Security Master Planning to Protect Water Resources

Lara Kammereck

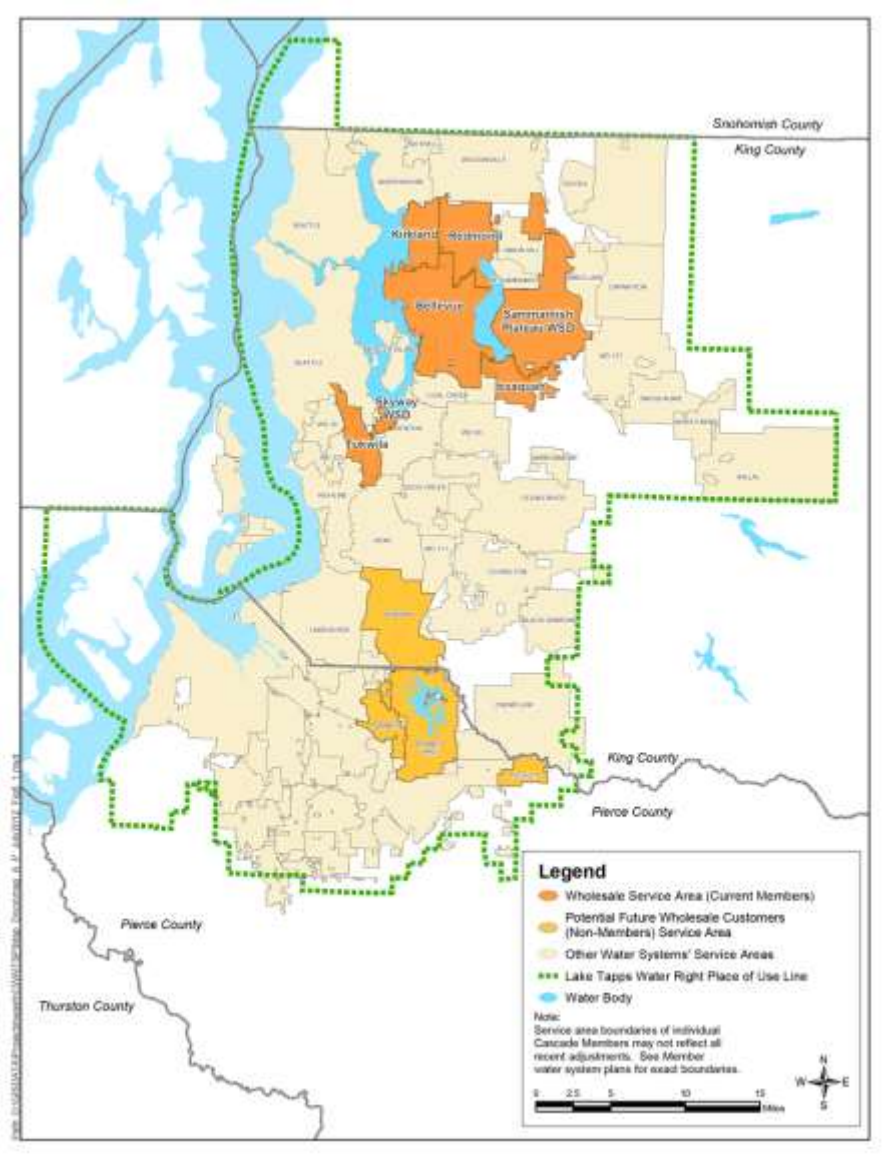
John Saunders

May 1, 2015

carollo
Engineers...Working Wonders With Water®

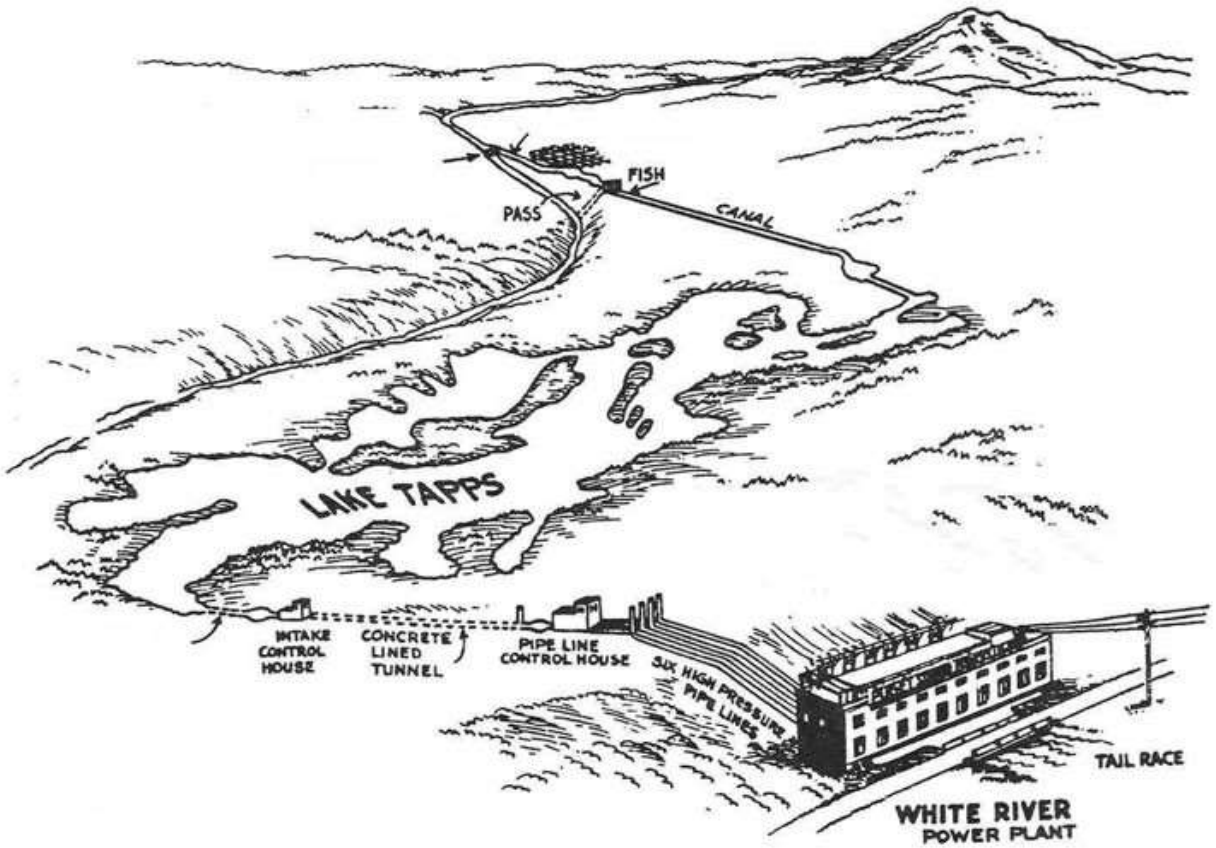
Who is Cascade Water Alliance?

- Joined together in 1999
- 350,000 residents
- 20,000 businesses
- City of Bellevue
- City of Issaquah
- City of Kirkland
- City of Redmond
- City of Tukwila
- Sammamish Plateau Water and Sewer District
- Skyway Water and Sewer District



Regional approach to providing a safe, clean, and reliable water supply

White River Facilities at Lake Tapps



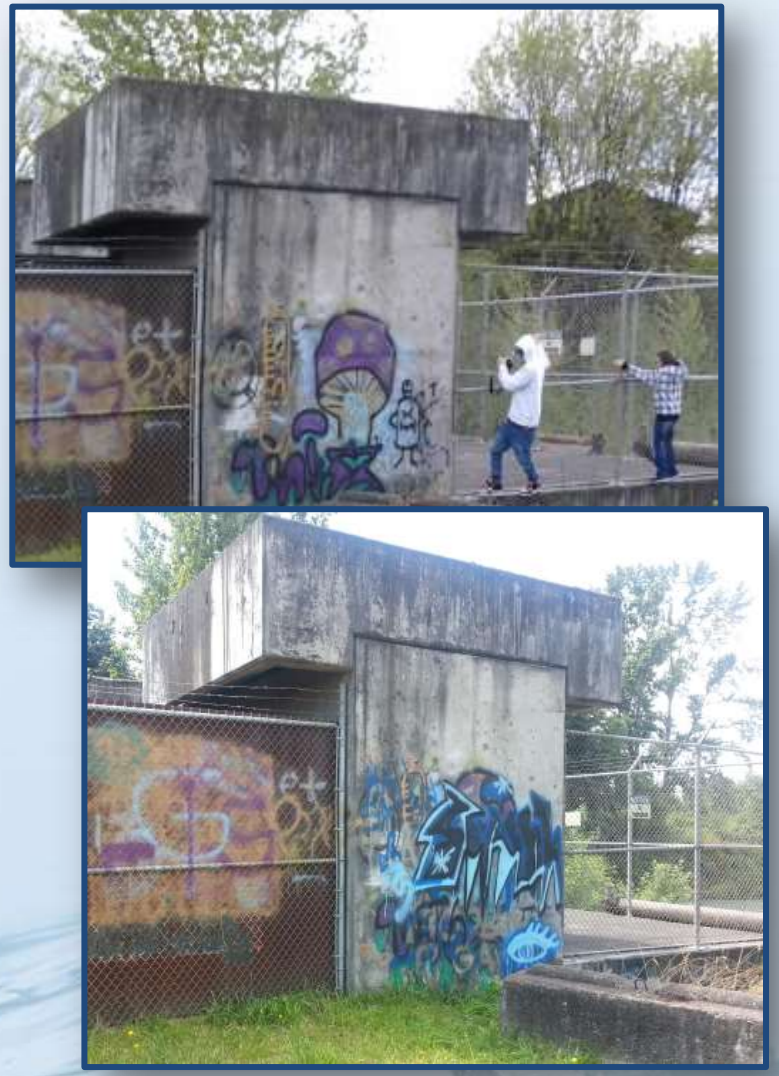
Security Master Plan needed to meet Mission

Cascade's Mission

Establish and maintain the condition, performance and safety of White River Facilities at Lake Tapps.

Case Study: Cascade Water Alliance Security Master Plan

- Proactive security plan
  - Asset/Facility Integrity
    - Operational
    - Structural
  - Public Safety/Liability
  - Financial Investments



Updated Prioritization

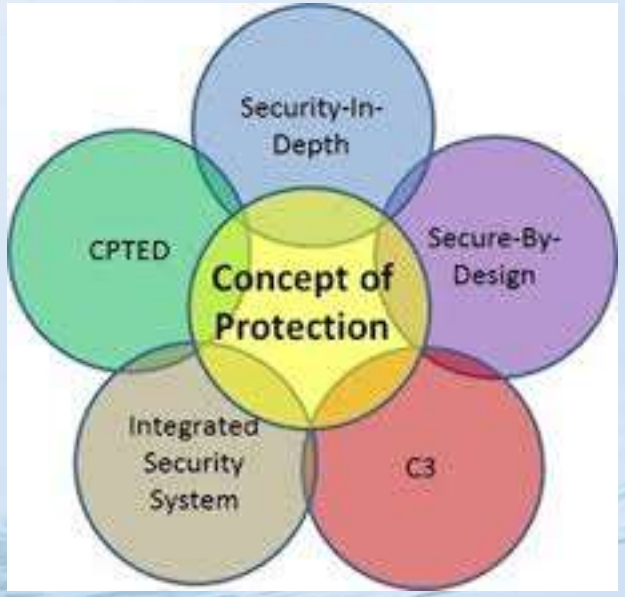
Tunnel Intake
Forebay
Penstocks
Powerhouse and Outflow Structure
Headworks High Priority Assets
Valve House
Fish Screening Facility
Pipe Inlet Structure
Dikes- High Priority
Gauging Station
Tunnel Bear Trap
Backflow Preventer
Dikes- Medium Priority
Twin Pipelines
Standpipes
Tailrace
Settling Basin & 6’ Valve
Canals
Dikes- Low Priority
Headworks Low Priority Assets
Railroad Bridge
Diversion Dam

Security Master Planning

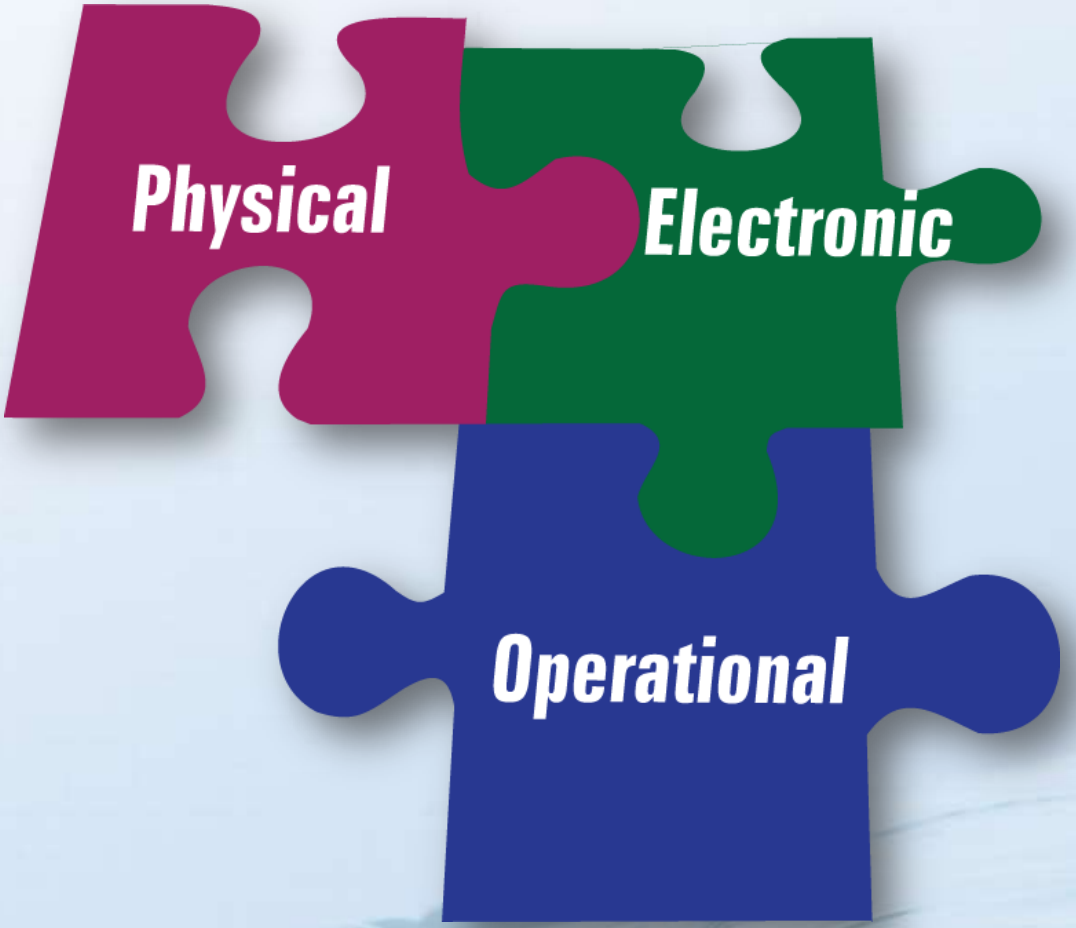
The Security Master Plan forms the basis for security planning and design for all aspects of the organization.

It is Security's business plan.

It identifies and builds the Security Culture



Solutions or Tools?



Methodology

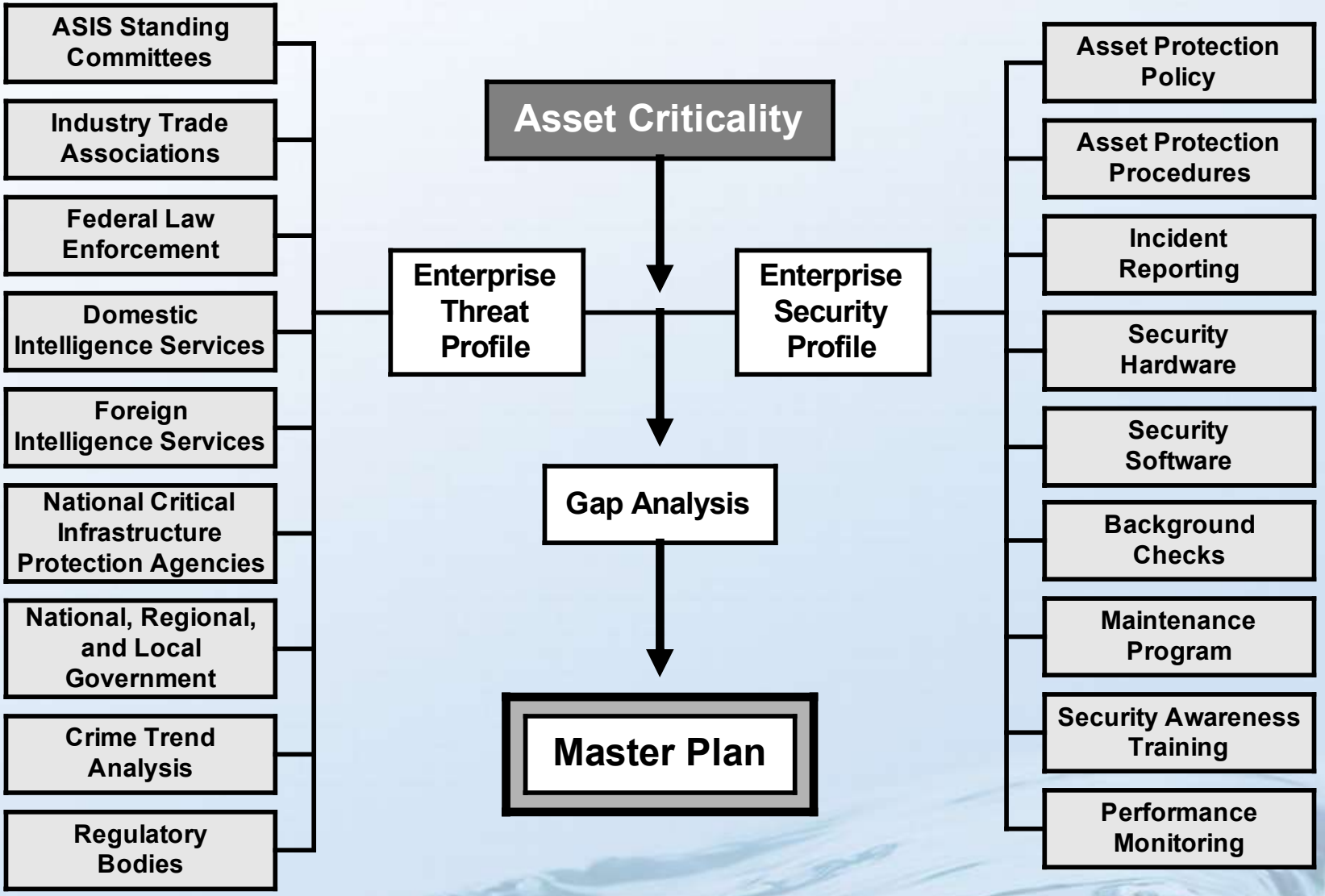
Identify The Objectives To Support The Mission!!!

Project Overview

Cascade's Objectives

- Reliably deliver water through the system assets to meet water supply partnerships and agreements.
- Protect and maintain the facilities to ensure their utility as a future water supply asset.
- **Minimize Cascade's potential liability associated with operation of the facilities**
- Continue to operate/maintain the facilities in a manner that supports current recreational use.

Methodology



Security Planning Process

What Are We Protecting?

1

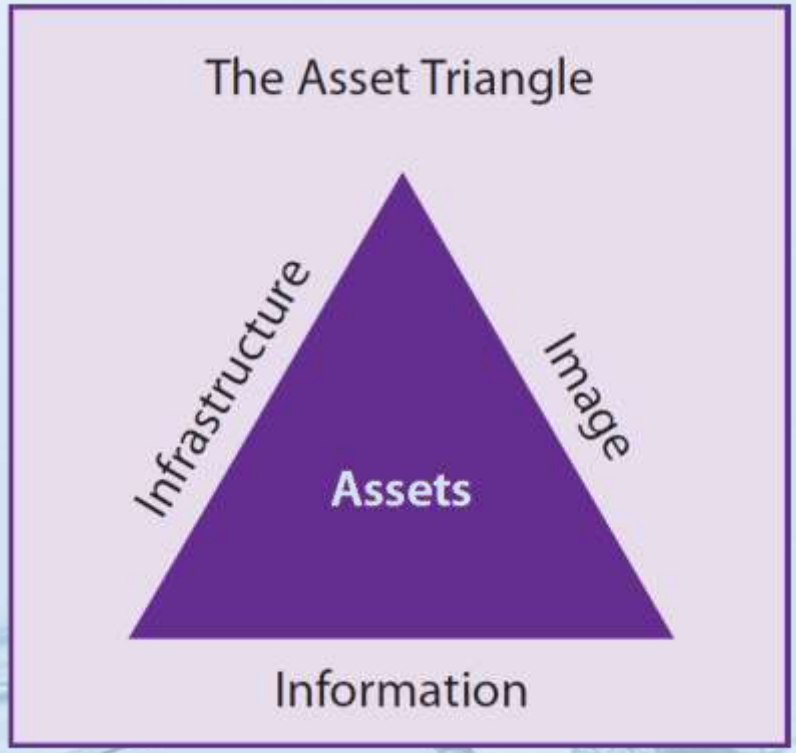
Asset Characterization/Prioritization

What if we didn't? What's the worst that could happen?

Consequence Analysis

1 What Are We Protecting?

What assets exist, how critical are they to the mission?



1 What Are We Protecting? Asset Characterization

- Each asset was individually characterized in terms of:
  - Operational importance
    - Failure consequence
  - Vulnerability
    - Based on proximity to community, vandalism history, accessibility of staff to monitor
  - Public Safety and Liability

What Are We Protecting it From?

2

Threat Characterization

How realistic or probable is that threat?

Threat Assessment

How realistic or probable is that threat?

2

Threats

- Malevolent (man made)
- Natural Hazards
- Dependency/Proximity

2

Threat Risk Assessment was completed using a modified RAMCAP approach

- All Hazards Approach and prioritization of assets is consistent, however the threat and some consequences are different
- **Less about terrorist threat, more about local issues**
- Unique assets dictate approach
  - **Focus on identifiable local threats**
  - This is not a true utility
  - Some assets are not relevant to a utility, yet are important to CWA
  - Geographic spacing

How Are We Protecting It?

3

How are we currently protecting it?

Vulnerability Analysis

Does anything need to change?

Risk/Resilience Assessment

Physical, Electronic, Operational

3

Are We Vulnerable?

- What vulnerabilities would allow a man-made or natural disaster or supply chain problem to cause these consequences?
- Given the scenario, what is the likelihood it will result in these consequences?

Existing and planned mitigation measures are part of this analysis.

Step 4: Recommendations

4 Risk and Resilience Management

- What options are available to
  - Reduce Risk
  - Increase Resilience and Continuity
- What are the costs and benefits of these options?
- How can the options be managed?

Best Practices Apply to All Aspects/Areas of Security

- *Physical Security* - site layouts, locks, fences, gates, materials….
- *Electronic Security* - card systems, system communication, security alarms, electronic intrusion detection….
- Operational Security - standard personnel procedures, training, staff responsibilities and access, etc…

The Result - Security That Makes Sense

- Listened to operational and financial challenges
- Coordinated closely with management and operation staff
- Provided solutions that met specific needs – not cookie cutter recommendations

Realistic, **effective security**

The Plan

- I - General Criteria, Threats, Best Practices
- II - RAMCAP and J100, G430 Standards Compliance
- III - Operational Security Recommendations
- IV - Detailed Site Assessments and Recommendations
- V - System Specifications
- VI - Typical Drawings

Acknowledgements

- Cascade Water Alliance
  - Jon Shimada
  - Joe Mickelson
- Carollo Engineers
  - Dave Sobeck
  - Hannah Pierce

System Recommendations

- Provide consistent locking systems to minimize improper use due to inefficiency and/or user frustration.
- Design and implement automated access control system for use at identified sites. Existing access control at the Powerhouse is limited and unable to provide the organizational requirements across the entire geography.