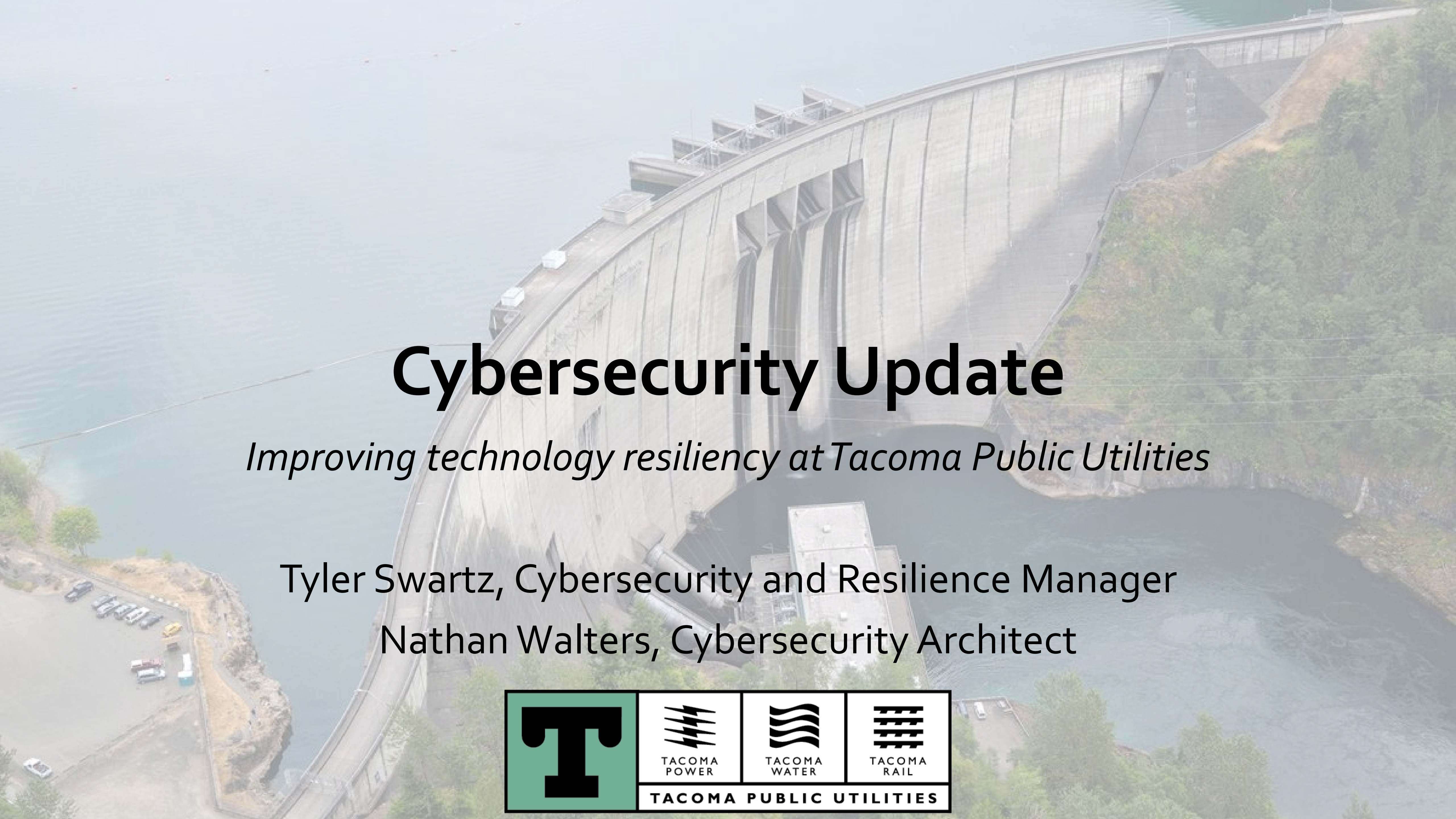


Cybersecurity Update

Improving technology resiliency at Tacoma Public Utilities

Tyler Swartz, Cybersecurity and Resilience Manager

Nathan Walters, Cybersecurity Architect

TACOMA POWER TACOMA WATER TACOMA RAIL

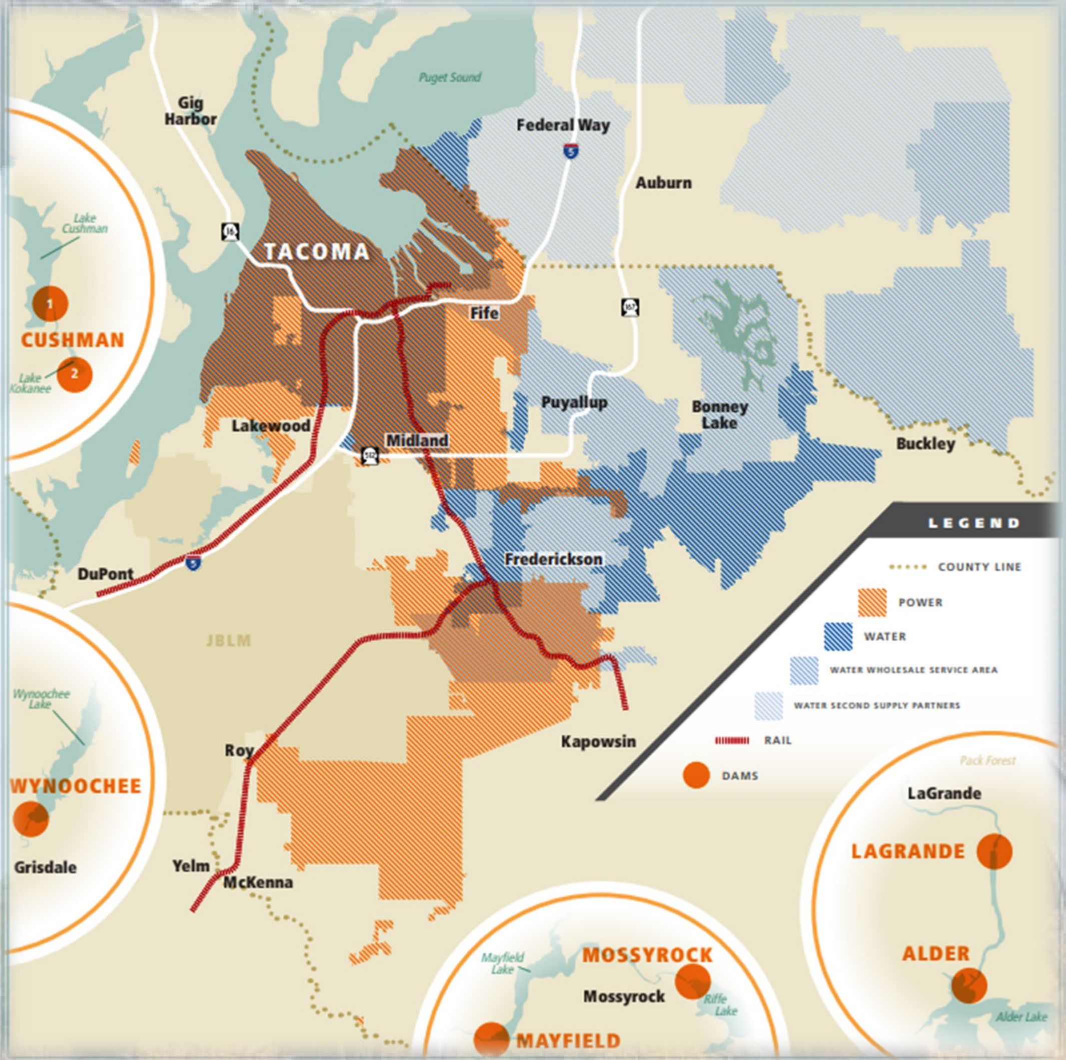
TACOMA PUBLIC UTILITIES

TACOMA POWER | TACOMA WATER | TACOMA RAIL

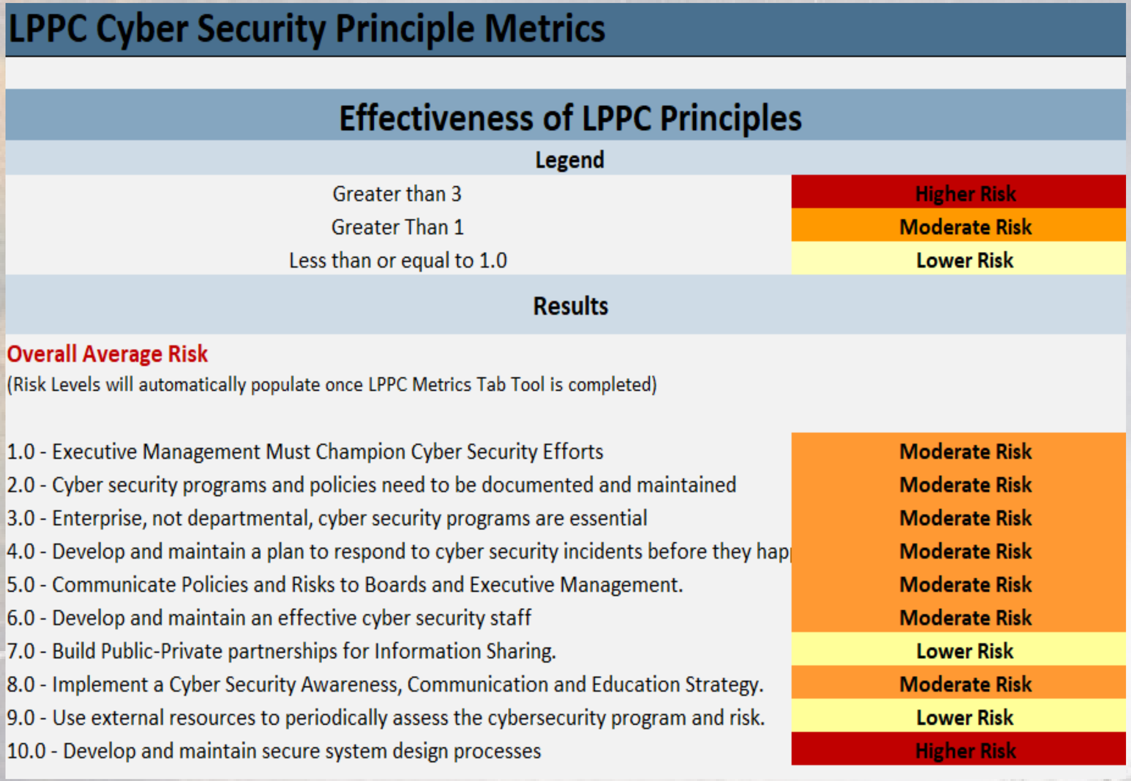
TACOMA PUBLIC UTILITIES

Agenda

- LPPC Maturity Assessment
- Current Threats
- GridEx VI Lessons Learned
- Cybersecurity Roadmap
- Questions



2020



LPPC Cyber Security Principle Metrics

Effectiveness of LPPC Principles

Legend

Greater than 3	Higher Risk
Greater Than 1	Moderate Risk
Less than or equal to 1.0	Lower Risk

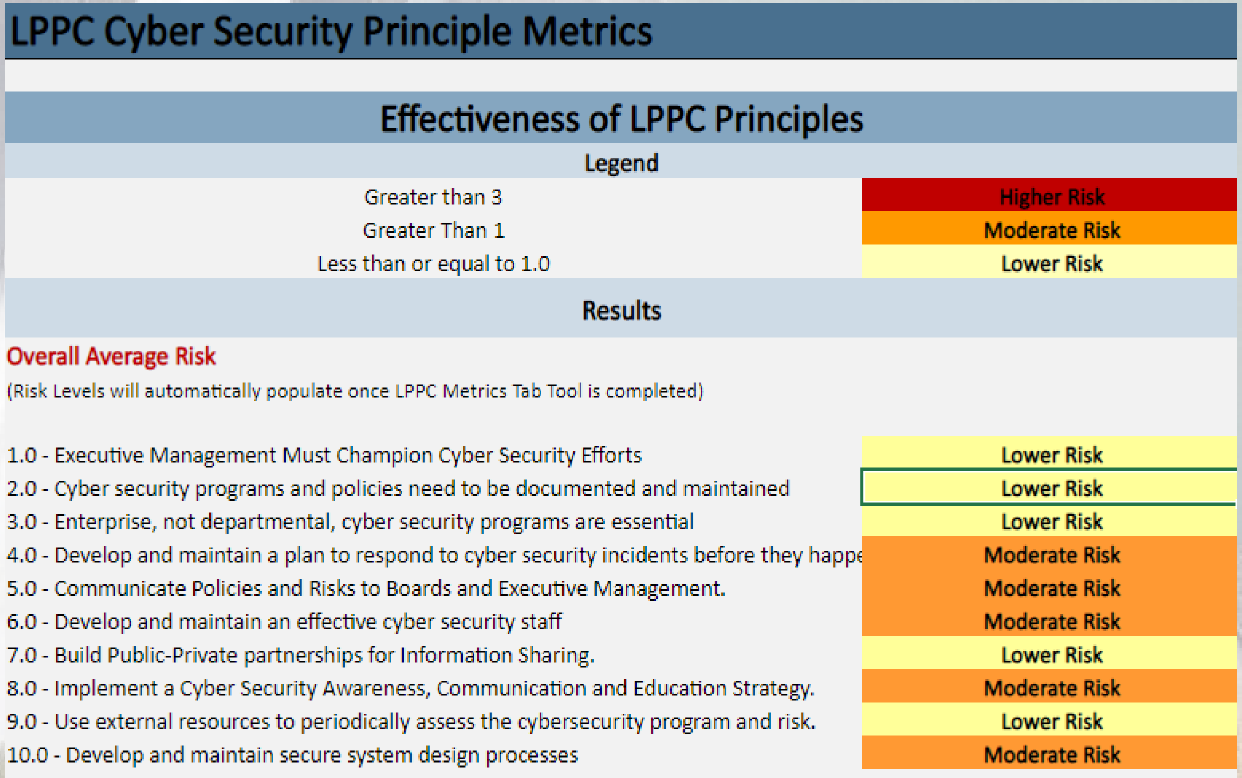
Results

Overall Average Risk

(Risk Levels will automatically populate once LPPC Metrics Tab Tool is completed)

1.0 - Executive Management Must Champion Cyber Security Efforts	Moderate Risk
2.0 - Cyber security programs and policies need to be documented and maintained	Moderate Risk
3.0 - Enterprise, not departmental, cyber security programs are essential	Moderate Risk
4.0 - Develop and maintain a plan to respond to cyber security incidents before they hap	Moderate Risk
5.0 - Communicate Policies and Risks to Boards and Executive Management.	Moderate Risk
6.0 - Develop and maintain an effective cyber security staff	Moderate Risk
7.0 - Build Public-Private partnerships for Information Sharing.	Lower Risk
8.0 - Implement a Cyber Security Awareness, Communication and Education Strategy.	Moderate Risk
9.0 - Use external resources to periodically assess the cybersecurity program and risk.	Lower Risk
10.0 - Develop and maintain secure system design processes	Higher Risk

2021



LPPC Cyber Security Principle Metrics

Effectiveness of LPPC Principles

Legend

Greater than 3	Higher Risk
Greater Than 1	Moderate Risk
Less than or equal to 1.0	Lower Risk

Results

Overall Average Risk

(Risk Levels will automatically populate once LPPC Metrics Tab Tool is completed)

1.0 - Executive Management Must Champion Cyber Security Efforts	Lower Risk
2.0 - Cyber security programs and policies need to be documented and maintained	Lower Risk
3.0 - Enterprise, not departmental, cyber security programs are essential	Lower Risk
4.0 - Develop and maintain a plan to respond to cyber security incidents before they happe	Moderate Risk
5.0 - Communicate Policies and Risks to Boards and Executive Management.	Moderate Risk
6.0 - Develop and maintain an effective cyber security staff	Moderate Risk
7.0 - Build Public-Private partnerships for Information Sharing.	Lower Risk
8.0 - Implement a Cyber Security Awareness, Communication and Education Strategy.	Moderate Risk
9.0 - Use external resources to periodically assess the cybersecurity program and risk.	Lower Risk
10.0 - Develop and maintain secure system design processes	Moderate Risk

Current Threats

- Industroyer2, an evolved malware targeting ICS networks
- Geopolitical instability, domestic and global concerns
- Supply Chain continues to pose an increasing level of risk to both physical and digital assets

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

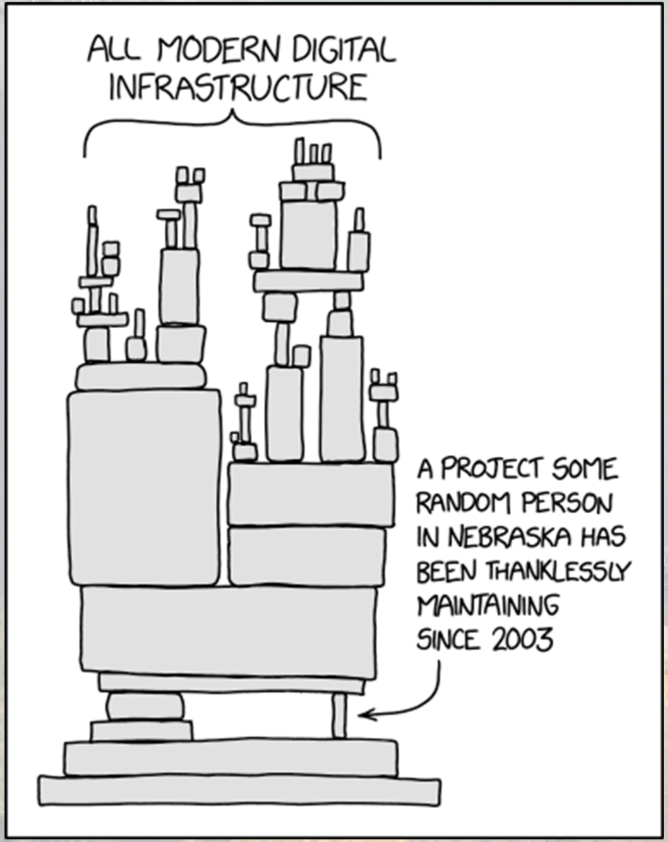
A DIVISION OF NERC

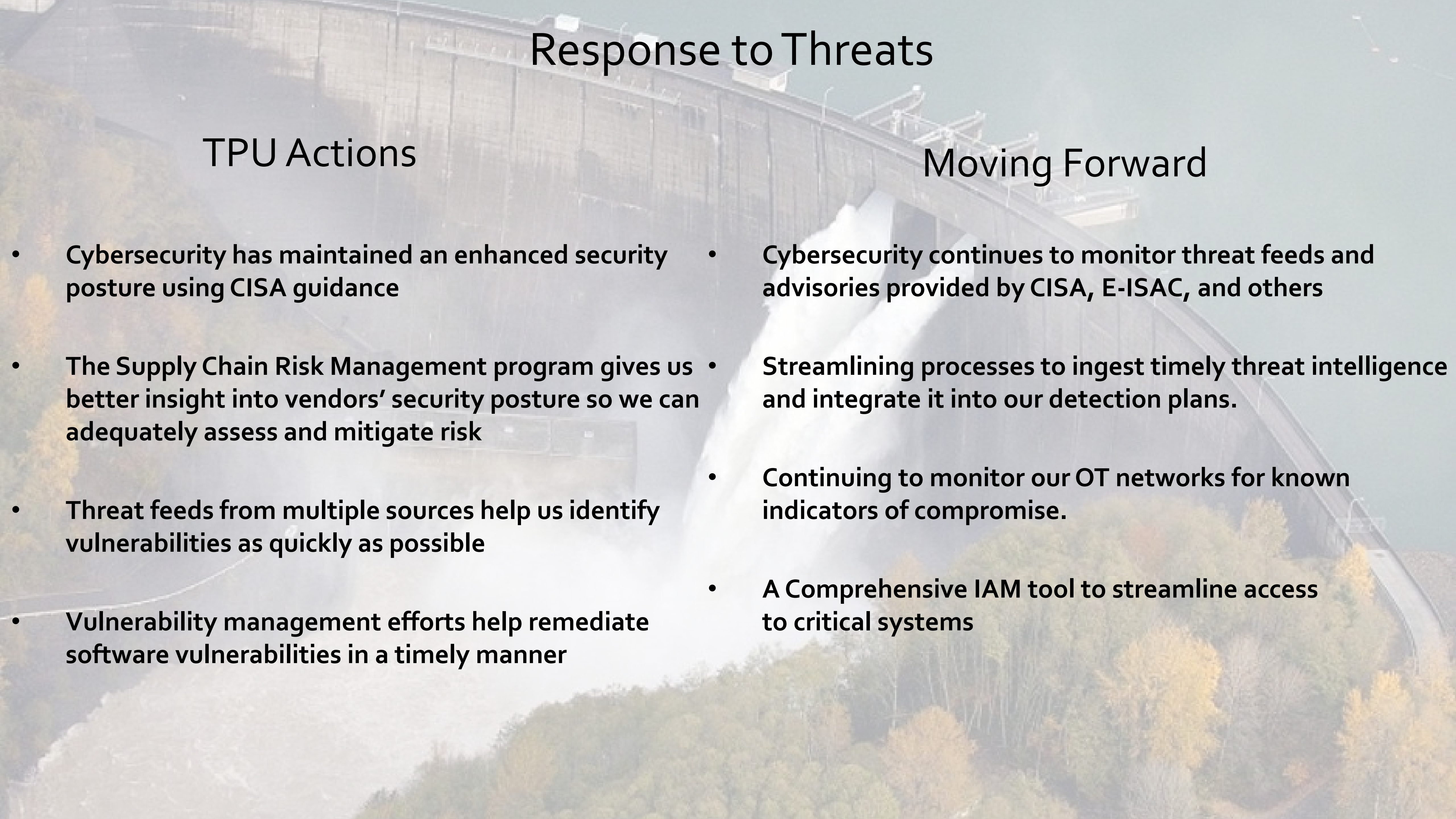
E-ISAC

ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

Supply Chain Risk Management

- A multi-modal organizational threat
- Supply Chain inadequacies present a growing risk to sourcing operational equipment/replacement parts in a timely manner
- Attacks on commonly-used software and their dependencies are an emerging threat vector


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003



Response to Threats

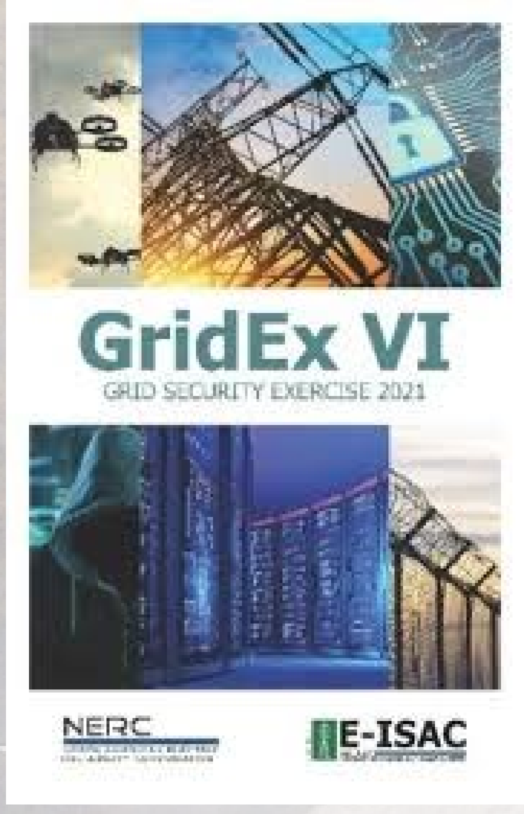
TPU Actions

- Cybersecurity has maintained an enhanced security posture using CISA guidance
- The Supply Chain Risk Management program gives us better insight into vendors' security posture so we can adequately assess and mitigate risk
- Threat feeds from multiple sources help us identify vulnerabilities as quickly as possible
- Vulnerability management efforts help remediate software vulnerabilities in a timely manner

Moving Forward

- Cybersecurity continues to monitor threat feeds and advisories provided by CISA, E-ISAC, and others
- Streamlining processes to ingest timely threat intelligence and integrate it into our detection plans.
- Continuing to monitor our OT networks for known indicators of compromise.
- A Comprehensive IAM tool to streamline access to critical systems

GridEx VI Lessons Learned



Crashoverride – 17DEC16

- Impacted transmission level substation in Ukraine.
- First Modular attack framework for attacking ICS
  -To include ability to be weaponized for DNP3

Dragonfly/HAVEX –

- Espionage effort targeted over 2,000 sites with emphasis on electric and petrochemicals utilizing OPC protocol to map ICS networks for spying.

BLACKENERGY 2 –

- Used by Sandworm APT.
- Tailored malware for HMI applications: Siemens, GE, and Advantech. While gaining foothold access to ICS Networks the HMI's were mostly leveraged for espionage and C2.

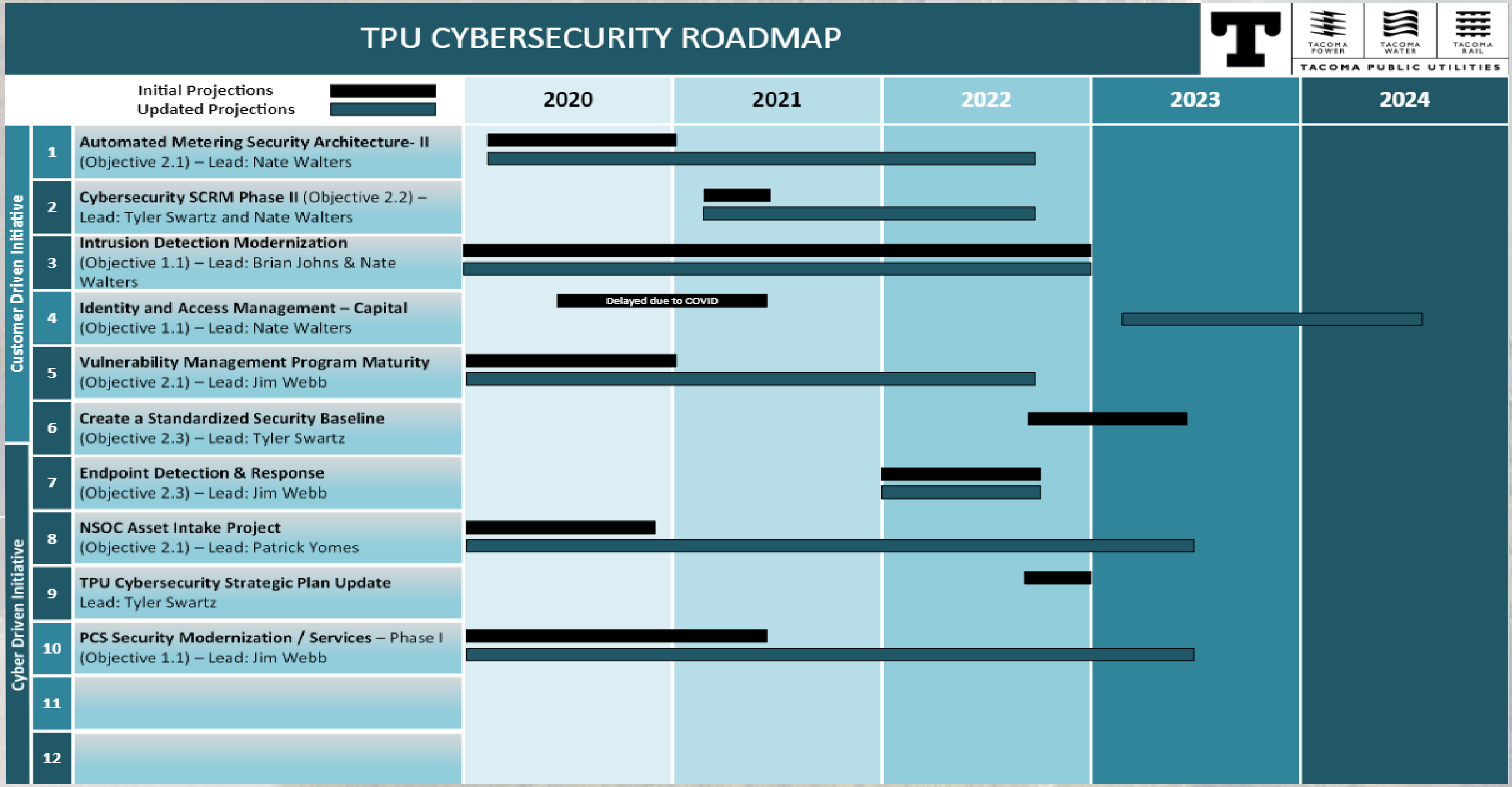
BACKENERGY 3 – 23DEC15

- Sandworm APT.
- Cyber attack on 3 power companies in Ukraine. First of It's kind.
- Over 50 substations disconnected effecting 225,000+ customers in darkness for 6 hours and destruction of serial To Ethernet devices. Impact lasted more than a year in some locations.

Exercise-Exercise

Key Roadmap

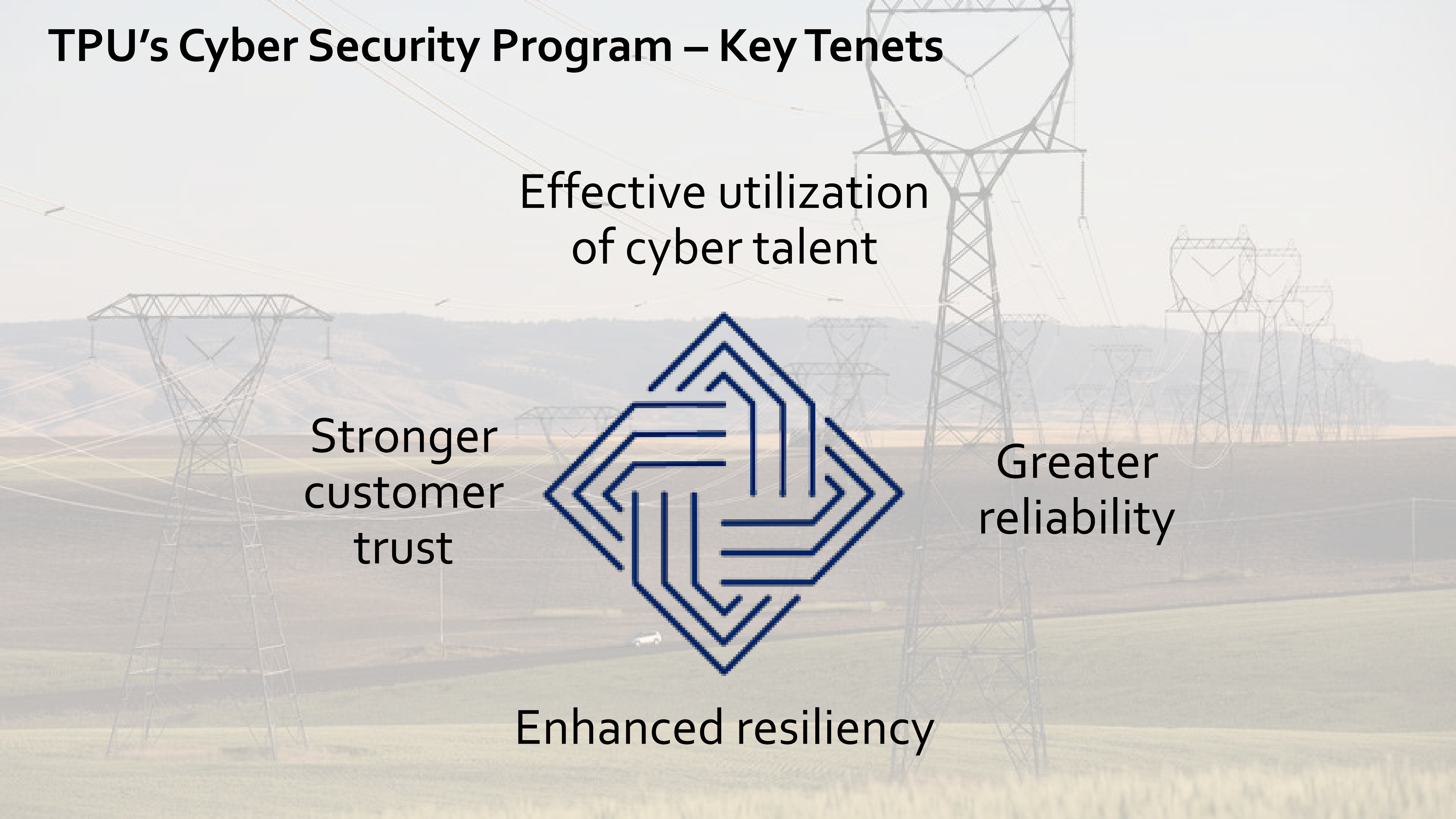
Integrate technology & foster innovation to deliver affordable, flexible, secure, resilient, and sustainable power & water services for our customers



TPU CYBERSECURITY ROADMAP

Initiative	#	Project
Customer Driven Initiative	1	**Automated Metering Security Architecture- II** (Objective 2.1) – Lead: Nate Walters
	2	**Cybersecurity SCRM Phase II** (Objective 2.2) – Lead: Tyler Swartz and Nate Walters
	3	**Intrusion Detection Modernization** (Objective 1.1) – Lead: Brian Johns & Nate Walters
	4	**Identity and Access Management – Capital** (Objective 1.1) – Lead: Nate Walters
	5	**Vulnerability Management Program Maturity** (Objective 2.1) – Lead: Jim Webb
	6	**Create a Standardized Security Baseline** (Objective 2.3) – Lead: Tyler Swartz
Cyber Driven Initiative	7	**Endpoint Detection & Response** (Objective 2.3) – Lead: Jim Webb
	8	**NSOC Asset Intake Project** (Objective 2.1) – Lead: Patrick Yomes
	9	**TPU Cybersecurity Strategic Plan Update** Lead: Tyler Swartz
	10	**PCS Security Modernization / Services** – Phase I (Objective 1.1) – Lead: Jim Webb
	11	
	12	

TPU's Cyber Security Program – Key Tenets



Effective utilization of cyber talent

Stronger customer trust

Greater reliability

Enhanced resiliency