



Western  
Area Power  
Administration

# Enterprise Risk Overview

Risk, Security and Staff



August, 23 2016

Desert Southwest All-Customer Meeting

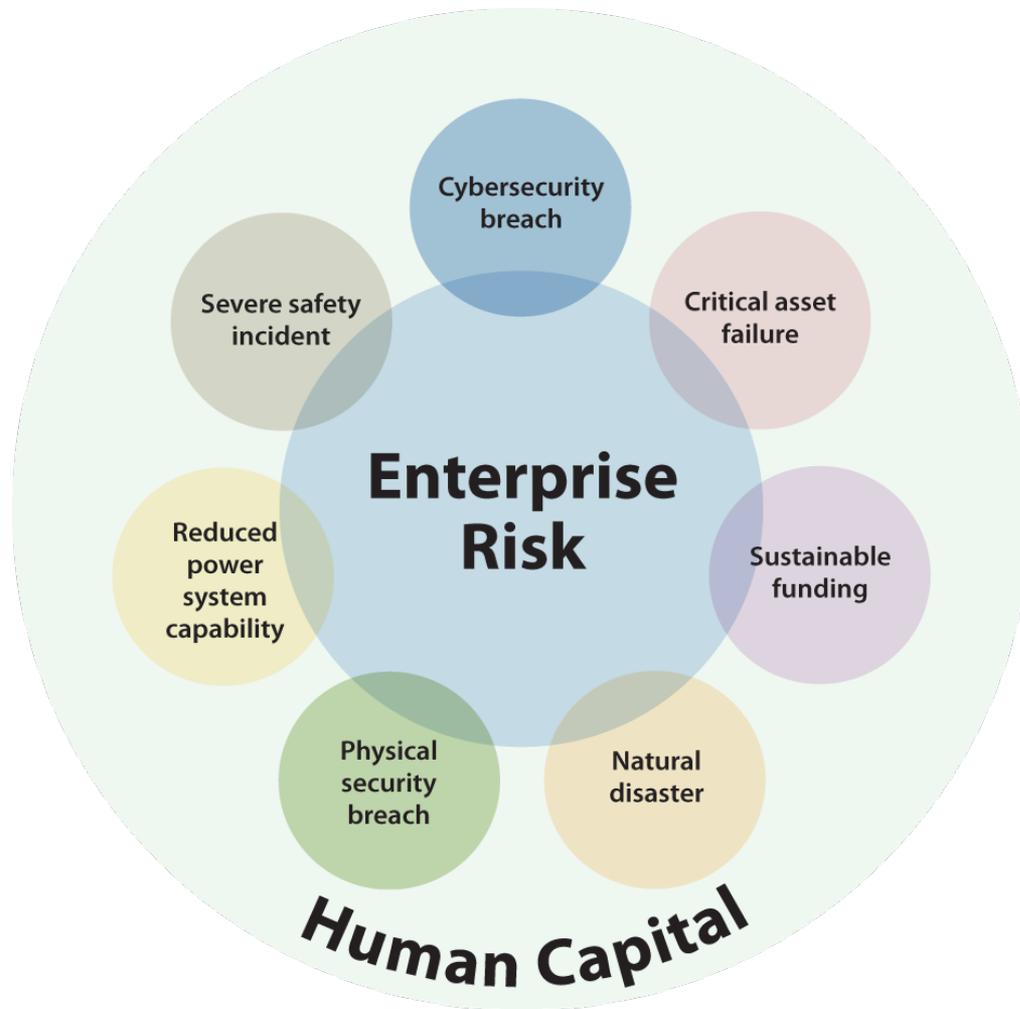
Phoenix, Arizona

# Introduction and Purpose

Mark A. Gabriel | Administrator and CEO



# Understanding critical risks



- Today we will discuss
  - ✓ Cybersecurity
  - ✓ Physical security
  - ✓ Human capital
- Inter-related when it comes to cost and risk acceptance
- Develop context and common understanding for future discussions



# Risk and cost

- Traditional definition is that:

$$\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact}$$

- An additional part of the equation:

$$\frac{\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impact}}{\text{Cost}}$$



# Cybersecurity

Dawn Roth Lindell | Senior VP and CIO



# Cyber attacks: capability vs. intent

- China
- The former USSR nations
- U.S. environmental extremists & anti-government
- Friendly nations
- ISIL
- Dec. 23, 2015, Ukraine Attack



# Ukraine Attack: an analysis

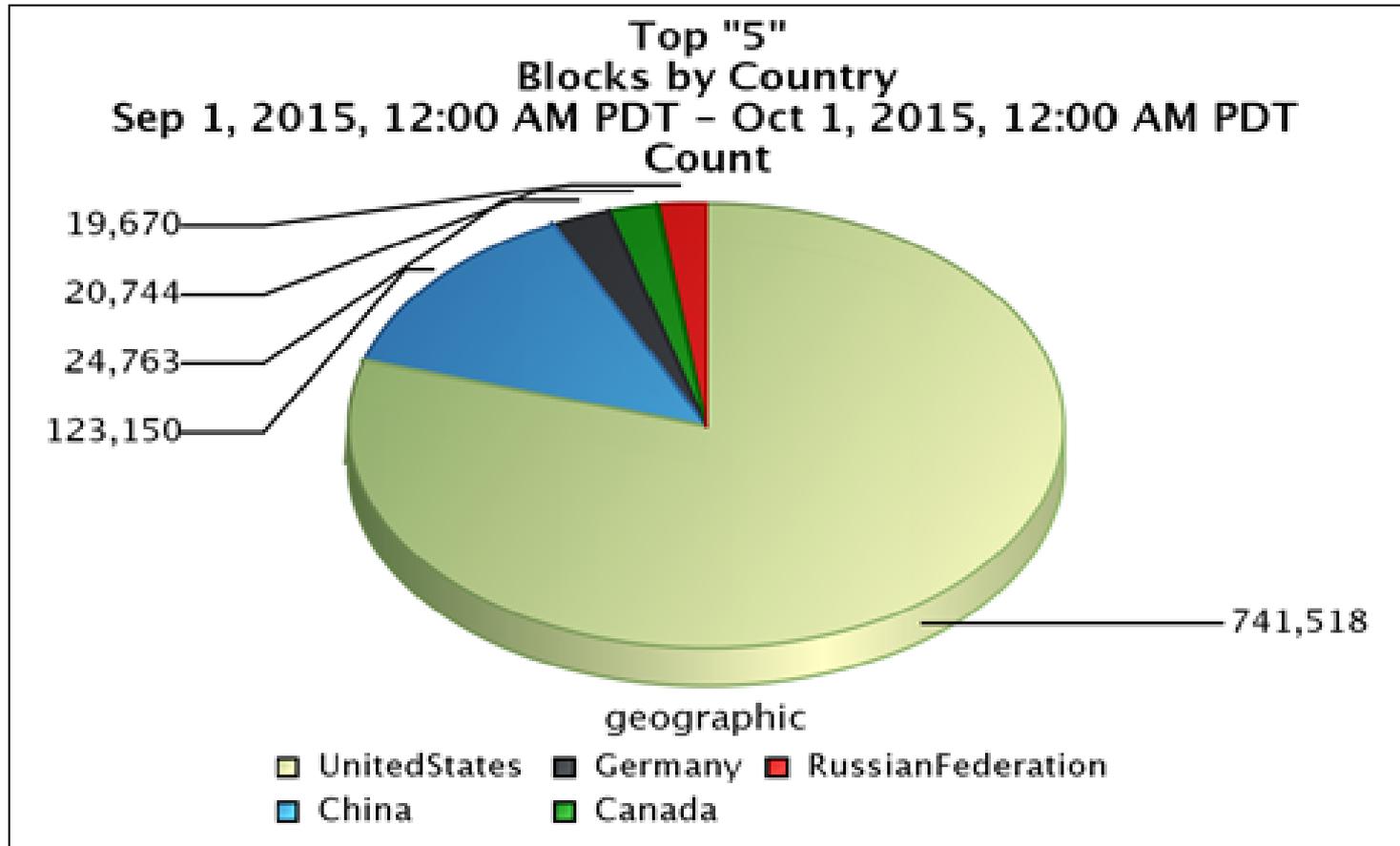
*Dec. 23, 2015*

By Michael Assante – SANS ICS Director

- Planning
  - Malware installed – blinded dispatchers
  - Denial of service to phone system – blocked customer calls
  - VPN in – undesirable state changes to distribution
  - Wiped SCADA servers – to delay restoration
- Coordination – multiple utilities attacked
- Malware used – definite cyber attack
- Direct remote access



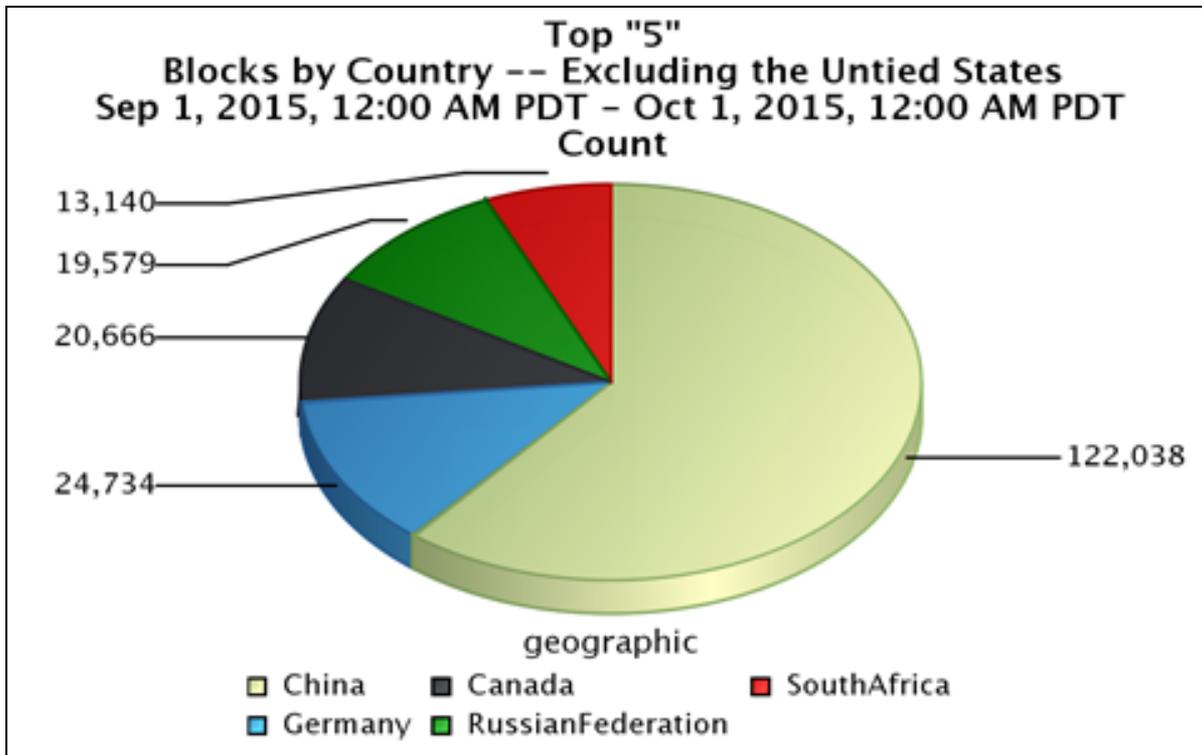
# What WAPA sees monthly: Including hits from within U.S.



# Removing the U.S. hits

## Other Hits

South-Korea	10,708
United Kingdom	10,522
Japan	10,486
Vietnam	8,197
Netherlands	7,013
Ireland	6,371
France	5,370
India	5,014
Poland	4,275
Kuwait	3,897
Ecuador	3,733
Mexico	3,553
Brazil	3,363
Italy	2,866
Ukraine	2,803



# Physical and cyber attacks

- “With the increased convergence of cyber and physical worlds, attacks are no longer limited to office computers and networks. They can now have physical impact in the real world.”

-Steve Durbin, Managing Director, Information Security Forum

- WAPA
  - 37 physical attacks in 2014
    - ✓ Thefts
    - ✓ Reconnaissance
  - 650% increase in cyber incidents 2012-2014



# Insider threat



- Angry, frustrated, resentful employees
- Overly helpful office person
- Not the sharpest crayon in the box.....
- IT staff that is too busy



# Cyber attacks

## **Power Grid USA Today article:** *March 2015*

- Physical and cyber attacks occur 1 in 4 days
- 362+ attacks since 2011
- Small and large utilities attacked
- Cited only 14 cyber attacks



# A year of key cyber attacks: 2014

## January: A public utility control system hacked

- Internet facing
- Weak password/brute force susceptible



## April: Heartbleed

- Half a million (17%) of internet's secure web servers believed attack vulnerable
- Allow theft
  - Servers' private keys
  - User session cookies and passwords
- **WAPA:**
  - 67 vulnerabilities identified and corrected



# 2014 cyber attacks, vulnerabilities

- **May:** Five Chinese nationals indicted
  - Computer hacking and economic espionage
  - Targets included Westinghouse Electric



Sun  
Kailiang



Huang  
Zhenyu



Wen  
Xinyu

- **June:** HAVEX Trojan—
  - ICS focused
  - Multi vector
    - Phishing e-mails
    - Redirects to compromised web sites
    - Watering hole through Trojanized update installers – 3 vendors
  - Allowed access to networks, maps servers



# 2014 cyber attacks/vulnerabilities

## **June:** Ugly Gorilla hack of Northeastern U.S. Utility

- Exposes cyberwar threat by China
- Stole schematics of pipelines
- Copied security guard patrol memos
- Cruised networks, viewed keystrokes
  - Potential to cut off a city's heat, explode a pipeline

## **September:**

1. Chinese Government hackers' intrusion of Televent
2. Shellshock/Bashdoor
  - Internet facing
  - Attacker can gain control over system
  - Vulnerability scanning
  - Millions of unpatched servers at risk



# 2014 cyber attacks, vulnerabilities

## **October:** Black Energy

- Converted crimeware tool
- Cloud-based ICS systems at risk
- Can brick systems it infects and skillfully hide from security analysts



## **December:** Sony hacked by North Korea

- On U.S. soil!
- Destructive malware deployed
- Stole employee Personally Identifiable Information
- Stole proprietary information
- FBI called within hours



# Ransomware fed agencies attacked

*March 2016*

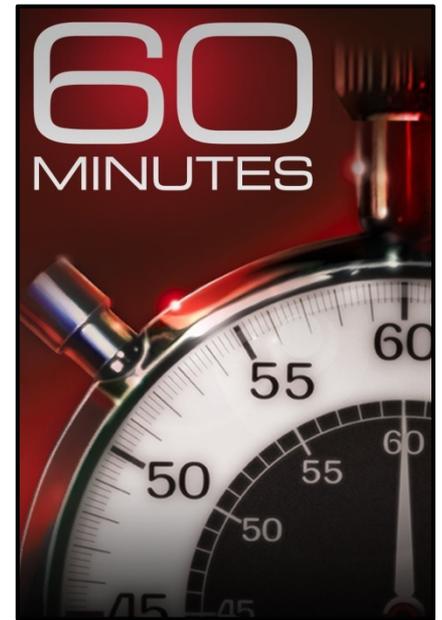
- Reported March 30 by Nextgov
- 321 total agencies attacked
- Phishing attack vector
- Sever the connection with the network
- Shared drives impacted
- Restore to a state prior to the email receipt



# 60 Minutes

*Nov. 30, 2014*

- “97% of all companies are getting breached”
  - Fire Eye CEO, Dave DeWalt
- Hundreds of thousands each week
- 229 days on average from breach to discovery
- 80% of access is through stolen/weak passwords
- Cited Target hack
  - Stole username and password from vendor
  - Installed malware to steal credit card info



# ICS vulnerabilities

- Study by Positive Research Center, Oct. 2015
- 146,136 ICS components web accessible
- Found 691 vulnerabilities in ICS components
  - 58% high severity
  - 39% medium severity
- By vendor:
  - Siemens – 124
  - Schneider Electric – 96
  - Advantech – 51
  - GE – 31



# Information sharing is critical!

- Secure, confidential, rapid
- Actionable
- Indemnify
- Cyber happens in milliseconds and is not regional



# WAPA response



- Measured response – fiscally responsible
- Implementation of multi-factor authentication costs:
  - Western Area Power Administration \$265,000
  - DOE Office of the Chief Information Officer \$1,191,692
  - Los Alamos National Lab \$777,360
  - Kansas City Plant \$705,800
  - Sandia National Laboratories \$1,826,682
  - Thomas Jefferson National Accelerator Facility \$650,700



# WAPA response

- Critical Infrastructure Protections v5 – 40,000 hours plus investment
- Network Access Control
- Secure Enclave Support Center– substations
  - Avoid spending \$6.5 million over 5 years – WAPA-wide solution
- 11 required presidential directives
  - Multi-factor authentication for administrative and standard accounts
  - Anti-phishing campaign



# WAPA response

- 2016 – full inventory of field equipment and supporting technology
  - Every region, all substations
  - Will develop a plan to replace technology
- Supply chain is crucial
  - Vendor user groups
  - Industry influence on vendor development
- Cyber security training – IT professionals
- Patching and upgrades **MUST** stay current



# WAPA response



- Industry sharing
  - WAPA Industry-Sharing Pilot
- DOE support
  - CRISP/CPM monitoring
    - Free to WAPA
  - Negotiated licenses
    - Microsoft cost reduced by nearly 90%
    - DOE-wide security tools – purchased by DOE HQ CIO
  - Integrated Joint Cyber Communications Center



# Major cyber security expenses

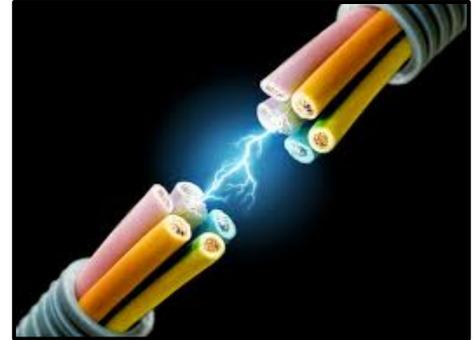
*by fiscal year*

- FY 11 program costs: \$130,000
- FY 12 NSOC implementation: \$365,791
- FY 13 NSOC maintenance: \$314,095
- FY 14
  - NSOC maintenance: \$486,012
  - Encase: \$113,746
- FY 15
  - SESC implementation: \$1,800,000
  - NSOC maintenance: \$511,543
  - Forward anti-phishing and training: \$30,000/year

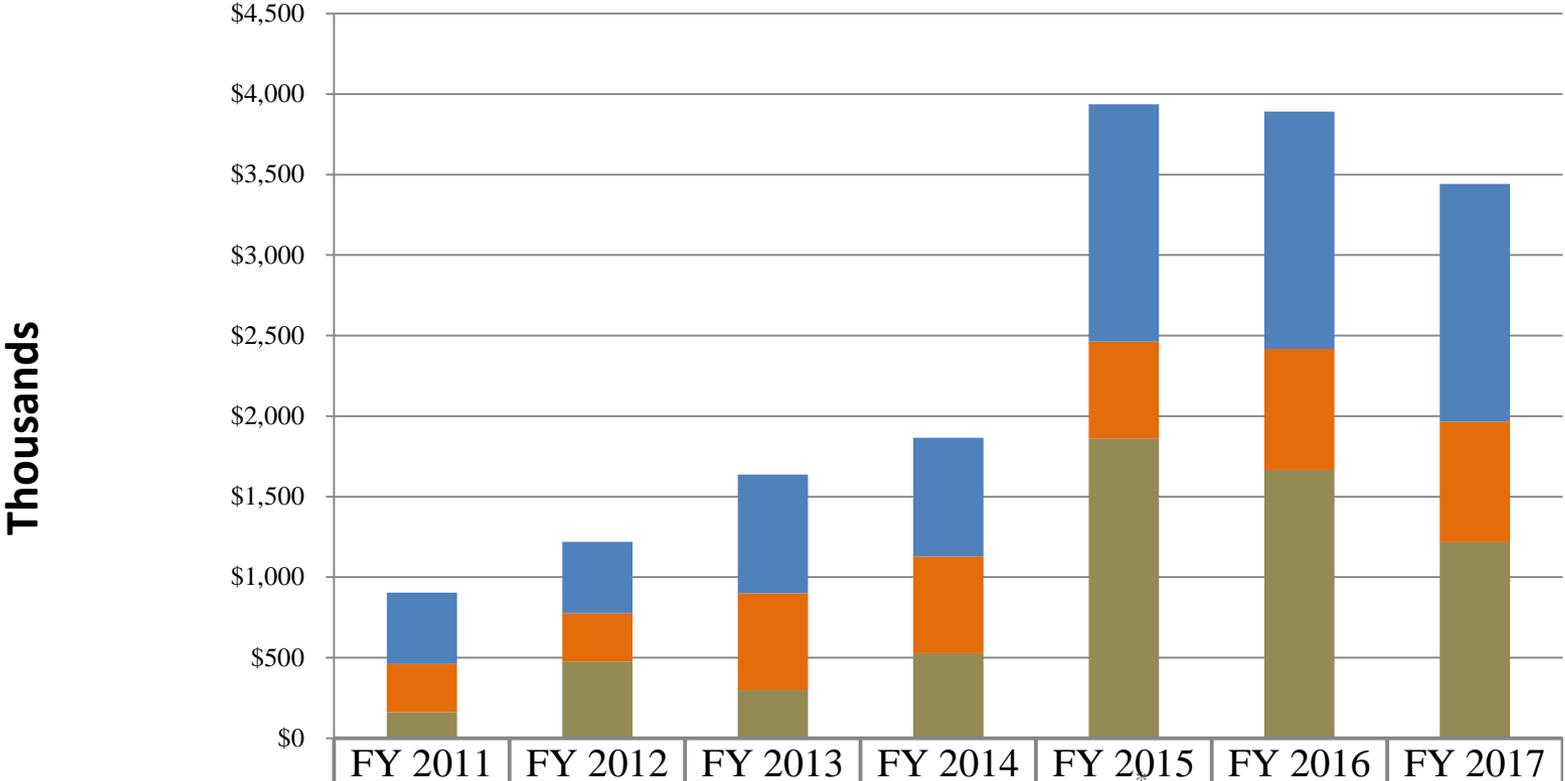


# Major cyber security expenses

- FY 16
  - SESC/NSOC maintenance: \$552,640
  - Data leakage prevention: \$470,000
  - NAC: \$350,000 (could be FY 17)
- FY 17
  - NSOC life cycle refresh: \$500,000
  - SESC maintenance: \$275,000
  - Begin replacement of old field equipment: \$ unknown
  - Sandbox environment: \$ unknown
- FY 18 NSOC/SESC maintenance: \$560,000

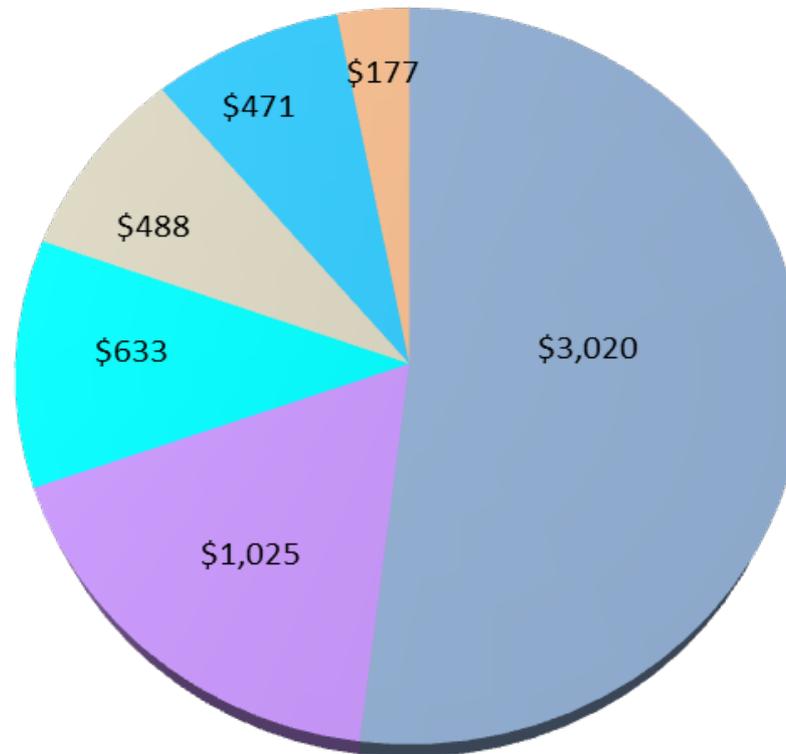


# Cyber security cost drivers



# IT cost savings/avoidance

**FY 2015 Total Savings \$5.8M**



■ Purchase Consolidation

■ Travel for Training

■ Personnel

■ Hardware

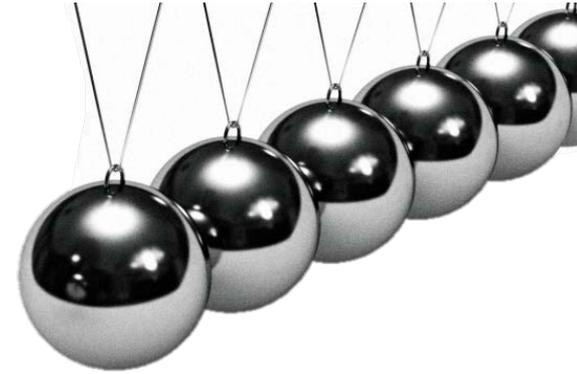
■ Systems

■ Processes/Work Efficiencies



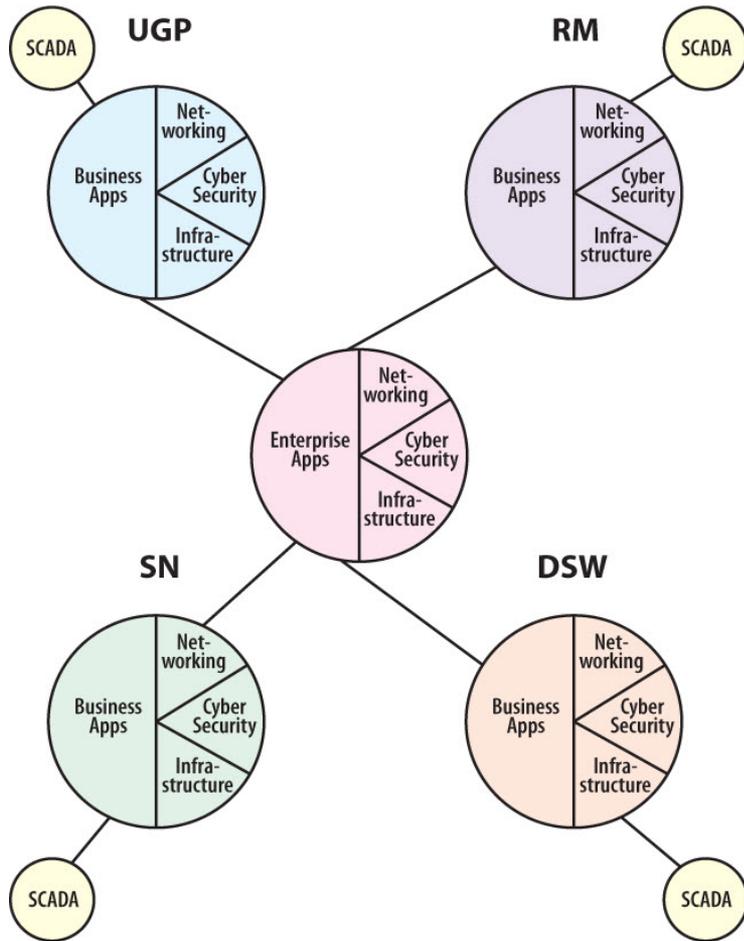
# Projects delayed

- 205 projects requested initially for 2016
- 32 are legally mandatory
- Key projects delayed:
  - Improved network segmentation (security)
  - Improved Network Access Control (security)
  - Expansion of network for IP meters
  - Replace SONET infrastructure – past end of life
  - Provide IP management for IP radios (security)
  - Upgrade VTC (cost savings)
  - Network lifecycle replacements
  - Plus 100 others



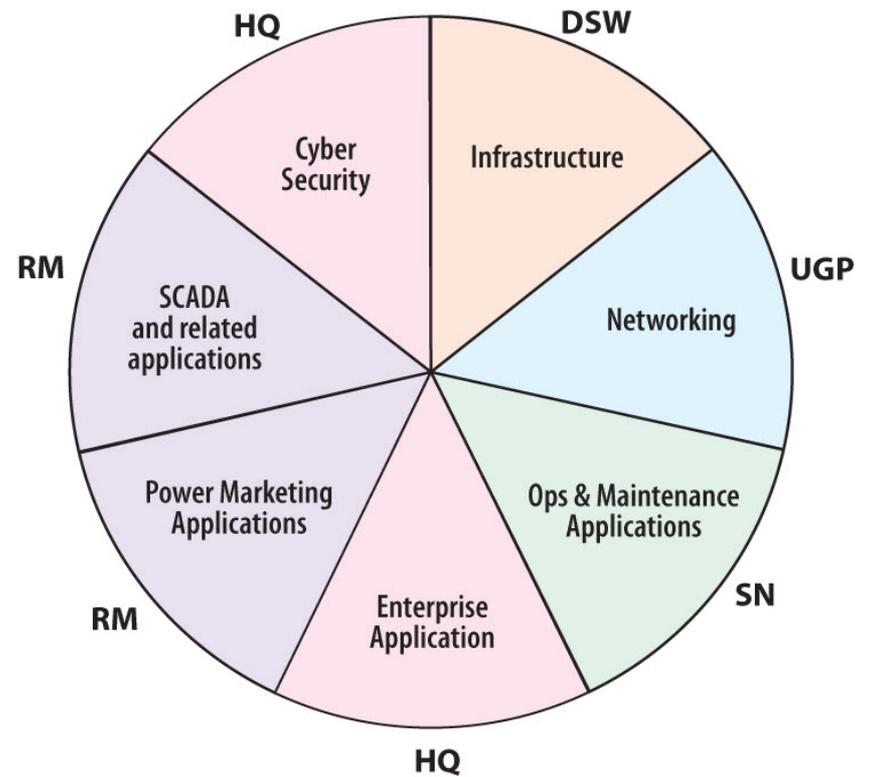
# IT Evolution

IT 5 years ago



IT Today

Western wide

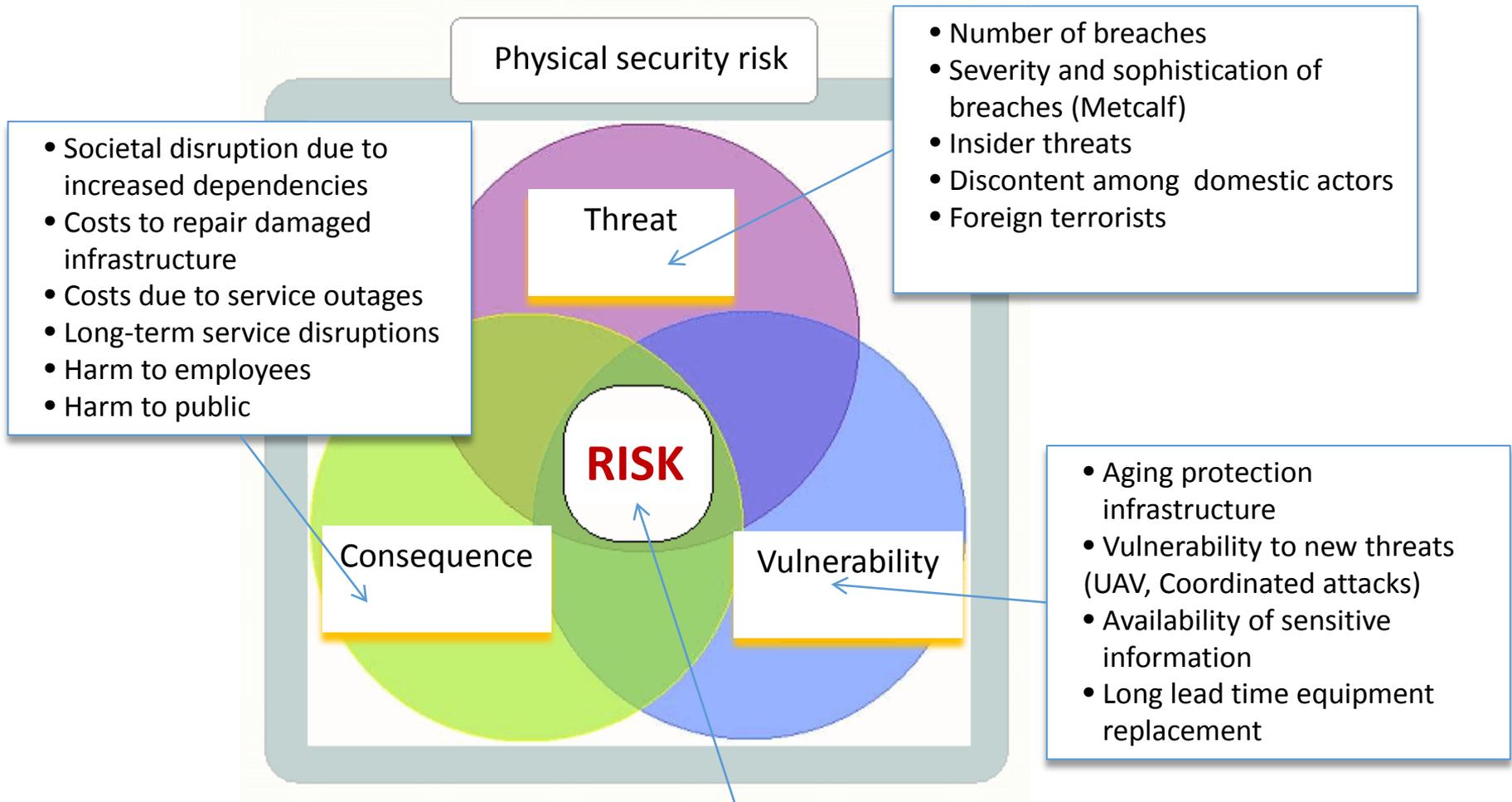


# Physical Security

Anthony Montoya | Executive VP and COO



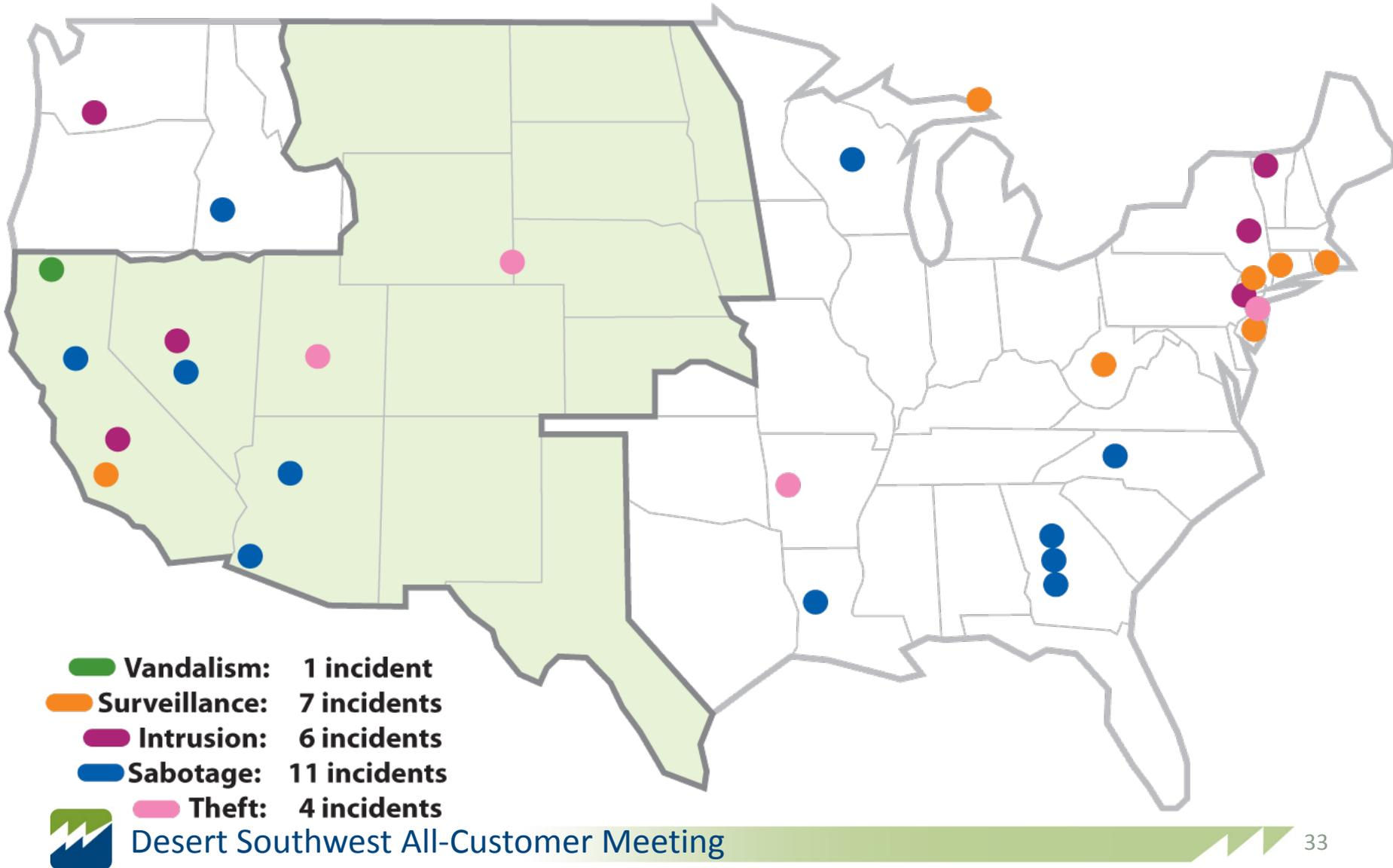
# Managing physical security risk



Risk due to malicious actor is **INCREASING!**



# National breaches



# Inspector general audits

- 2003
  - Risk assessments inadequate
- 2010
  - Incomplete required risk assessments, security measure performance testing, and implementation of recommended security enhancements
    - ✓ 2013
      - Formalized Office of Security and Emergency Management
      - Consolidated WAPA's security programs
    - ✓ 2014
      - Updated Risk Management process
      - Developed All-Hazard Risk Assessment
- 2016
  - Progress noted
  - New recommendations; regions working through lists



# WAPA's response

- Agile process and culture of compliance
- Making strides in all areas
- Consistent high marks in NERC, WECC, MRO
- Fundamental security commitment



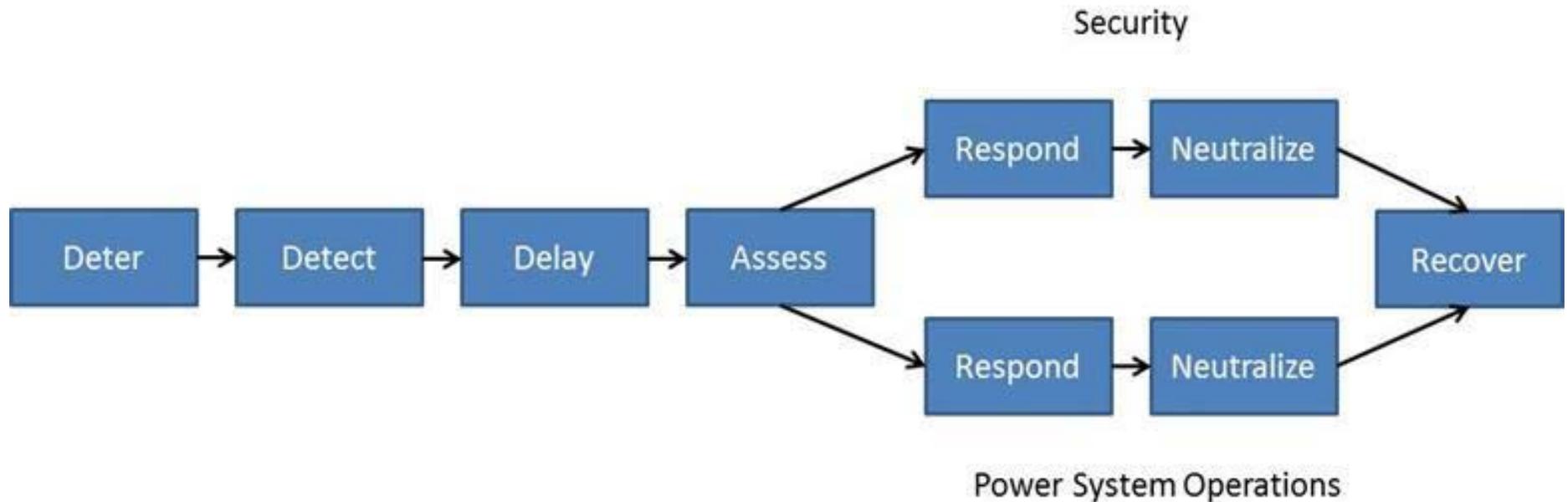
# Risk assessments

- NERC CIP 14 – risk to bulk electric system
  - WAPA CIP 14 sites
  - Reassess every 2.5 years
- Current status
  - Have met NERC Compliance requirements
  - Validation of study work complete
  - Development and verification of mitigation plans complete
  - Average estimated mitigation cost estimate per site \$677K
    - ✓ Highest site - \$2.161M (located in UGP)
    - ✓ Lowest site - \$64K (located in SN)
- Non-CIP 14 sites (330+)
  - Baseline assessments underway and to be completed by 2019
  - Reassess every five years



# Risk assessments

## Basic Approach to Physical Security



# Risk assessments

Facility Security Level = FSL

- FSL = categorization based on analysis of several security-related facility factors
  - Factors serve as basis for identification of baseline standards
    - ✓ Facility population
    - ✓ Facility size
    - ✓ Mission criticality
    - ✓ Symbolism
    - ✓ Threat to tenant agencies



# Risk assessments

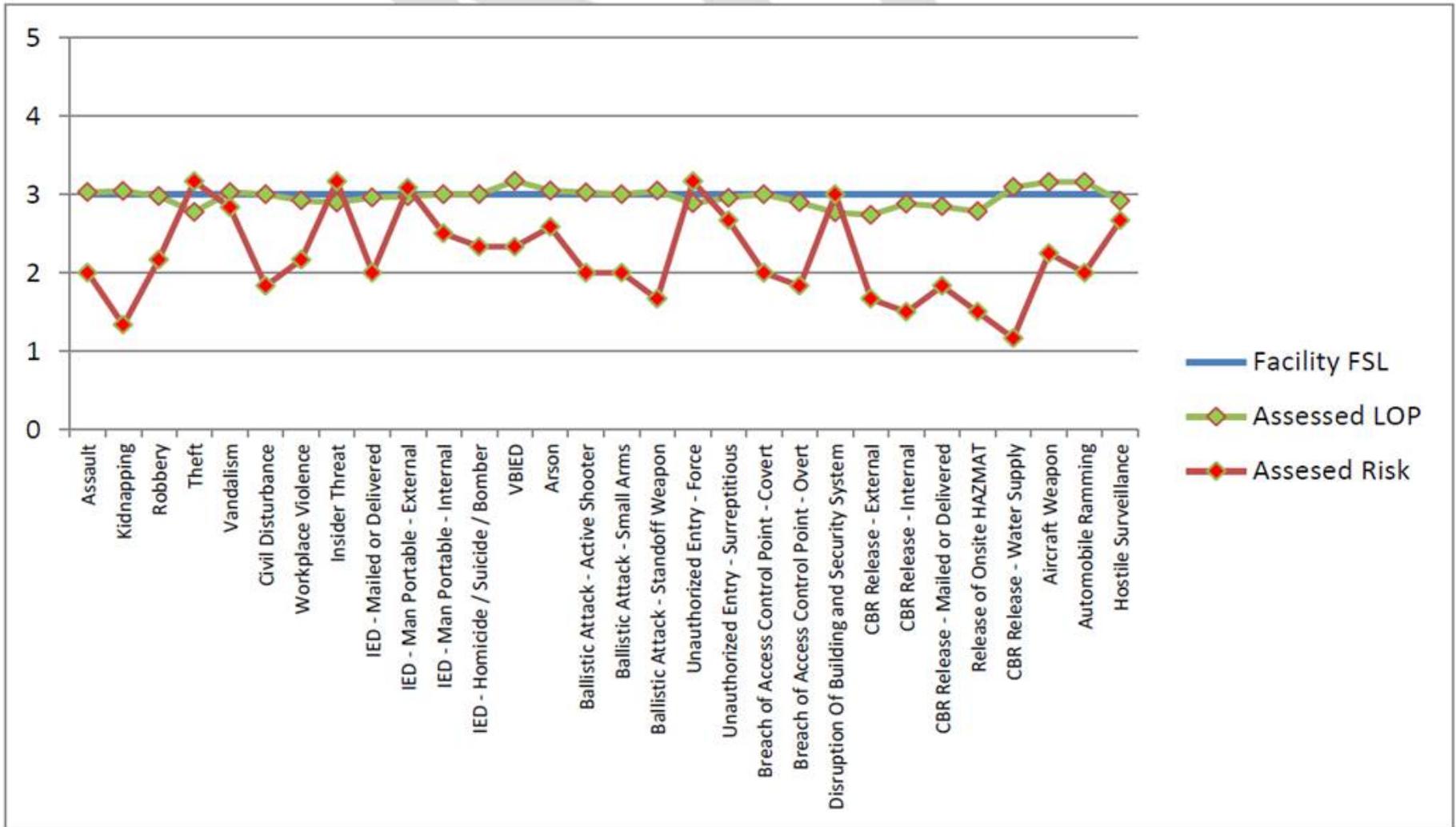


Figure 9.2 - Levels of Protection and Risk Graph



# Baseline physical security criteria

- Primarily for new constructions
- Incorporate industry standards and best practices
- Countermeasure selection is risk-based and customized for local conditions (threat, etc.)

Western Security Criteria					
Criterion	Level 1 - Minimum*	Level 2 - Low	Level 3 - Medium	Level 4 - High	CIP-014 - Very High*
Perimeter Fence	Security chain link fence 7-ft tall, 1 inch mesh, 9-gauge nominal wire diameter after coating (ASTM A 392).	Security chain link fence 7-ft tall, 1 inch mesh, 9-gauge nominal wire diameter after coating (ASTM A 392).	Security chain link fence 7-ft tall, 1 inch mesh, 9-gauge nominal wire diameter after coating (ASTM A 392).	Anti cut/anti climb fence 10 f-ft tall (height can be adjusted to 7 ft if there are safety issues with lines)	Anti cut/anti climb fence 10 f-ft tall (height can be adjusted to 7 ft if there are safety issues with lines)
Barbed Tape/concerntina	at top of fence, can be used at the bottom for fenceline	at top of fence, can be used at the bottom for fenceline	at top of fence, can be used at the bottom for fenceline	at top of fence, can be used at the bottom for fenceline	at top of fence, can be used at the bottom for fenceline
Exterior Openings < 96 sq. in.	prevent unauthorized access (i.e. grills, rebar or locks)	prevent unauthorized access (i.e. grills, rebar or locks)	prevent unauthorized access (i.e. grills, rebar or locks)	prevent unauthorized access (i.e. grills, rebar or locks)	prevent unauthorized access (i.e. grills, rebar or locks)
	Drainage ditches, culverts, vents ducts, and other openings that pass through the perimeter fence	Drainage ditches, culverts, vents ducts, and other openings that pass through the perimeter fence	Drainage ditches, culverts, vents ducts, and other openings that pass through the perimeter fence	Drainage ditches, culverts, vents ducts, and other openings that pass through the perimeter fence	Drainage ditches, culverts, vents ducts, and other openings that pass through the perimeter fence



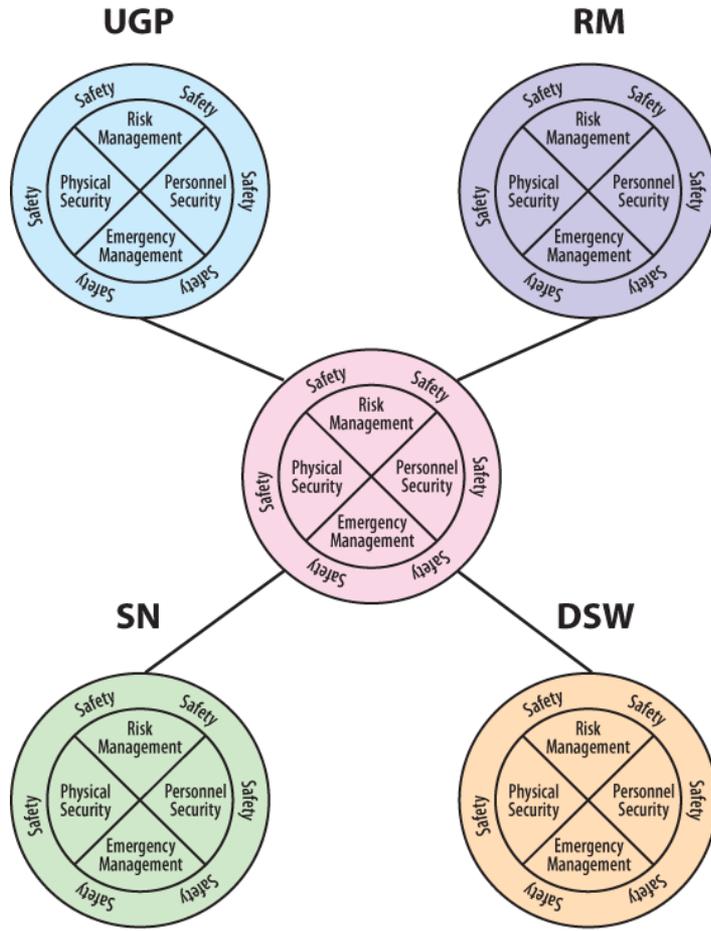
# Performance testing

- Performance Assurance Plan draft completed
- Contractor engaged through DOE to conduct testing
  - Protection Strategies Incorporated
- Verification of contractor methodology and scoring scheduled late August at Mead Sub
- New systems are tested prior to acceptance
- Will include intrusion testing at critical sites



# WAPA-wide Security Evolution

## Security 3 years ago

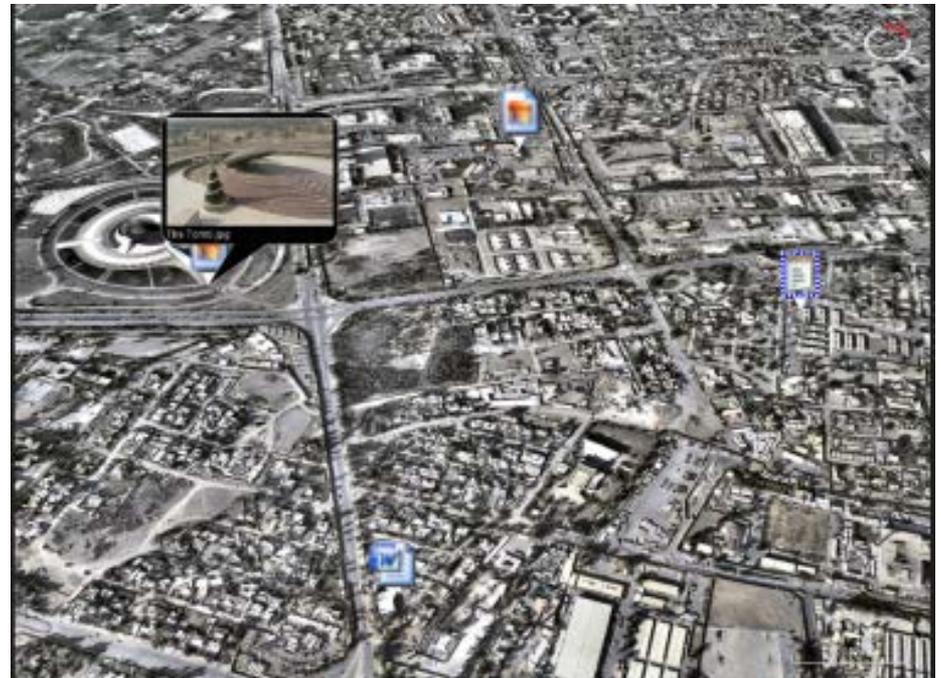
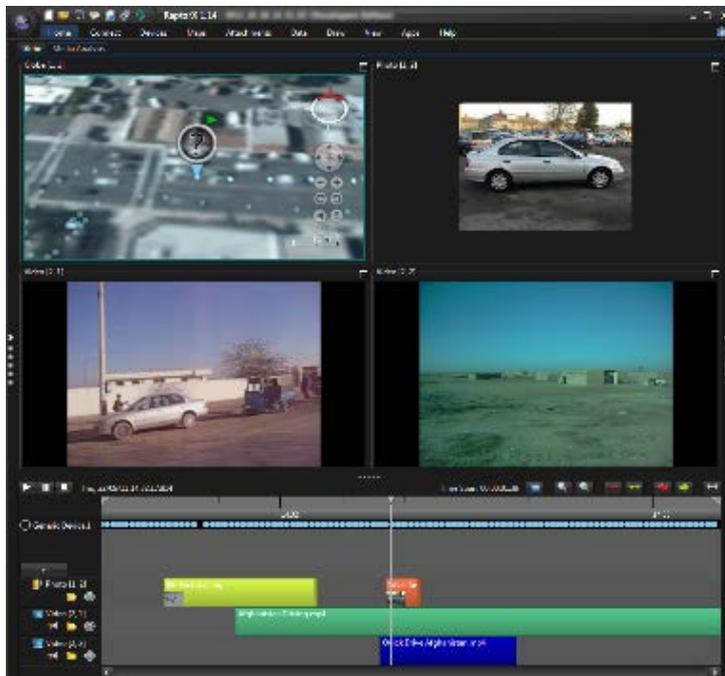


## Security Today



# Raptor X

- Flexible platform for intelligence collection, monitoring, and analysis
- Geo-data interfaced



# Raptor- X

- Developed by Department of Energy STL
- Pilot in an electric utility environment at SN



# Human Capital

Anthony Montoya | Executive VP and COO

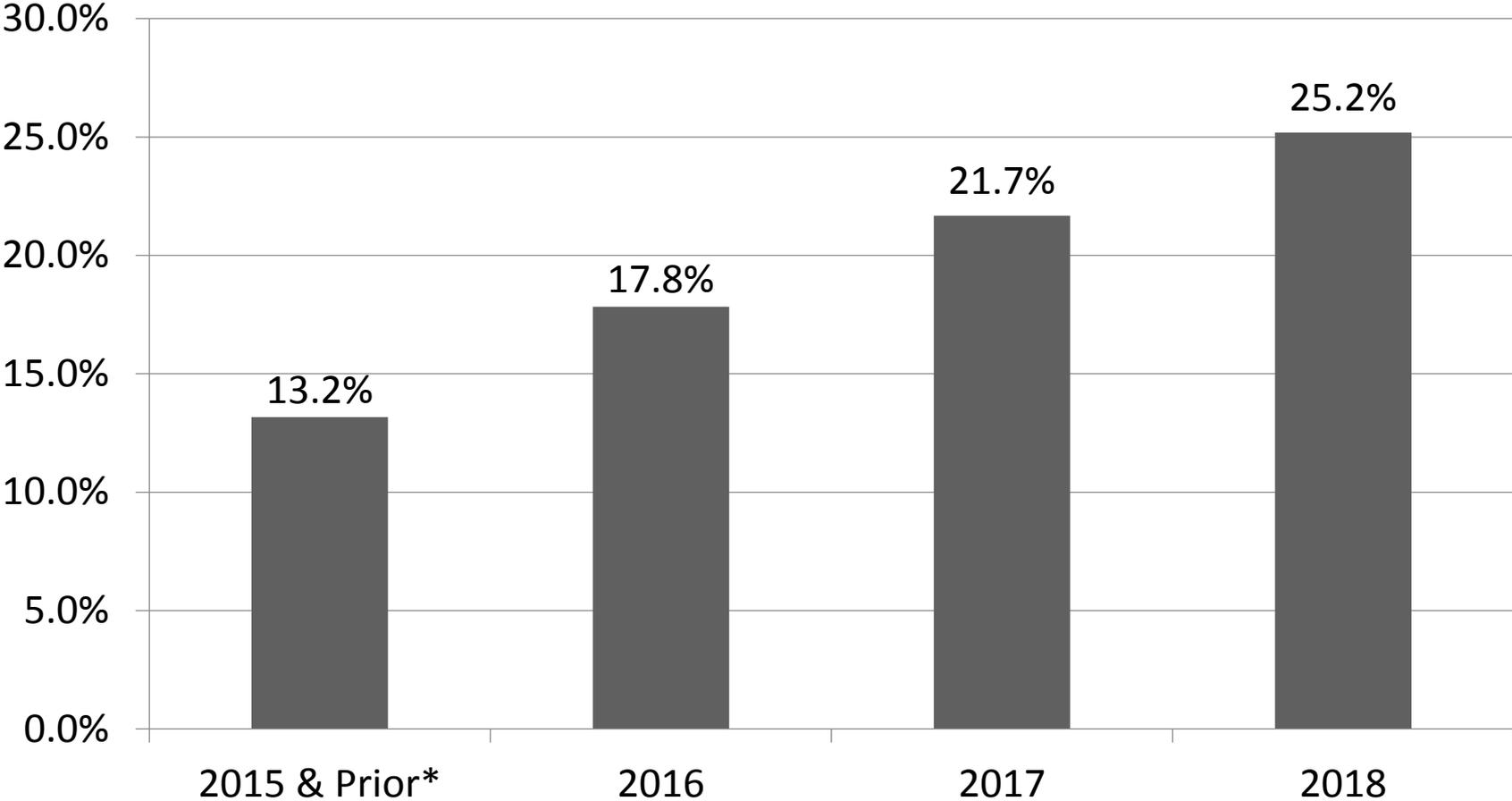


# Human capital SWOT analysis

	Enablers	Challenges
I n t e r n a l	Strengths	Weaknesses
	<ul style="list-style-type: none"> <li>• Industry leading technical experts</li> <li>• WAPA institutional knowledge</li> <li>• Passion and commitment to WAPA's mission and customers</li> </ul>	<ul style="list-style-type: none"> <li>• Aging workforce – mission critical positions</li> <li>• Retirement eligibility growing rapidly</li> <li>• Managerial development</li> </ul>
E x t e r n a l	Opportunities	Threats
	<ul style="list-style-type: none"> <li>• Strengthen workforce planning and management</li> <li>• Improve leadership development</li> <li>• Improve knowledge management</li> </ul>	<ul style="list-style-type: none"> <li>• Extensive competition for engineers, IT specialists, and experienced senior managers</li> <li>• Younger workforce mobility</li> </ul>



# Retirement eligible projections



# Engineering special pay rate initiative

- Joint study with other PMAs
- Aimed at mitigating risks such as:
  - PMAs compensate new graduates 11% - 19% lower than industry
  - PMAs compensate existing engineers 6% - 67% lower than industry
  - 46% of industry engineers estimate to retire within the next 5 – 10 years
- DOE has concurred with initiative
- Currently being reviewed by OPM
- Annual (FY 17-20) impact = \$4.3M - \$4.7M



# Other potential salary impacts

- Determined outside of WAPA
  - General schedule salary adjustments
  - Locality pay adjustments
- Determined by WAPA
  - Wage board salary adjustments
  - Administratively Determined salary adjustments

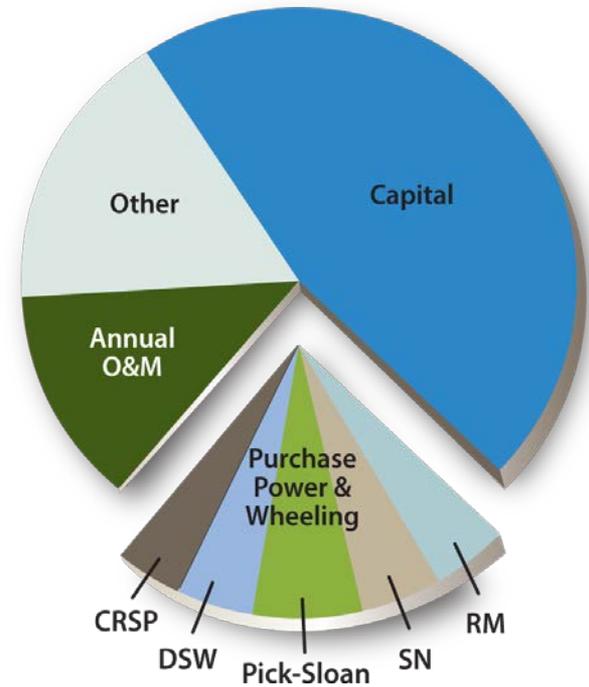
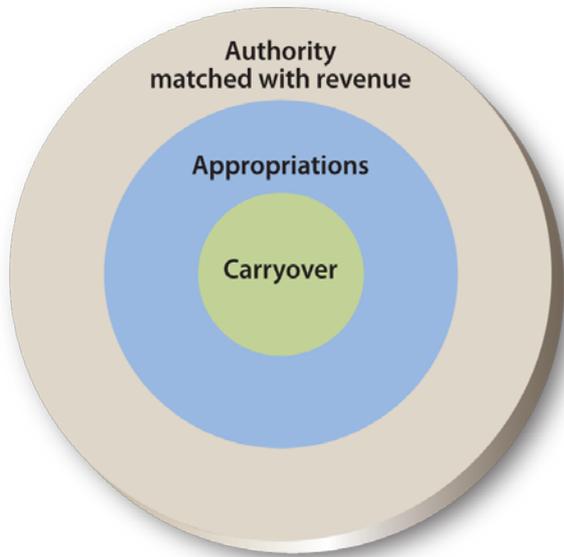


# Sustainable Funding

Linda Kimberling | Senior VP and CFO



# Where we are now: funding



# How we get unobligated balances

- Difference between amounts budgeted and executed
- Some illustrative examples:
  - Mitigate risk such as PP&W
  - Construction project delays in execution years
  - Employee pay raises budgeted but not enacted
  - Revenue exceeds power repayment study estimate:
    - Better than average water year
    - Selling power high to cover contract commitment purchases later in the day



# Unobligated balances strategy

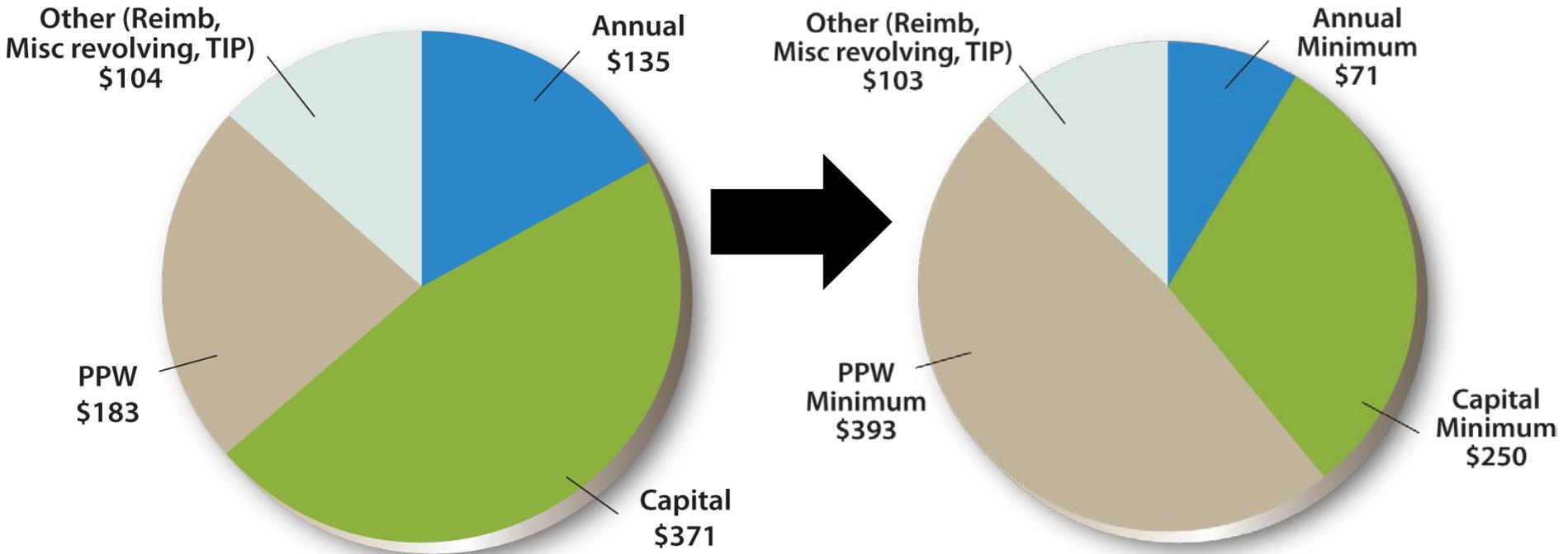
- Sustainable funding tool in support of WAPA's mission
  - Sound fiscal management
  - Continue operations during emergency situations
  - Mitigates risk during continuing resolutions or lapses in appropriations
- GAO Audit: Committed to Congress to finalize and implement unobligated balances strategy



# Moving strategy forward

FYE 15 Unobligated Balance  
By purpose: \$793 (in Millions)

Estimated Unobligated Balance  
By purpose: \$817 (in Millions)



# Discussion and Comments

Ron Moulton | Senior VP and DSW Regional Manager



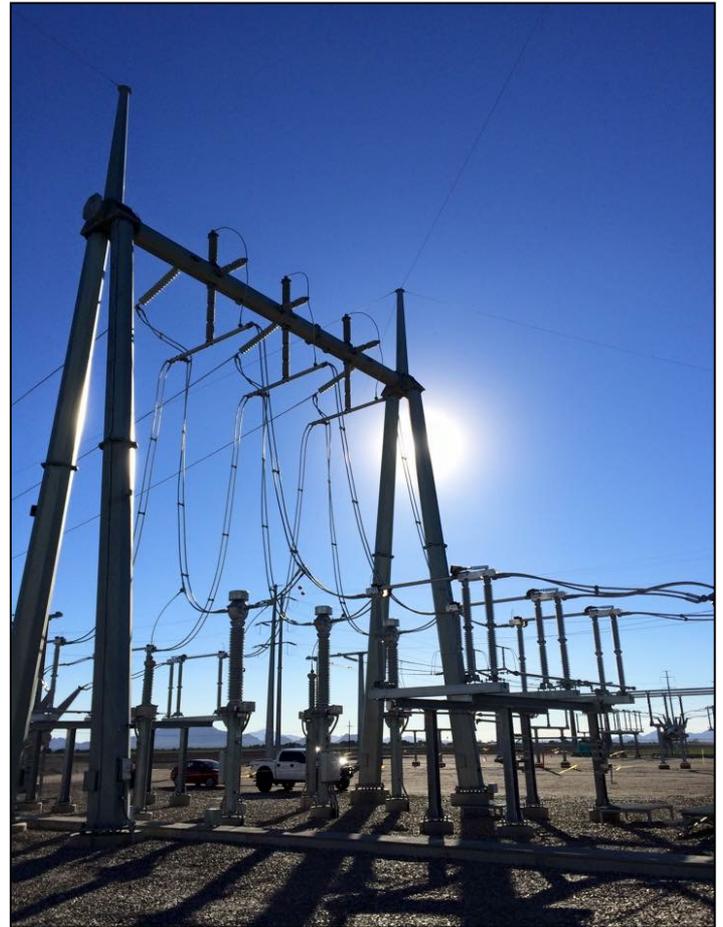
# Committed to transparency

- Lowest possible rates consistent with sound business principles
- Critical to focus on the big issues we are all facing
- Need customer support to meet your changing needs
- Customer engagement is critical
- *The Source:* [www.wapa.gov](http://www.wapa.gov)



# What is next?

- Collecting your thoughts
  - Keeping dialogue open
  - Upcoming customer meetings



# Thank you

