System-wide Security Assessment for MetroLink

June 19, 2018

Presented to:

EAST-WEST GATEWAY
Council of Governments

Presented by:

wsp

AGENDA

- Welcome / Introductions / Safety Moment
- Security Risk Assessment Methodology
- Project Overview & Approach
- Stakeholders
- Other Discussion / Next Steps

PROJECT OVERVIEW

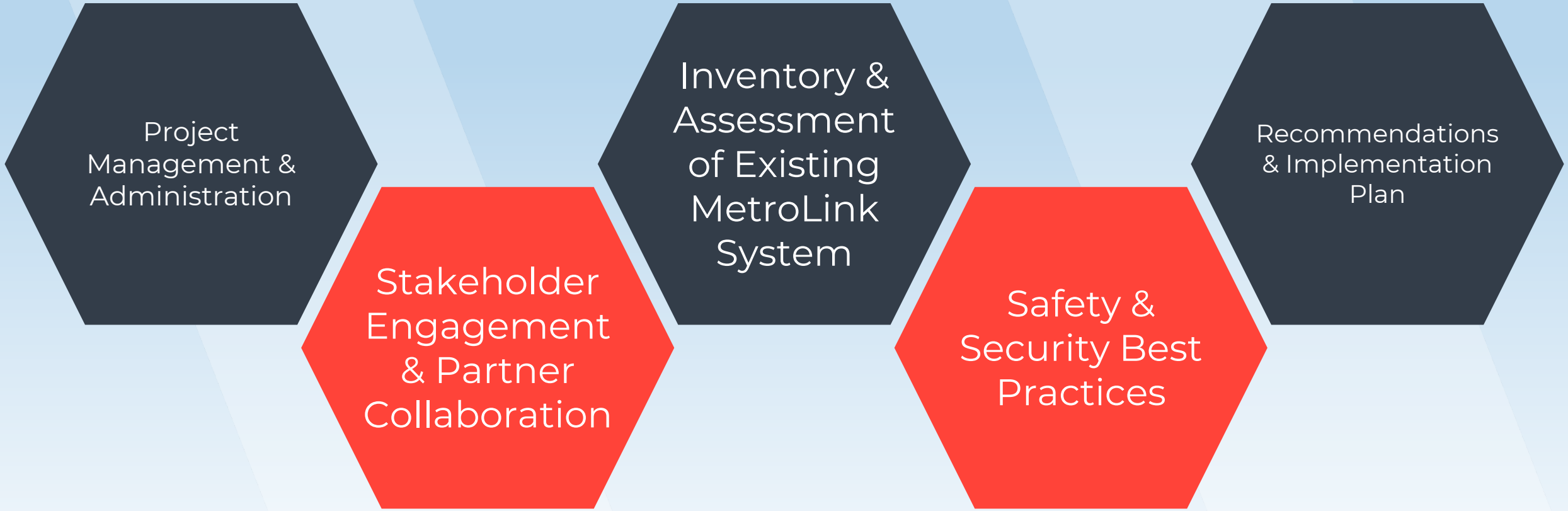
Perform a comprehensive security assessment of the St. Louis MetroLink System, resulting in recommendations to improve the security of the system

MetroLink, the 46-mile long light rail system in St. Louis, Missouri, is owned and operated by Metro Transit under the Bi-State Development Agency. It has been in operation since July 1993 and carries 46,180 passengers daily.

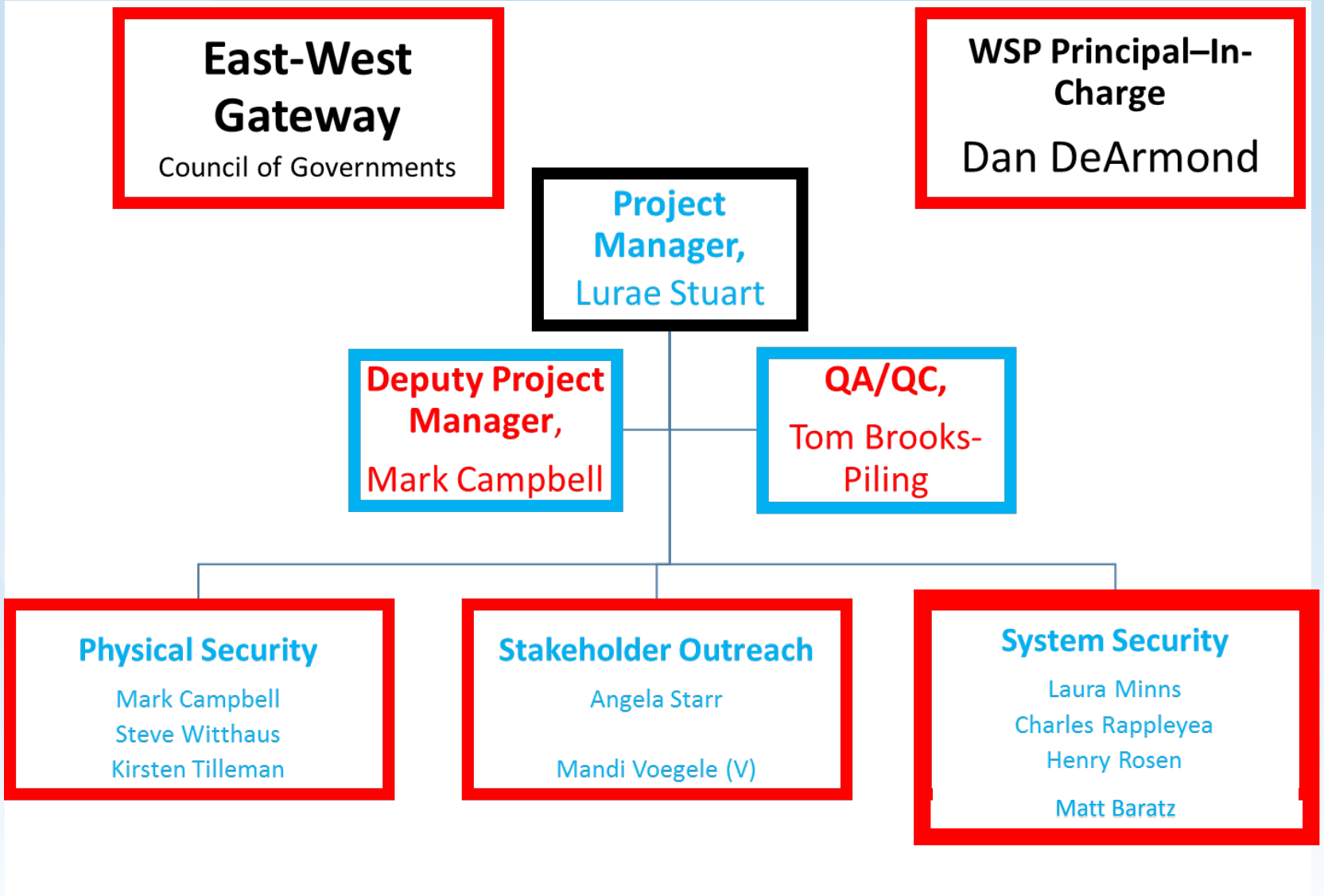
Responding to several violent episodes, the City of St. Louis, St. Clair County, St. Louis County, and Bi-State signed a Memorandum of Understanding outlining a plan to improve MetroLink security in cooperation with law enforcement.

The project's scope has evolved into a comprehensive assessment of the overall security at MetroLink stations and aboard MetroLink trains.

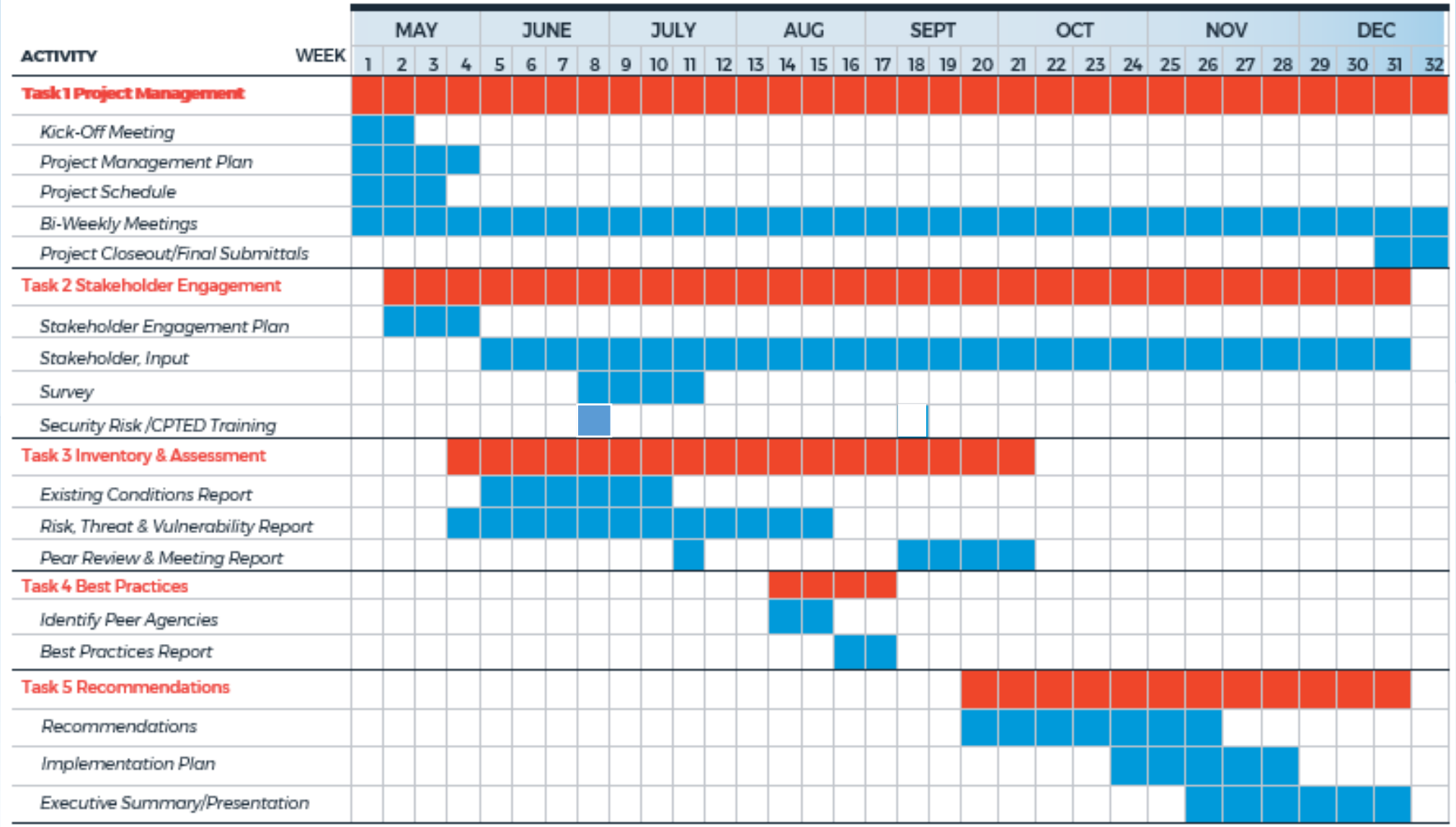
CONTRACT TASKS



Project Team



Draft Project Schedule



Security Risk Assessment Methodology

Key Terminology

- **Safe** – freedom from unintentional harm to people, equipment, reputation
- **Secure** – freedom from intentional harm to people, equipment, reputation
- **Hazard** – real or potential condition that can cause injury, illness, death, damage
- **Threat** – any intentional action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services
- **Vulnerability** - any weakness, flaw or condition that allows and/ or can be exploited, for the successful realization of a potential threat against the system and its assets
- **Risk** – likelihood + severity (consequence) of a realized threat
- **Acceptable Risk** – when further risk reduction measures will not result in significant reduction of risk

Risk Acceptance

The key for the Council and Partners is establishing exactly what is meant by acceptable or tolerable risk.

The expression “acceptable risk” usually, but not always, refers to the level at which further risk reduction measures or additional expenditure of resources will not result in significant reduction of risk” – ANSI B1.0 - 2010

Risk acceptance is a policy decision that must be owned & embraced by the system, as a whole, not individuals within the system

Risk acceptance is defined within the Security Risk Management Process

KEY POINT

“Accepting” a risk does not mean the risk is eliminated

- “Residual risk” still remains
- Remaining risk is sufficiently low to be outweighed by the benefits of the existing operation

Risk-Based Hazard Management

Define the System

Define
- Physical Characteristics
- Functional Characteristics

AND

Understand & Evaluate
- People
- Procedures
- Facilities & Equipment
- Environment

Identify

Identify
- Hazards
- Threats & Vulnerabilities

AND

Determine
- Causes
- Contributing Factors

Assess

Determine
- Severity & Probability
- Consequence & Likelihood

AND

Decide to
- Accept Risk
- Eliminate/ Mitigate

Resolve
- Assume Risk

OR

Implement Corrective Action
- Eliminate or
- Mitigate

Follow-Up

Monitor for
- Effectiveness
- Unexpected Outcome

Security Risk Assessment: Threat

INTENT	CAPABILITY				
	Similar exploit has been used	Operational capability confirmed by credible evidence	Some evidence that operational capability exists; not confirmed	No evidence of operational capability but feasibility confirmed	No evidence and even feasibility unconfirmed
Tactic has been used in the past and a similar attack may be planned	Very High	Very High	High	Medium	Low
Tactic has been used before and it is credible that it is being considered for further use	Very High	High	High	Medium	Low
Tactic has not been used before but is under consideration	High	High	Medium	Medium	
Tactic has not been used before but it may be under consideration	Medium	Medium	Medium	Low	
Tactic has not been used before and is not known to be under consideration	Low	Low	Low	Very Low	

Threat Rating	Threat Rating Definition
VERY HIGH	Significant and proven threat present based upon demonstrated intent and demonstrated capability
HIGH	Threat present based upon stated/demonstrated intent with demonstrated capability.
MEDIUM	Medium level threat exists based upon either strong intent or some degree of stated/demonstrated capability.
LOW	General threat exists and should be monitored – no proven intent or demonstrated capability
VERY LOW	General threat may exist with intent and capability feasibility unconfirmed

Security Risk Assessment: Vulnerability

Vulnerability Level	Assessment Criteria
Very High	• Non-existent physical and procedural mitigations • Inadequate mitigation measures: likely to fail to deter, detect, delay, or respond • No security awareness culture • No business or operations contingencies to manage security events and recover. • Severe disruptions are likely
High	• Some mitigations are present, but likely ineffective at deterring, detecting, delaying, or responding • More than 50% of existing mitigation measures are likely to fail to deter, detect, delay, or respond • No security exercises performed or planned • Few contingencies/plans are in place for business and operations recovery. • Significant disruptions likely
Moderate	• 50% of advanced physical and procedural mitigation measures are effective with remaining measures likely to fail to deter, detect, delay, or respond to a security risk • Existing mitigations are capable of deterring, detecting, delaying, and responding to basic security risks • Exercise program exists and exercises are performed for select areas • Basic security awareness culture • Contingencies/plans are in place across most but not all key areas of business and operations. • Disruptions are likely
	• 50% - 80% of advanced physical and procedural mitigation measures are effective • Existing mitigations are capable of deterring, detecting, delaying, and responding • Procedures and evidence of audit and review of existing security measures

- **Vulnerabilities** can be procedural or physical
- **Physical vulnerability**: a deficiency, flaw, or absence of physical measures designed to deter, detect, delay, and/ or respond to a threat
- **Procedural vulnerability**: the lack of policies and procedures, which are designed to deter, detect, delay, and/or respond to a threat

Security Risk Assessment: Likelihood

Threat	Vulnerability				
	Very High	High	Moderate	Low	Very Low
Very High	Almost Certain A	Almost Certain A	Highly Likely B	Likely C	Likely C
High	Almost Certain A	Highly Likely B	Highly Likely B	Likely C	Possible D
Medium	Highly Likely B	Likely C	Likely C		
Low	Likely C	Likely C	Possible D		
Very Low	Possible D	Possible D	Possible D		

Likelihood Rating	Likelihood Characteristics
Almost Certain (A)	Vulnerability exists and threat is proven and demonstrated. Threat realization can be expected to occur during the system's operational phases
Highly Likely (B)	Vulnerability exists and threat is proven although may not be demonstrated. Threat realization may be expected during system's operational phases
Likely (C)	Some vulnerability exists and threat has some resource, experience, and skill, though may not be demonstrated. Threat realization may occur during the system's operational phases
Possible (D)	Limited vulnerability and threat may be under resourced or lack experience and skill, should not occur during the system's operational phases
Remote (E)	Limited vulnerability exists or threat has not been proven or demonstrated, not expected during the system's operational phases

Security Risk Assessment: Severity / Consequence

Severity	Characteristics			
	People	Equipment/ Services	Financial	Reputational
Catastrophic 1	Several deaths and/or numerous severe injuries	Total loss of equipment or system interruption, requiring months to repair	Estimated loss from the incident in excess of $5 million	Ongoing international media coverage, irreparable reputational damage, government intervention Weeks - Months
Significant 2	Low number of deaths and/or severely injured	Significant loss of equipment or system interruption, requiring weeks to repair	Estimated loss from the incident in the range of $500,000 to $5 million	Prolonged media campaign, serious reputational damage, sustained government involvement Days - Weeks
Moderate 3	Minor injury and possible serious injury	Some loss of equipment or system interruption, requiring seven or less days to repair	Estimated loss in the range of $ 50,000 to $500,000	Adverse media coverage, reputational damage, government involvement
Minor 4	Possible minor injury	Some loss of equipment, no system interruption, less than 24 hours to repair	Estimated losses are relatively minor, in the range of $1,000 to $49,999	Local media coverage and some reputational damage
None/ Negligible 5	No injury	Minor damage to equipment no system interruption, no immediate repair necessary	Estimated loss from the incident are likely less than $1,000	No adverse media coverage or reputational damage

Security Risk

Potential Consequences or Severity	Likelihood				
	Almost Certain A	Highly Likely B	Likely C	Possible D	Remote E
Catastrophic – 1	Very High 1A	Very High 1B	High 1C	High 1D	Moderate 1E
Significant – 2	Very High 2A	High 2B	High 2C	Moderate 2D	Moderate 2E
Moderate – 3	High 3A	High 3B	Moderate 3C	Moderate 3D	Low 3E
Minor – 4	Moderate 4A	Moderate 4B	Moderate 4C	Low	Very Low
Low/Negligible – 5	Low 5A	Low 5B	Low 5C		

Risk index	Risk Rating	Action Required
1A, 1B, 2A	VERY HIGH	Risk must be immediately mitigated and constantly monitored
1C, 1D, 2B, 2C, 3A, 3B	HIGH	Risk must be treated and constantly monitored
1E, 2D, 2D, 2E, 3C, 3D, 4A, 4B	MODERATE	Risk should be managed and reduction strategies implemented
3E, 4D, 5A, 5B, 5C	LOW	Risk may be accepted after a risk review
4E, 5D, 5E	VERY LOW	Risk would normally not be treated

Project Overview & Approach

WSP Security Assessment Approach

Stakeholder Engagement & Partner Collaboration

Stakeholder Engagement Plan

- Stakeholder contacts
- Engagement database
- Activities to engage stakeholders (surveys, workshops)

Stakeholder Activity Facilitation & Media Messaging

- Facilitation of activities to engage stakeholders
- Taking input and providing feedback about the project
- Developing public-facing messaging and media-relations

Security Risk & CPTED Training

- Customized security risk and CPTED Training to emphasize the risk based approach to system security
- Scheduled for June 28th

Inventory & Assessment of Existing MetroLink System

MetroLink Inventory

- Inventory of current security conditions
- Physical assets, procedures, staffing, relationships

Security Staffing Assessment

- Current state of security staffing
- Effectiveness and efficiency
- Challenges and needs
- Performance measures

Fare System Analysis

- Effectiveness of the fare enforcement program
- Equity of fare enforcement program

Best Practices / Peer Review

- Peer review by transit / rail staff from comparable agencies
- Best practice review

Threat & Vulnerability Assessment

- Acceptable / Tolerable Risk
- As Low As Reasonable Practicable (ALARP) Risk
- Mitigations / Controls

Recommendations & Implementation Plan

Recommendations

- Summary of recommendations to improve security of the system
- Physical enhancements, procedural adjustments, & strategic direction

Implementation Plan

- Plan to implement recommendations
- Order of magnitude cost estimate
- Implementation timeframe

Presentations / Summaries

Stakeholders

Stakeholders

Metro

St. Claire County

St. Louis County

Passengers

???

City of St. Louis

Citizens for Modern Transit

ATU / SEIU

First Responders (PD/FD)

Questions?

THANK YOU

Discussion & Questions