

TPU SAFETY PROGRAM UPDATE



Public Utility Board Study Session
October 10, 2018
John Lawrence
Jim Boyd

TPU IS COMMITTED TO SAFETY EXCELLENCE

- Top management is **visibly** committed
- Middle management is **actively** involved
- Front-Line supervision is **performance**-focused
- Employees are actively **participating**
- System is **flexible** to accommodate culture
- Safety system is **positively perceived** by workforce



TPU SAFETY FOCUS

Key Objectives

- Key Performance Indicators
- National Safety Council
- Caterpillar Safety Services
- Organizational Structure
- 19/20 Safety Budget
- Injured Worker Prevention Programs



TPU SAFETY METRICS

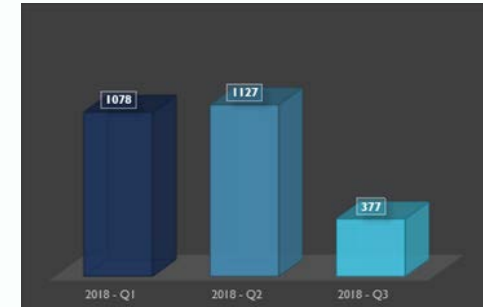
Quarter 2, 2018 Performance Metrics Report Tacoma Public Utilities



Financial Performance:		Power	Water		Rail			
1	Debt Service Coverage	<div></div>	1	Debt Service Coverage	<div></div>	1	Debt Service Coverage	<div>N/A</div>
2	Liquidity - Days Cash on Hand	<div></div>	2	Liquidity - Days Cash on Hand	<div></div>	2	Liquidity - Days Cash on Hand	<div></div>
3	Budget Performance	<div></div>	3	Budget Performance	<div></div>	3	Budget Performance	<div></div>
Operational Excellence:		Power	Water		Rail			
4	Residential Bill Comparison	<div></div>	4	Residential Bill Comparison	<div></div>	4	Railroad Tariffs Comparison	<div></div>
5	O&M Cost per Customer	<div></div>	5	O&M Cost per Account	<div></div>	5	Operating Ratio	<div></div>
6	Outage Duration	<div></div>	6	Unplanned Service Disruptions	<div></div>	6	Revenue Moves per Shift	<div></div>
7	Outage Frequency	<div></div>	7	Distribution System Leakage	<div></div>	7	On-Time Switching	<div></div>
8	Non-Carbon Power Resources	<div></div>	8	Regulatory Compliance	<div></div>	8a	Diesel Conversion	<div></div>
9	Power Conservation	<div></div>	9	Water Conservation	<div></div>	8b	Storm Water Remediation	<div></div>
Commitment to Cust & Employees:		Power	Water		Rail			
10	Customer Satisfaction	<div></div>	10	Customer Satisfaction	<div></div>	10	Customer Satisfaction	<div></div>
11	Employee Satisfaction	<div>TBD</div>	11	Employee Satisfaction	<div>TBD</div>	11	Employee Satisfaction	<div>TBD</div>
12	Employee Safety	<div></div>	12	Employee Safety	<div></div>	12	Employee Safety	<div></div>
13	Call Center Responsiveness	<div></div>	13	Call Center Responsiveness	<div></div>			
			14	Technical Service Complaints	<div></div>			

TPU'S NEW LEADING SAFETY PERFORMANCE INDICATORS

- Senior Leadership Performing Crew Site Visits and Observations
 - Definition of “senior leadership” = Workgroup Manager / Division Manager level or higher including Chief Officers
 - Definition of “senior leadership performing work observations” = Documented field audit of safe & unsafe processes, equipment, and practices which can include work process review, employee interviews, written program review, JHA review, and field observations.
 - Number of observations performed/documented by quarter (gross number of observations & ratio of observations per 100 EE)
- Corrective Actions
 - Definition of “timely implementation of corrective actions” = All hazards identified through any method including but not limited to regular worksite inspections, field observation programs, ergonomic assessments, injury or vehicular incident review, good catch or near miss reporting shall be reviewed to develop strategies and corrective actions for abatement which are intended to be completed within a 90-day timeframe.
- Good Catch / Near Miss
 - Definition of “GC/NM” = An unintended, unplanned, or unexpected event that could have, but did not result in personal injury or property damage.
 - Number of GC/NM reported by quarter (gross number reported & ratio of GC/NM per 100 EE)



NATIONAL SAFETY COUNCIL

- Extensive background and experience in Safety Process Management systems
- Provides comprehensive solutions to developing and implementing program components
 - ✓ Plans, Policies and Programs
- Provide training to Safety Staff assuring common safety practices and understanding across the utility



Initial Engagement

WE Engaged Our Employees
Communicated The Results
Got Commitment From Leaders AT All Levels

Division	# of Respondents			Score			Perception Gap		
	Emp.	Sup.	Mgr.	Emp.	Sup.	Mgr.	Emp. Sup.	Emp. Mgr.	Sup. Mgr.
COMPOSITE	993	134	97	72.7	74.4	77.2	5.0	7.2	4.3
Tacoma Power	551	81	52	74.1	75.1	75.5	4.4	5.9	3.8
Tacoma Water	165	28	16	79.5	75.2	84.7	8.1	9.0	13.8
Customer Service	131	15	5	62.6	64.8	67.1	10.8	16.2	13.0
Tacoma Rail	85	6	8	63.1	88.0	86.1	41.1	38.5	6.6
City Administration	61	4	16	73.4	61.3	73.4	20.0	7.4	32.1



CATERPILLAR SAFETY SERVICES

Next Engagement

WE

- Would like to leverage Caterpillar to implement recommendations & next steps
- Are initially focusing on employees with the greatest exposure to hazards
- Intend to train all supervisors & managers responsible for employees with greatest exposure to hazards
- Will implement Train The Trainer Programs for long term sustainability



CATERPILLAR SAFETY SERVICES

Scope of Work

➤ Safety Culture Training

- ✓ **Supervisor Training in Accountability & Recognition Techniques S.T.A.R.T. (approx. 70 TPU Supervisors & Managers)**
 - Provide managers and supervisors the skills to affect safety perceptions and behaviors throughout organization. Why accountability works' how incidents impact the bottom line & leadership's role in improving culture
- ✓ **Safety Excellence Workshops (approx. 670 employees)**
 - Designed to equip participants with key insights, strategies and tools necessary to enable strong safety performance
 - Integrating safety management into the daily operation of the business at all levels
 - Establishing a positive safety culture built upon catching employees doing things right
 - Building trust, improving management credibility, and strengthening communications
- ✓ **Speak up/Listen up training**
 - Designed to help employees learn how to give safety-related feedback to co-workers. Improve workplace safety by learning simple, easy-to-use feedback techniques.
- ✓ **Provide Safety Steering Committee training & on-going consultation**
 - Using the assessment findings produced from the TPU Safety Perception Survey begin building a plan that identifies priorities, resources, specific actions to address opportunities to strengthen TPU's Safety Culture
- ✓ **Provide Train the Trainer training**

➤ Rapid Improvement Workshops

- ✓ **Engage front-line employees in developing high quality, measureable accountability systems that integrate safety activities into everyday processes**

CATERPILLAR SAFETY SERVICES

Scope of Work

➤ On/off site consultation

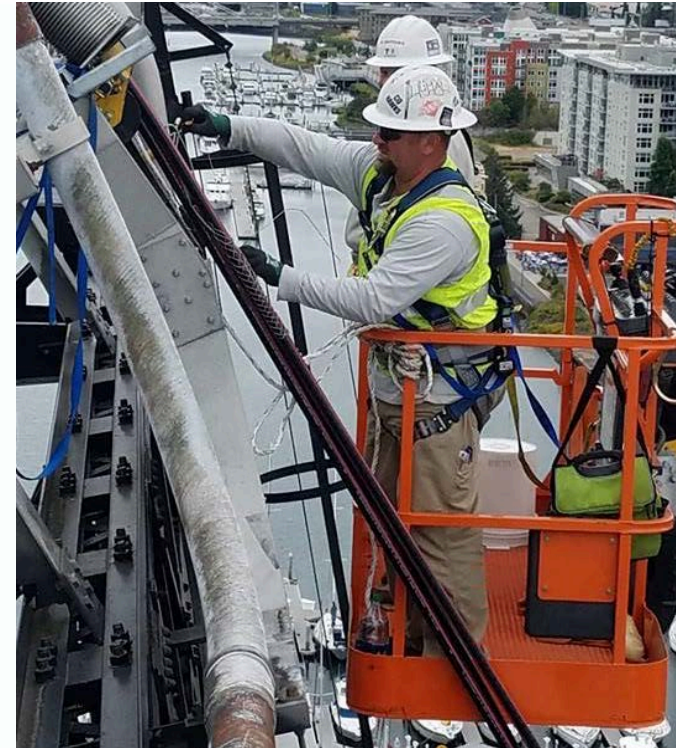
- ✓ Employee Communications & Messaging
- ✓ Strengthen TPU's Safety Culture
- ✓ Safety Training Development
- ✓ Process Improvement
- ✓ Accountability & Recognition
- ✓ Safety Excellence

➤ Capital Intellect

- ✓ Establish internal expertise for long term sustainability
- ✓ Acquire Caterpillar training tools & materials
- ✓ Develop 30 trainers across TPU

➤ Contract Costs

- ✓ \$397,678.00
- ✓ Initial focus 670 employees
- ✓ Price per employee \$593.55

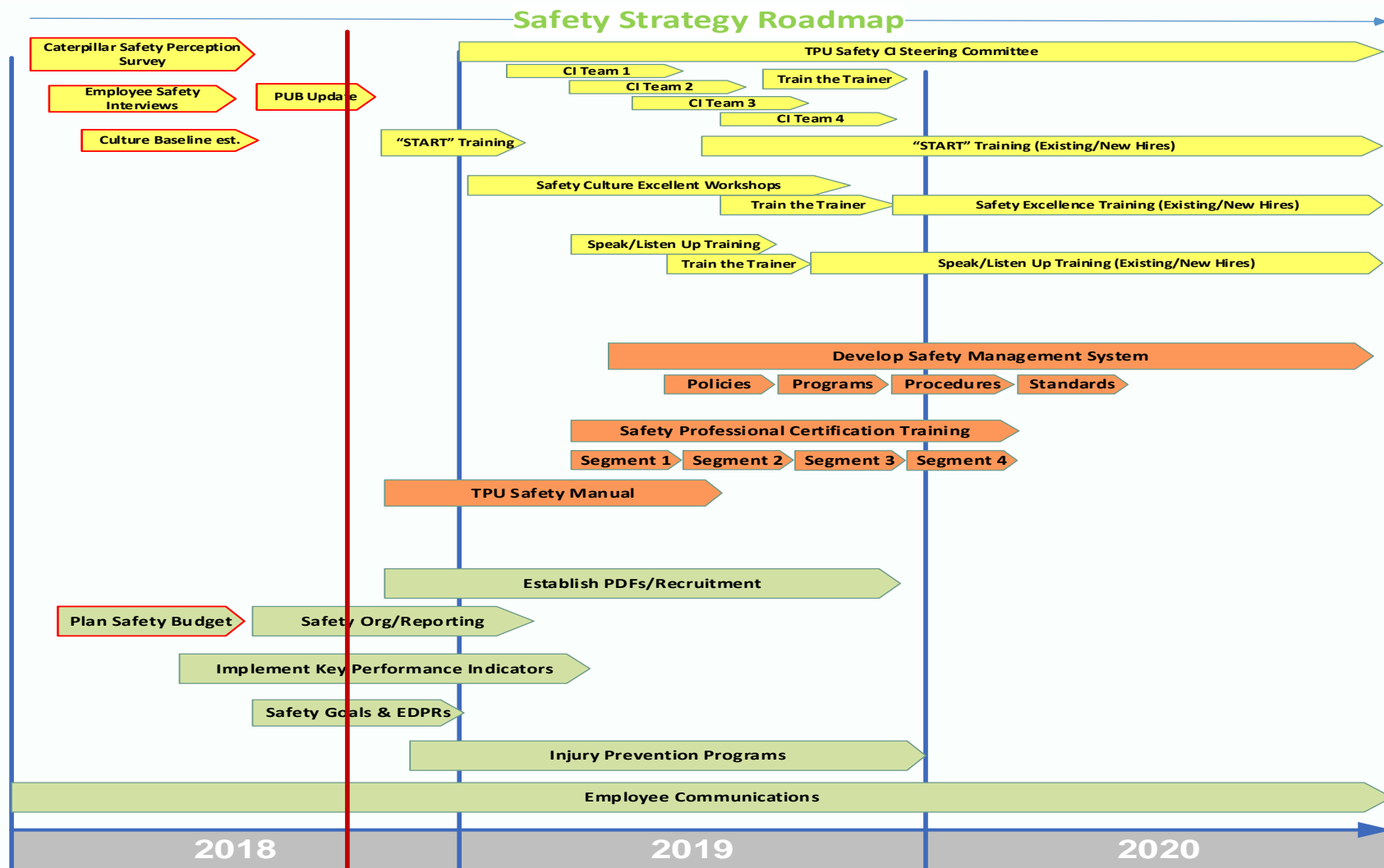


TPU'S SAFETY STRATEGY ROADMAP

Caterpillar Safety Services

National Safety Council

TPU Led Initiatives



SAFETY ORGANIZATIONAL STRUCTURE & BUDGET

➤ Safety Workshop

✓ Executive Leadership Across City of Tacoma

- Safety Excellence
- Identify gaps & opportunities
- Recommend organizational structure

➤ TPU 19/20 Budget

✓ New FTEs

✓ Professional Services

- Caterpillar Safety Services
- National Safety Council



EXPLORING INJURY PREVENTION & WORKER CARE PROGRAMS

- Develop and implement programs that will educate employees on soft tissue injury prevention as well as provide stretching and pre-work warm up routines
- Develop and implement programs to provide initial support to injured workers to assist in evaluating the injury and treatment path moving forward



NEXT STEPS

- Utility Board Approval for Caterpillar Safety Services
- Implement TPU KPIs
- Finalize Organizational Structure and Staffing Plan
- Recruit and hire for Safety Support Staff Positions
- Continue Joint Labor Engagement
- Continue Employee Communications Updates



Legislative Policies

October 10, 2018

- Clark Mather, Community and Government Relations Manager



Overview

- Review edits seeking to incorporate PUB feedback to the City of Tacoma's Legislative Policies Statement
- Feedback due to General Government staff on October 11
- City Council scheduled to adopt resolution on October 16

Incorporating PUB feedback

- **Page 25 – Defining sustainability**
 - “Sustainability is a balance between equity, the environment, and the economy.”

Incorporating PUB feedback

- **Page 57 – Protecting City of Tacoma’s telecommunications authority**
 - “The City supports policies that allow current telecommunications operations and the flexibility to provide emerging services. The City opposes any restriction of its authority to operate a telecommunications utility.”

Incorporating PUB feedback

- Page 61 – Telecommunications section update
 - ~~Voice over Internet Protocol (“VoIP”) and IPTV are two examples of services that should be treated just like their equivalents, traditional cable and telephone services.~~

Incorporating PUB feedback

- **Page 61 – Net neutrality**
 - The City supports policies that promote net neutrality, open internet access, and customer privacy for all citizens of the United States.

What's Ahead...

Tacoma City Council scheduled to adopt resolution/Legislative Policy Statement

- Tuesday, October 16, 2018

2018 General Election

- Washington General Election – Tuesday, November 6, 2018

TPU's legislative policies before the PUB

- Wednesday, December 12, 2018

2019 Legislative Session

- 2019 Legislative Session: Monday, January 14, 2019
 - » *Long Session*, lasting for 105 calendar days

116th Congress

- Convenes Thursday, January 3, 2019

CYBERSECURITY UPDATE

UTILITY TECHNOLOGY SERVICES

TYLER SWARTZ, TERRY GIFFORD

OCTOBER 10, 2018







AGENDA

- Background
- TPU Cybersecurity
- Maturity Model
- Key Accomplishments
- Tactical Roadmap
- Questions

“Most people are starting to realize that there are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don’t know it. Therefore, prevention alone is not sufficient...”

Ted Schlein, Security Expert

CYBERSECURITY THREAT ACTORS

ADVERSARY	MOTIVES	TARGETS	IMPACT
 Nation State	<ul style="list-style-type: none"> Economic, political and/or military advantage 	<ul style="list-style-type: none"> Trade secrets Sensitive business info Emerging technologies Critical infrastructure 	<ul style="list-style-type: none"> Loss of competitive advantage Disruption to critical infrastructure
 Organized Crime	<ul style="list-style-type: none"> Immediate financial gain Collect information for future financial gains 	<ul style="list-style-type: none"> Financial Systems Personally Identifiable Information Payment Card Information 	<ul style="list-style-type: none"> Costly regulatory inquiries and penalties Customer or investor lawsuits or confidence
 Hacktivists	<ul style="list-style-type: none"> Influence political and/or social change Pressure business to change their practices 	<ul style="list-style-type: none"> Sensitive business info Information related to key executives, employees, customers & partners 	<ul style="list-style-type: none"> Disruption of business activities Brand and reputation Customer confidence
<hr/>			
 Insiders	<ul style="list-style-type: none"> Personal advantage, monetary gain Professional revenge Patriotism 	<ul style="list-style-type: none"> Deals & market strategies Intellectual property, R&D Business operations Personnel information 	<ul style="list-style-type: none"> Sensitive info disclosure Operational disruption Brand and reputation National security impact

EVOLUTION OF CYBERSECURITY

	Historical Security Perspective	Today's Leading Cybersecurity Insights
Scope of the challenge	<ul style="list-style-type: none"> Limited to your four walls and the extended enterprise 	<ul style="list-style-type: none"> Spans your interconnected global business ecosystem
Ownership and accountability	<ul style="list-style-type: none"> IT led and operated 	<ul style="list-style-type: none"> Business-aligned and owned; CEO and board accountable
Adversaries' characteristics	<ul style="list-style-type: none"> One off and opportunistic; motivated by notoriety, technical challenge and individual gain 	<ul style="list-style-type: none"> Organized, funded and targeted; motivated by economic, monetary and political gain
Information asset Protection	<ul style="list-style-type: none"> One-size-fits-all approach 	<ul style="list-style-type: none"> Prioritize and protect "critical assets"
Defense posture	<ul style="list-style-type: none"> Protect the perimeter; respond <i>if</i> attacked 	<ul style="list-style-type: none"> Plan, monitor, and rapidly respond <i>when</i> attacked
Security intelligence and information sharing	<ul style="list-style-type: none"> Keep to yourself 	<ul style="list-style-type: none"> Public/private partnerships; collaboration within industry

TPU CYBERSECURITY MISSION/VISION

Mission

Cybersecurity Enables the business by ensuring trust in TPU's operational networks and systems.



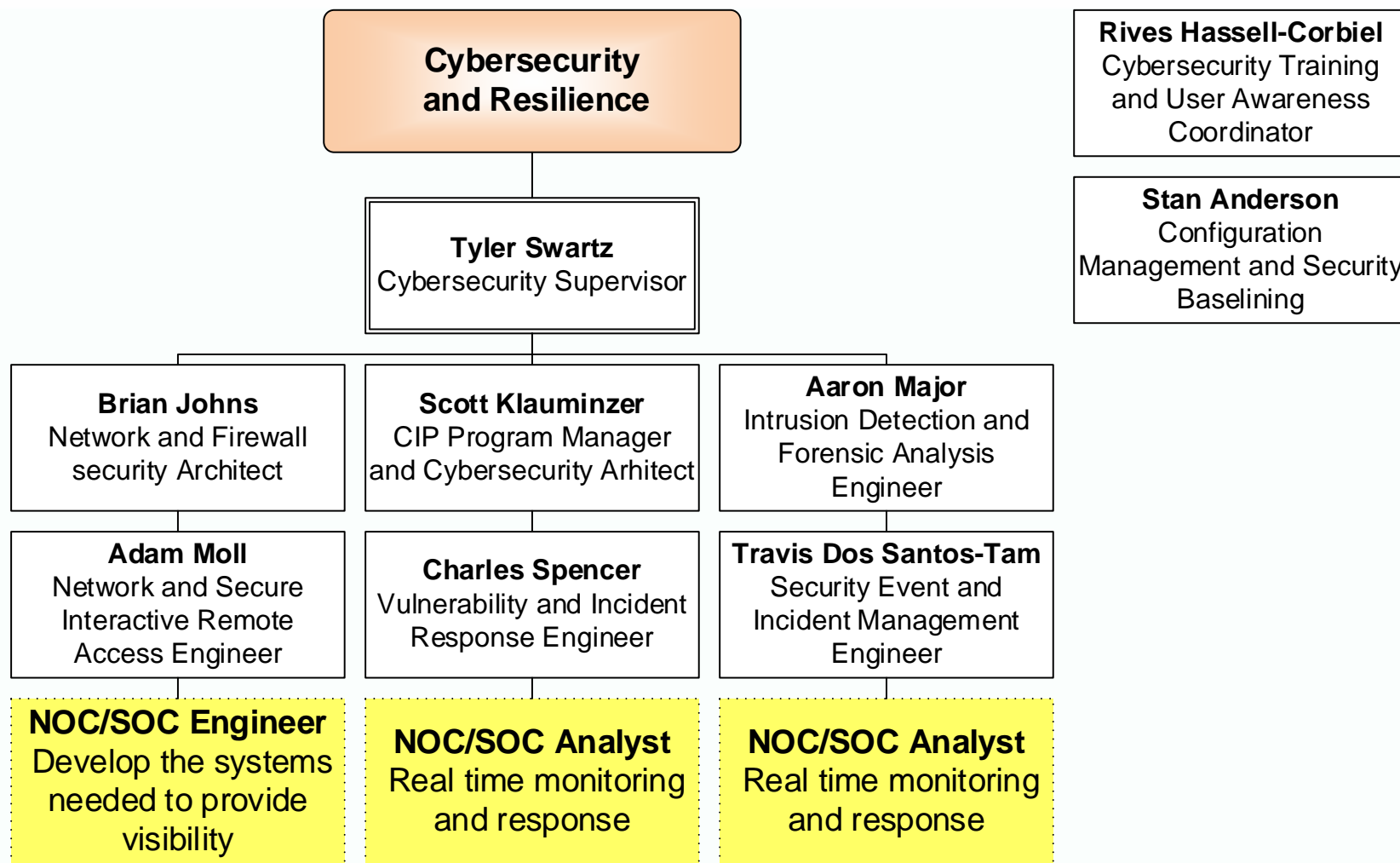
Vision

Visibility – Provide a clear, accurate view of operational technology infrastructure and software assets, and communicate their impact on the Utility.

Awareness – Identify and analyze vulnerabilities, threats and gaps in security controls to prioritize and report the risks posed to the Utility.

Response – Address the most critical risks consistently and effectively, taking into account any mitigating controls.

TPU CYBERSECURITY ORGANIZATION



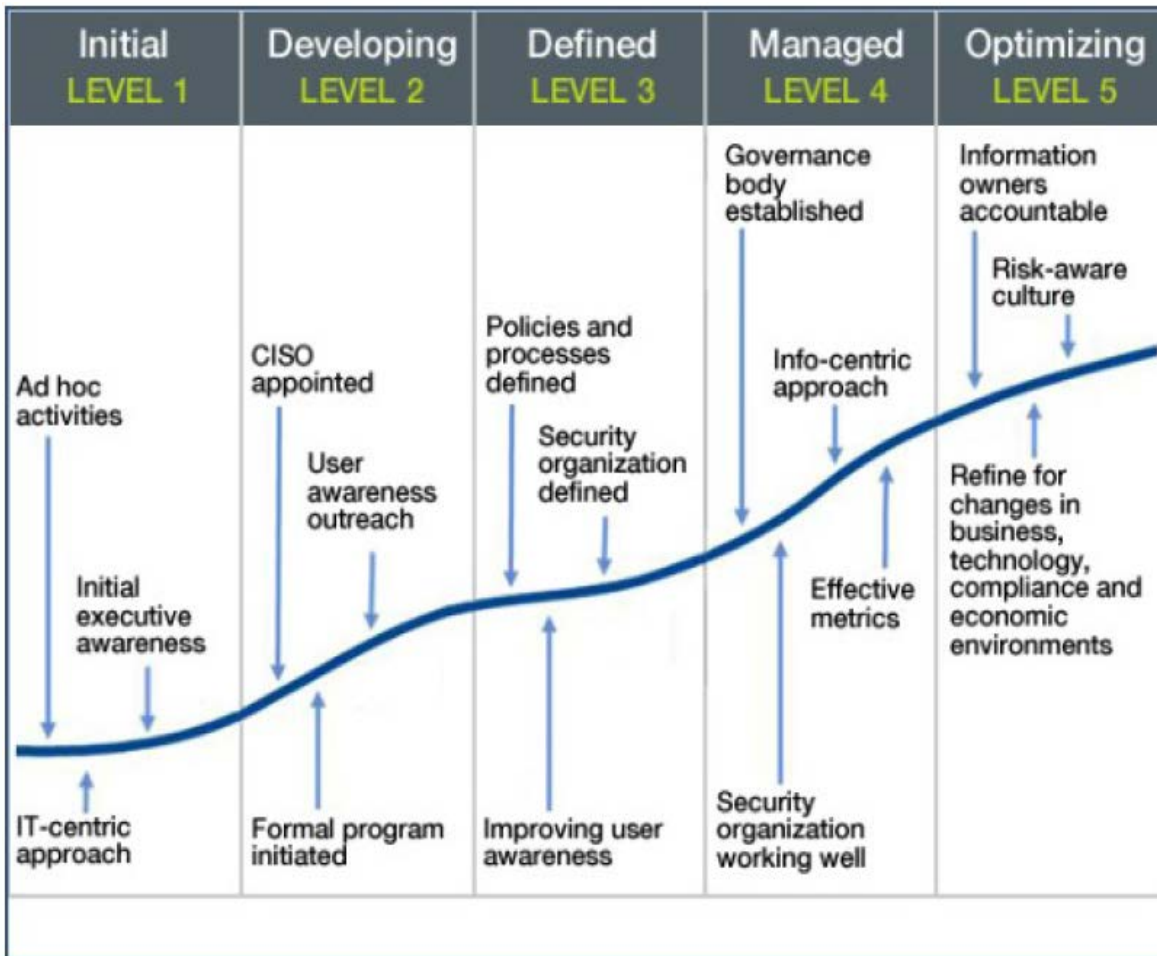
PARTNERS AND INFORMATION SHARING

Partners/Resources

- Ron Jimerson, CoT Chief Information Security Officer
- Large Public Power Counsel – Cyber Security Task Force (LPPC – CSTF)
- FBI Cyber Taskforce
- Industrial Control System – Cyber Emergency Response Team (ICS-CERT)
- Electronic – Information Sharing and Analysis Center (E-ISAC)
- Multi State – Information Sharing and Analysis Center – (MS-ISAC)
- Energy Sector Security Consortium (Energysec)
- And Many More



CYBERSECURITY MATURITY



Previous Cybersecurity Maturity Score – Level 2
Current Cybersecurity Maturity Score – 2.5
Electric & Utility Benchmark 3.8

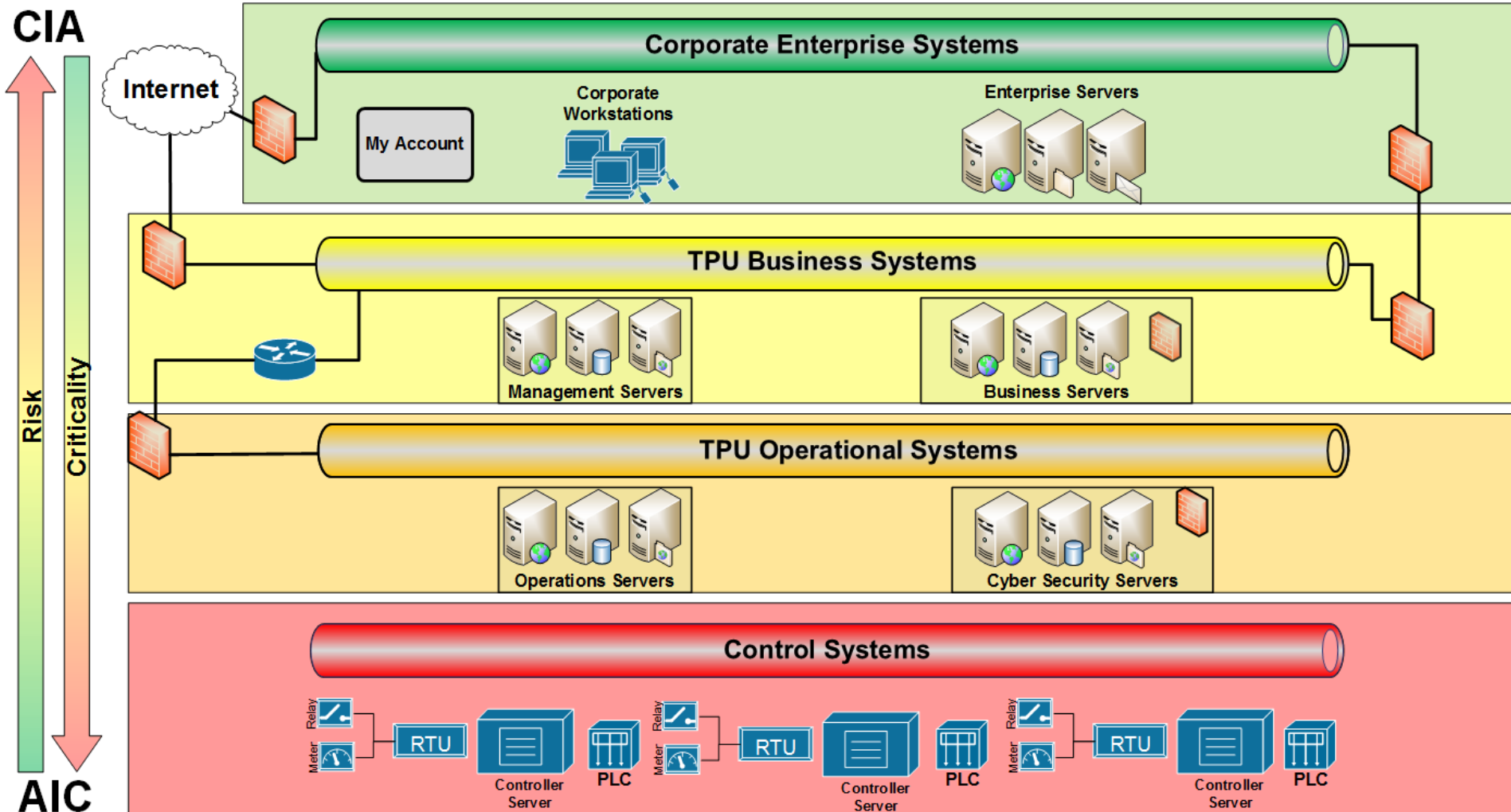
Current State

- We are currently in the developing stage
- All positions are now fully staffed and disciplines assigned
- Cyber Program Policy and Administrative Privileges Policy in flight.
- In process of selecting user awareness vendor

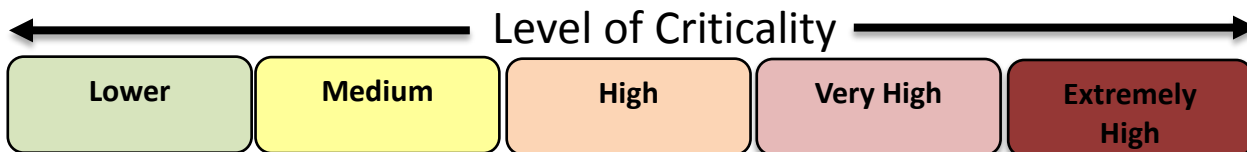
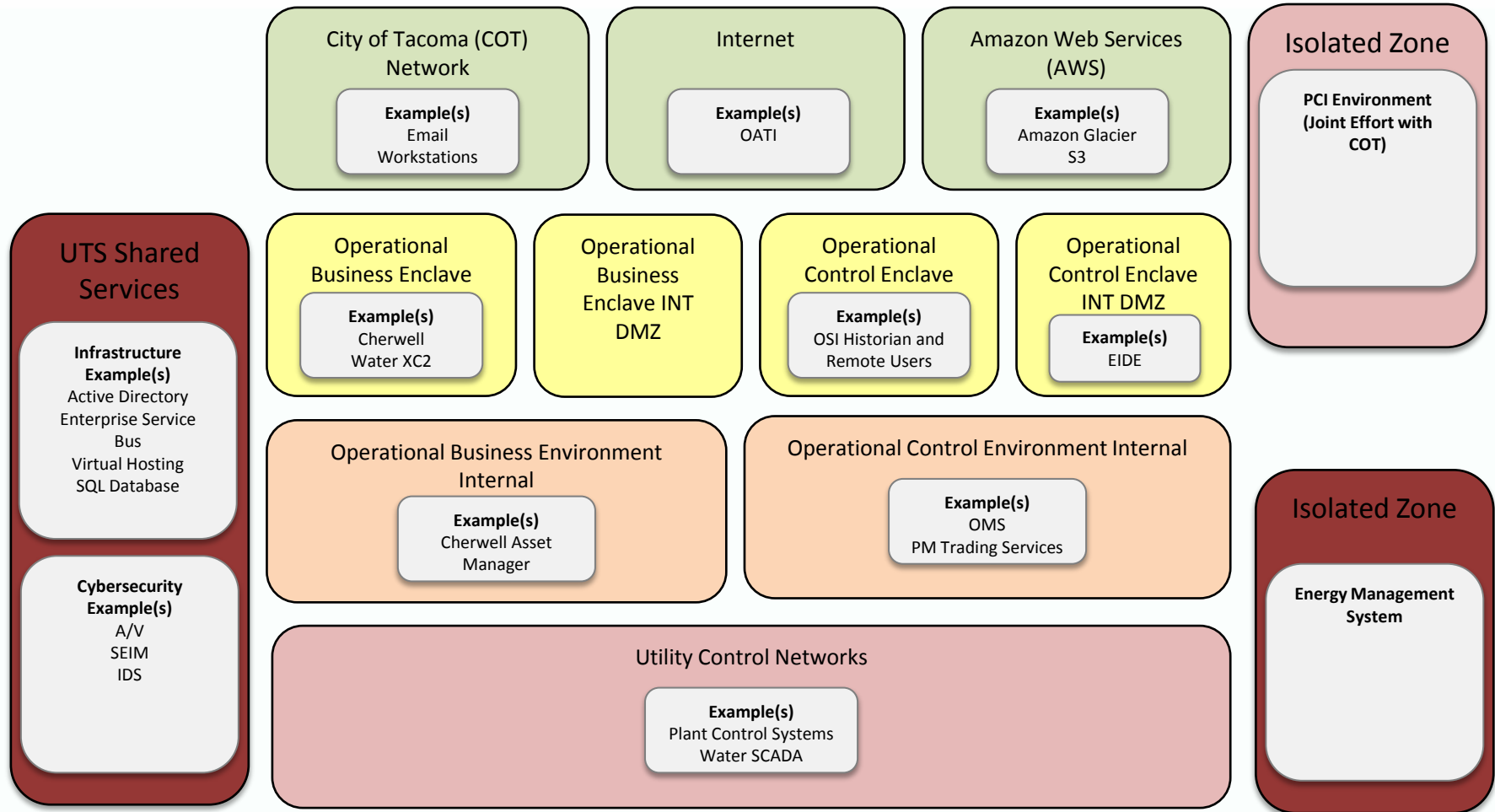
Future State

- Leverage NIST Framework for High, Medium, and Low Cyber Security Activities
- Reach 3.5 target maturity by next report out
- Monitoring & reporting on key security metrics to all levels of management
- Increase TPU to target maturity of 4.0
- Able to rapidly tailor security controls as required

VISIBILITY (PREVIOUSLY)

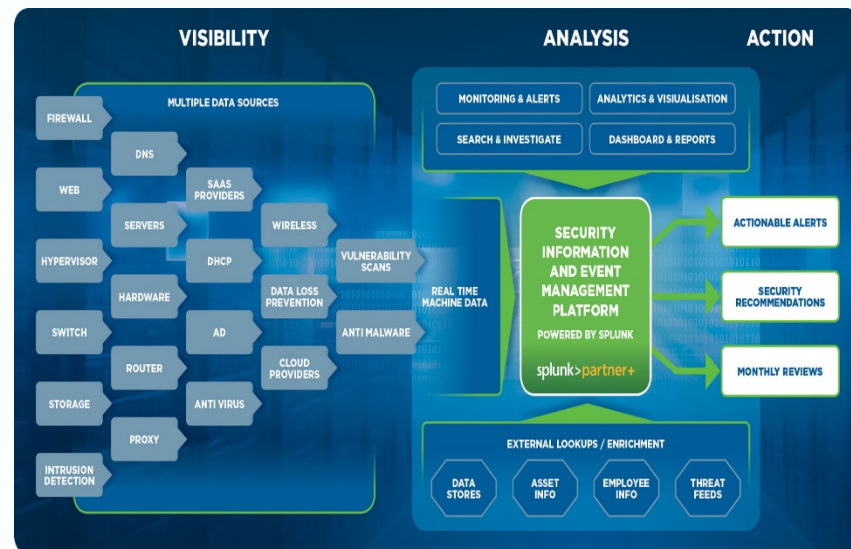


DEFENSE IN DEPTH



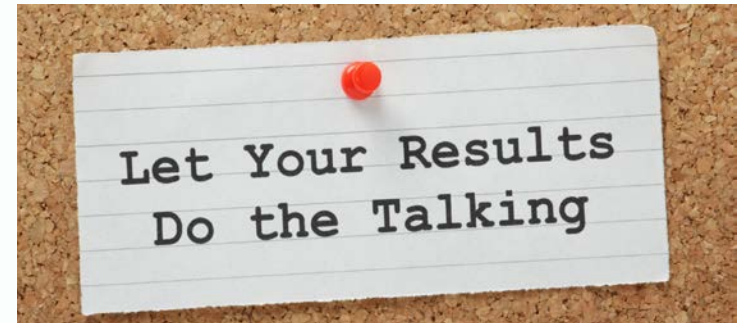
KEY ACCOMPLISHMENTS IN 2017/2018

- **EMS Replacement Project**
- **User Awareness Campaign**
- **Deployed robust secure interactive remote access solution**
 - The solution offers better security and efficiency to the way we work.
- **Upgraded event management solution to industry leader in the space**
 - With the new solution we can now provide visibility to areas we have not had the resources to do so without requiring additional staffing to do so.
- **Security services deployed to Nisqually project**
 - We are increasing our visibility at the hydro projects allowing for a more rapid and targeted response should an incident occur.

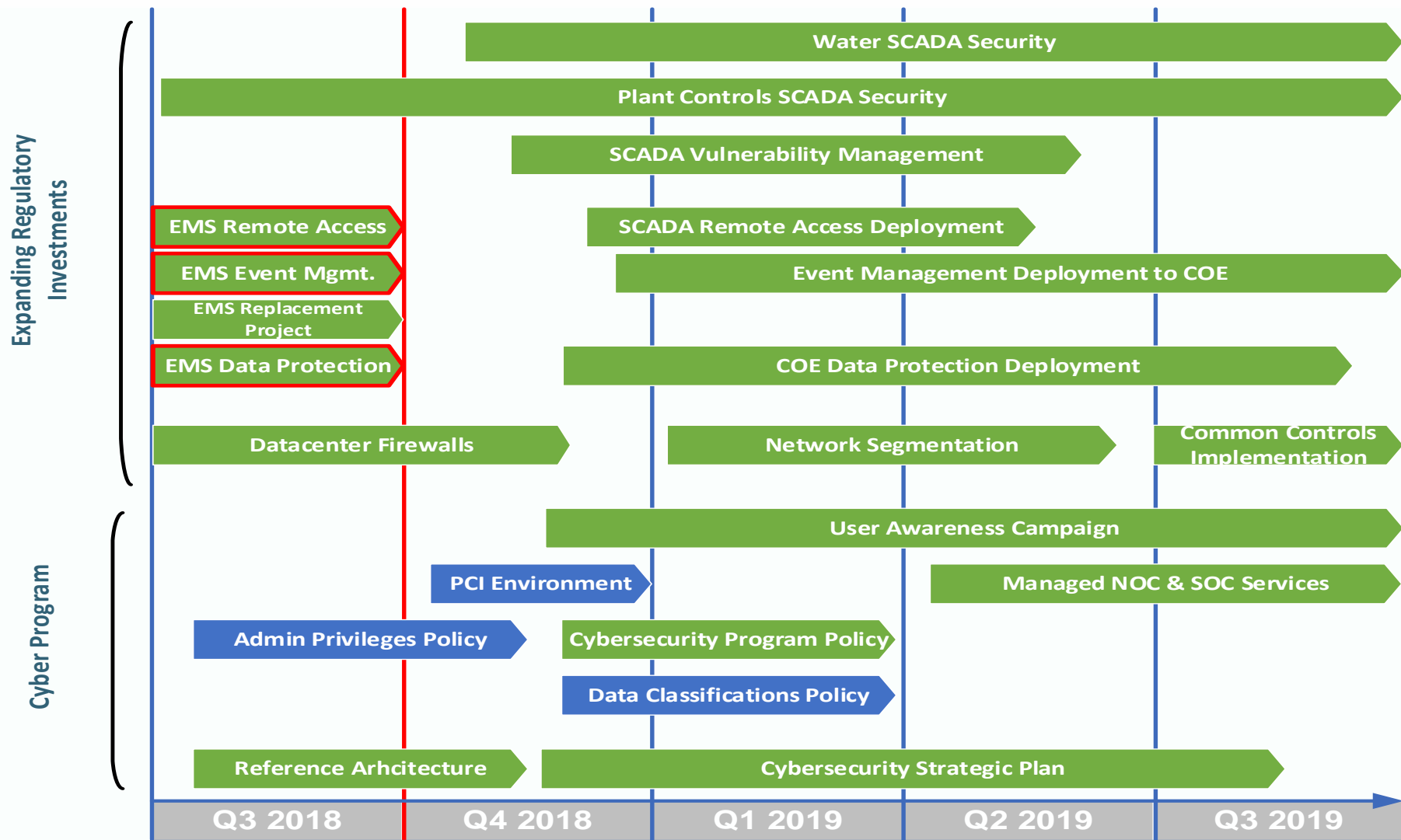


KEY ACCOMPLISHMENTS IN 2017/2018

- **We have begun a campaign to limit local administrative privileges**
 - Within one year we have scaled back users with local administrative privileges to their workstations and seen an 80% decrease in malware incidents
- **New Data protection suite deployed in both the EMS and operational networks**
 - We are moving our posture from one of pure defense to a hybrid model. The new data protection suite gives us the ability to rapidly restore should an incident occur.
- **Increased TPU's cybersecurity from 2.0 to 2.5**
 - We are on track to meet the goals set for this biennium and have a roadmap that will lead us to our target maturity of 4.0



CYBER SECURITY TACTICAL ROADMAP



*Blue projects are joint efforts with ITD

QUESTIONS

