal area. The Results Washington team will work with agencies to gather and review performance data. This will provide valuable real-time information to help state managers spot trends and make data-driven decisions that will improve quality, speed up service delivery and support meeting improvement goals.

Access to an unprecedented array of performance data

Governor Inslee's goal councils identified key outcome measures and leading indicators for each of his five goal areas. These indicators require agencies to work together in developing strategic plans to meet the established goals. Results Washington will provide unprecedented transparency and access to information about how well we're making progress toward the goals. The goal councils, Results Washington team and Lean fellows will meet monthly to review performance data with the Governor, covering one goal area per month on a rotating basis. The data will be displayed and updated — with charts, graphs and context — on the Results Washington web portal.

Expanding state government's Lean initiative

Washington's businesses and health care industries have discovered the value of Lean as a way of doing business and achieved tremendous results. Lean is a system of proven principles, methods and tools that encourages employee creativity and problem solving. Lean is applied at all levels of an organization to review policies and procedures from a customer's point of view and consider what adds value and what can be eliminated. As part of Results Washington, we are creating a new Lean fellowship program, led by a Lean expert, to work side-by-side with agencies on performance improvement plans. Lean efforts will help state agencies more efficiently serve the people and businesses of Washington.

Engaging employees, partners and the public to deliver results

Previous state government performance management efforts typically measured only selected state agency outcomes. While Results Washington will continue to do that, it will also have a broader focus. Results Washington will use higher-level measures that gauge how well state government — and its public and private sectors partners — are doing. For example, one proposed outcome measure in the Prosperous Economy goal area is increasing the average wage for workers statewide. In the World-Class Education goal area, one proposed outcome measure is increasing the percentage of children enrolled in high-quality early learning programs.

Governor Inslee understands that state government alone cannot deliver success. By setting the vision and mission, and establishing clear expectations of continuous improvement against clear goals and targets to achieve, we will build a healthier, better-educated and more prosperous Washington.

"Let's get it done."

Appendix C

Guiding Principles (from the Draft Comprehensive Campus Master Plan, January 1997)

The following administrative principles shown below will guide future campus development:

1. The University Physical Master Plan reflects the University's strategic objectives in setting forth priorities in building and environmental projects
2. The preservation of the history and values inherent in the campus environment serves as the context for future growth and development of the University's campus
3. Provide convenient and safe access to and through the campus for the University's guests, faculty, staff and students
4. Future growth of the University occurs predominantly to the south
5. The central part of campus serves as the "academic core" of the University
6. The northern part of campus is primarily residential in nature

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.

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

TRUSYS

WESTERN WASHINGTON UNIVERSITY

ACCESS CONTROL SYSTEM ROADMAP

Dave Miller, Principal, TRUSYS

March 15, 2013

CONTENTS

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.

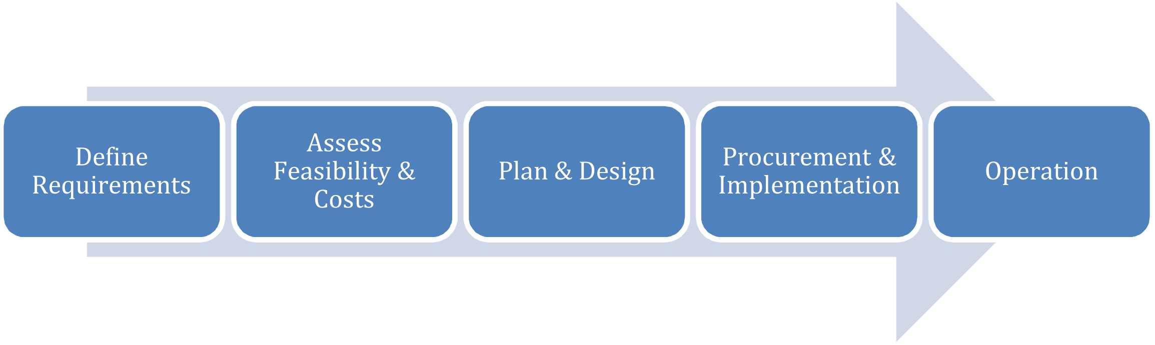


Figure 1 - 5-Point Roadmap

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:

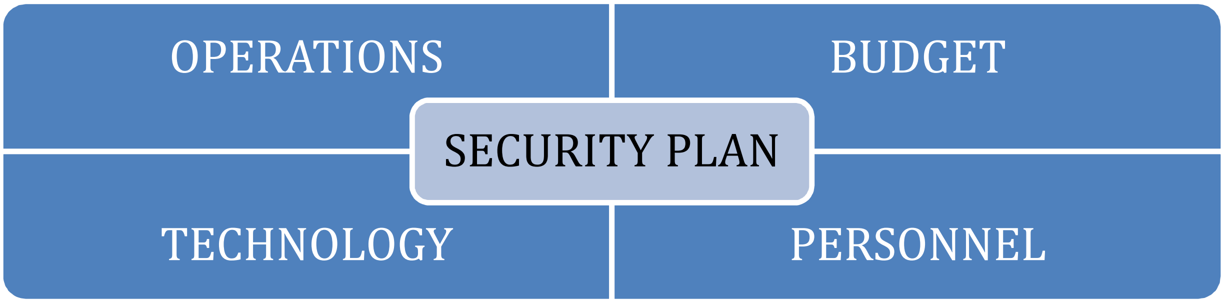


Figure 2 - Security Plan

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

ACCESS CONTROL TECHNOLOGY

Technology issues that require definition for the new ACS are:

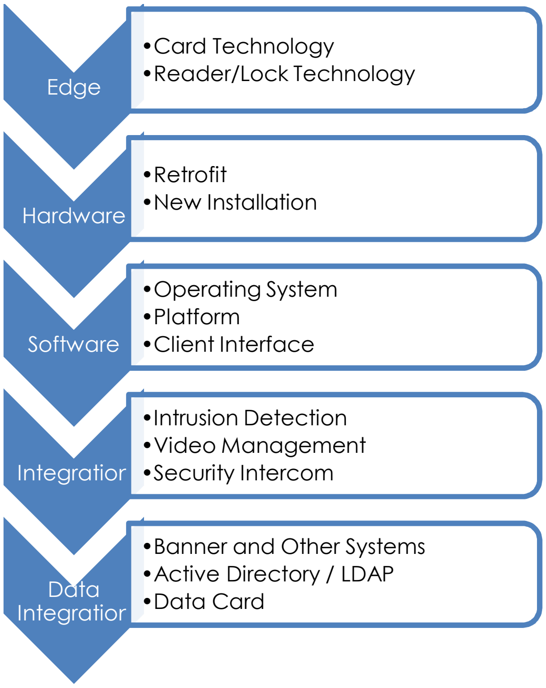
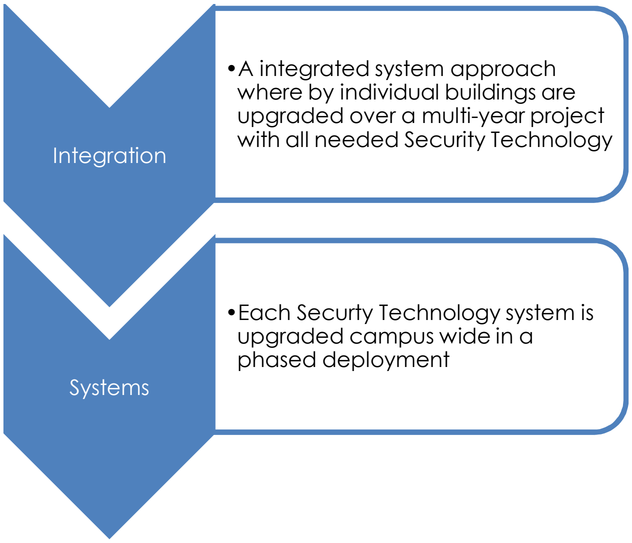


Figure 3 - Defining ACS Requirements

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:



- A integrated system approach where by individual buildings are upgraded over a multi-year project with all needed Security Technology
- Each Securty Technology system is upgraded campus wide in a phased deployment

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

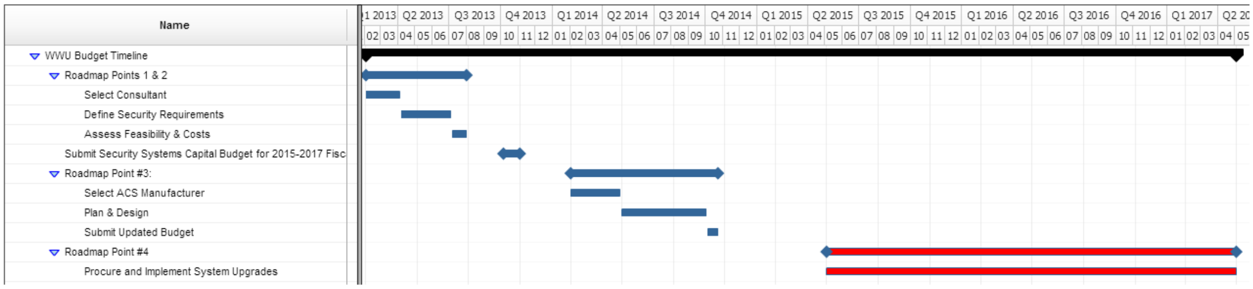
The detailed selection process for determining card technology, reader/lock technology, hardware, and system software is not included with the Consultant Design Fees noted above.

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.

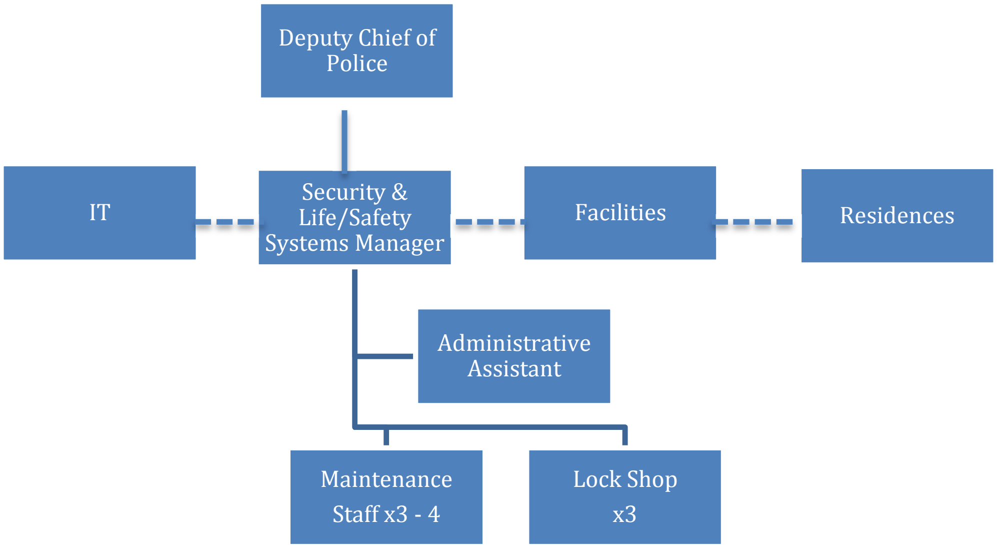
- 1 – Supervisor: The Supervisor will have the additional duties of covering sick or unexpectedly absent dispatchers, and to be the Terminal Agency Coordinator.
- 6 – Dispatchers: This will allow normal eight (8) hour shift coverage and minimize overtime. The Chief expressed a desire to have shifts maintained 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

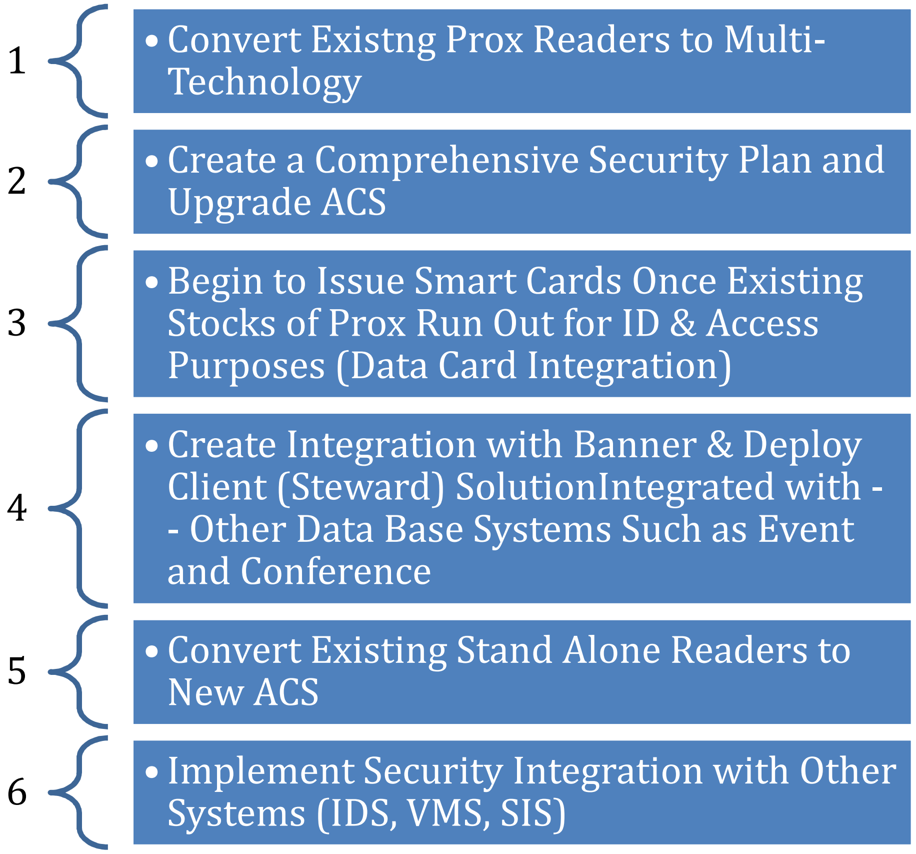
In the market place today, Access Control System (ACS) is the system around which security system integration is achieved. Many ACS manufacturers realize that they do not have the ability to design, develop and manufacturer all the needed systems such as intrusion detection (IDS), video management (VMS),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



1
- Convert Existng Prox Readers to Multi-Technology

2
- Create a Comprehensive Security Plan and Upgrade ACS

3
- Begin to Issue Smart Cards Once Existing Stocks of Prox Run Out for ID & Access Purposes (Data Card Integration)

4
- Create Integration with Banner & Deploy Client (Steward) SolutionIntegrated with -- Other Data Base Systems Such as Event and Conference

5
- Convert Existing Stand Alone Readers to New ACS

6
- Implement Security Integration with Other Systems (IDS, VMS, SIS)

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.

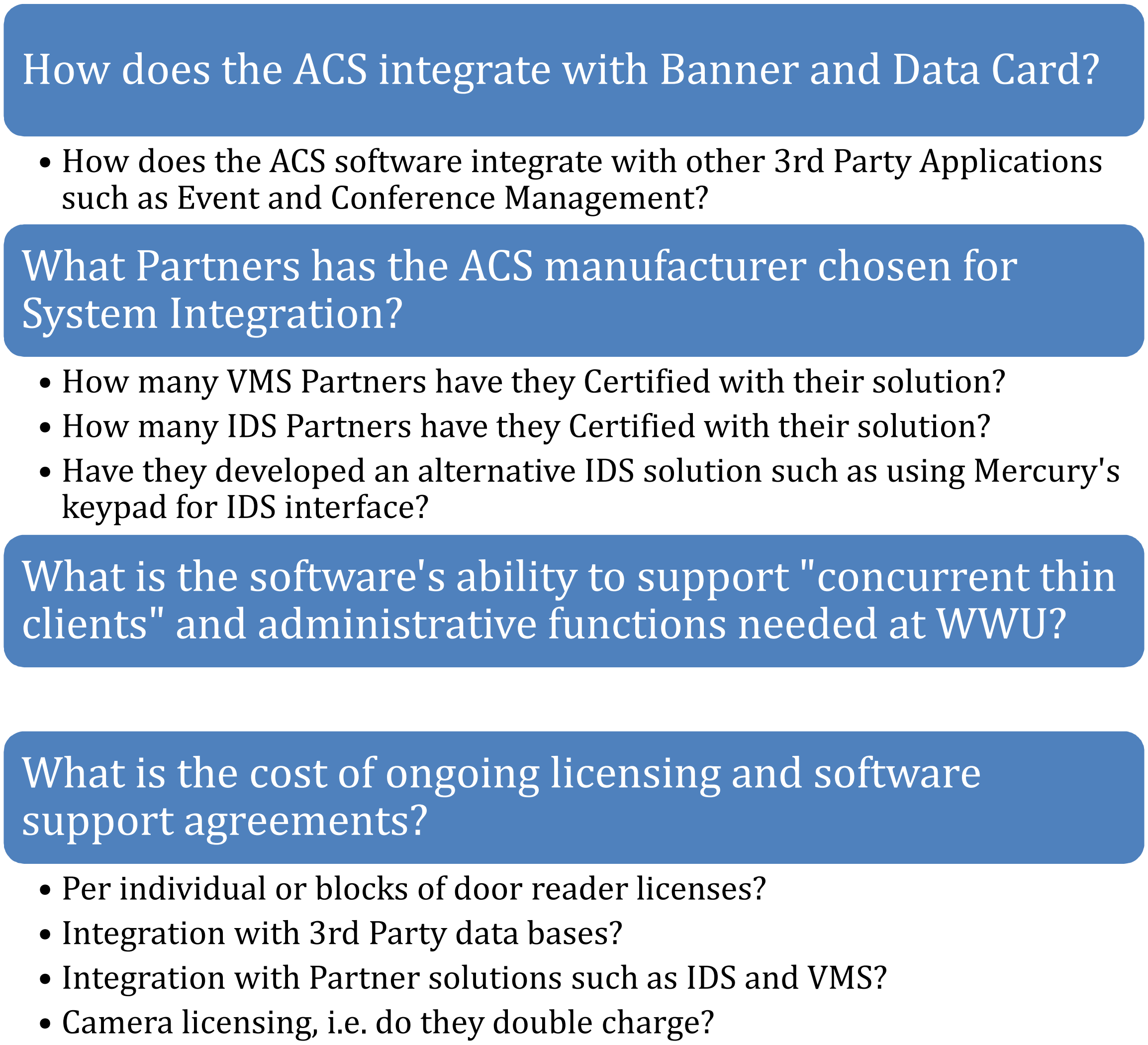
   The decision can be made later whether or not to maintain the above practice or shift to an MDF/IDF model for buildings that have not yet had ACS installed.

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

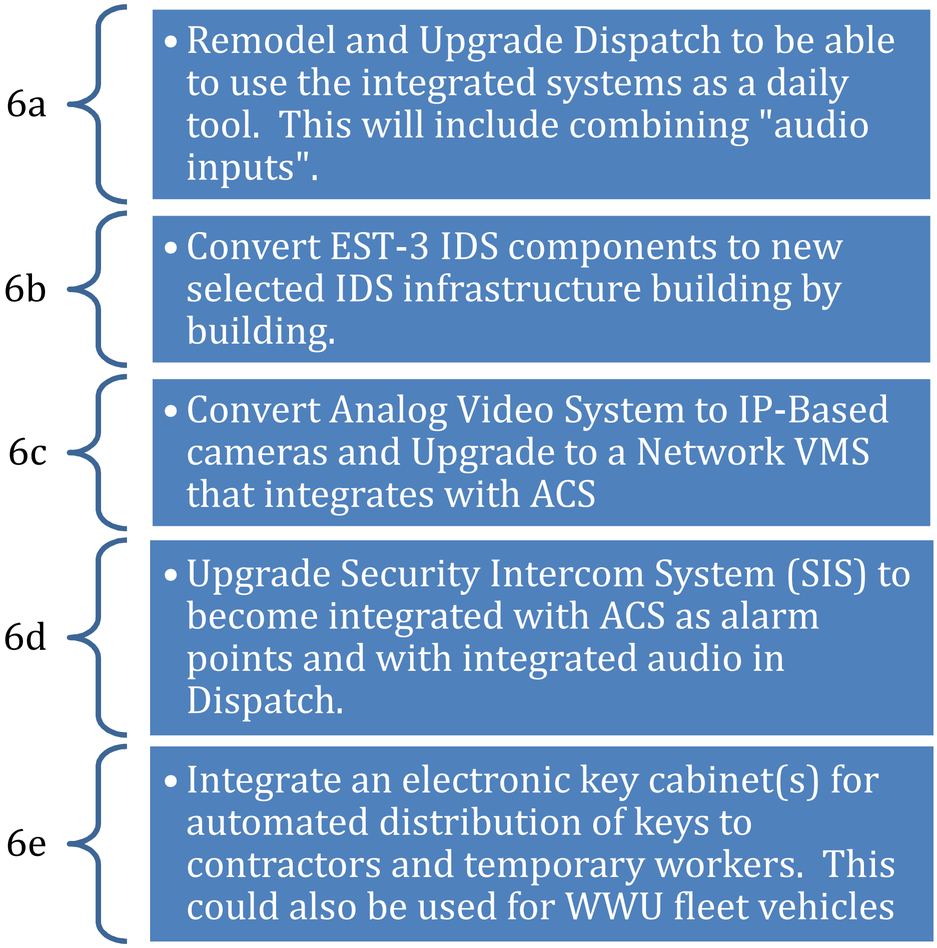
WWU should select an ACS solution that meets their needs and expectations.

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.



6a

- Remodel and Upgrade Dispatch to be able to use the integrated systems as a daily tool. This will include combining "audio inputs".

6b

- Convert EST-3 IDS components to new selected IDS infrastructure building by building.

6c

- Convert Analog Video System to IP-Based cameras and Upgrade to a Network VMS that integrates with ACS

6d

- Upgrade Security Intercom System (SIS) to become integrated with ACS as alarm points and with integrated audio in Dispatch.

6e

- Integrate an electronic key cabinet(s) for automated distribution of keys to contractors and temporary workers. This could also be used for WWU fleet vehicles

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.

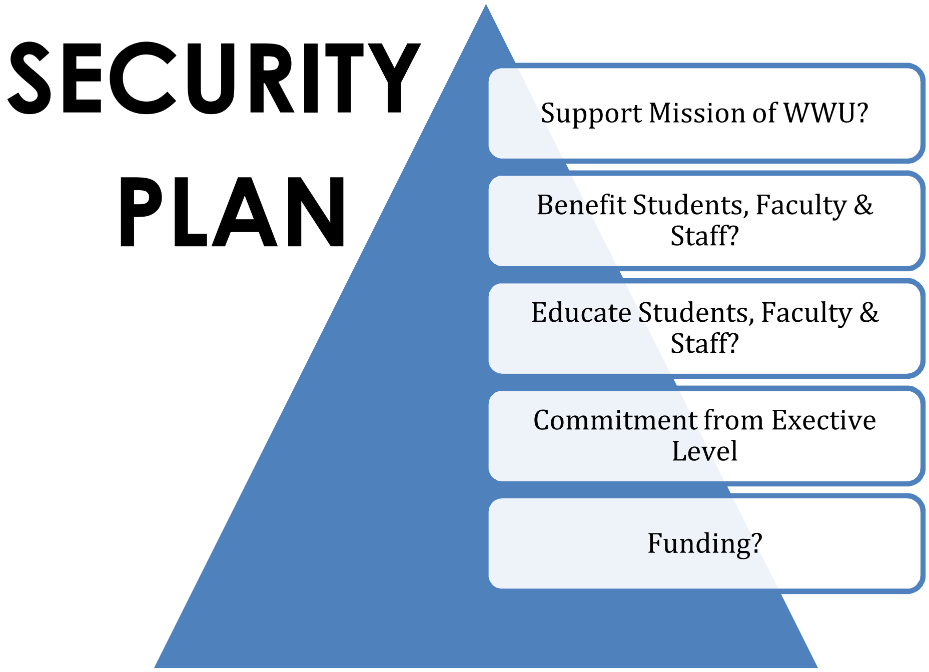

SECURITY
PLAN
Support Mission of WWU?
Benefit Students, Faculty & Staff?
Educate Students, Faculty & Staff?
Commitment from Exective Level
Funding?

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.

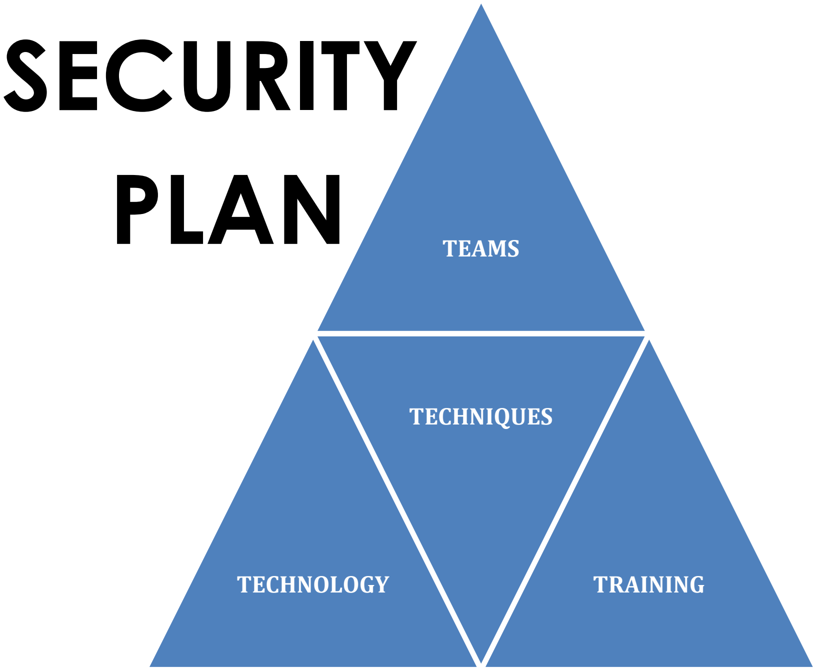


Figure 2: Building Blocks for Security Plan

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 are required.

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.

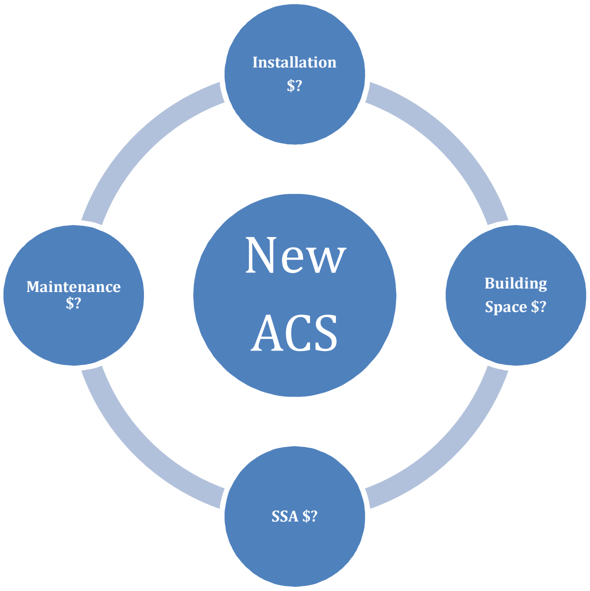
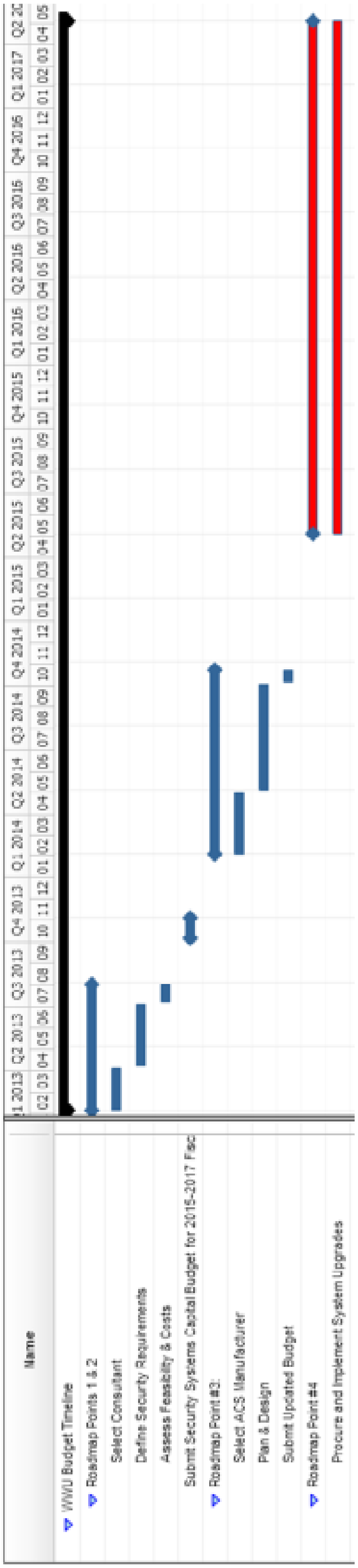


Figure 1: Uncertainty of Cost/Budget

BUDGETARY ESTIMATE FIGURE 1: TIMELINE (ENLARGED VIEW)


Name
WWU Budget Timeline
Roadmap Points 1 & 2
Select Consultant
Define Security Requirements
Assess Feasibility & Costs
Submit Security Systems Capital Budget for 2015-2017 Fisc
Roadmap Point #3:
Select ACS Manufacturer
Plan & Design
Submit Updated Budget
Roadmap Point #4
Procure and Implement System Upgrades
Q2 2013
Q3 2013
Q4 2013
Q1 2014
Q2 2014
Q3 2014
Q4 2014
Q1 2015
Q2 2015
Q3 2015
Q4 2015
Q1 2016
Q2 2016
Q3 2016
Q4 2016
Q1 2017
Q2 20