Cybersecurity and Data Privacy of Advanced Metering Infrastructure (AMI)

‘The Digital Foundation to Enhance the Customer Experience’

Public Utility Board Study Session
February 13, 2019
COMMON PHISHING TRAITS

1. Generic Greeting
2. Invokes Fear
3. Requires Action
4. Threatening Language
5. Grammar Issues
6. Generic Closing
Objectives

1. How Cybersecurity requirements were reflected in the AMI procurement process
2. How UTS will apply cybersecurity methods to the AMI system
3. Understanding customer data privacy concerns and AMI meter data
Cybersecurity requirements

• External Requirements were modeled from the Federal Risk and Authorization Management Program (FedRAMP)

• Internal requirements were modeled using NIST 800-53 Security Controls

• Over 900 security controls concerning confidentiality, integrity, and availability of the systems were vetted during the procurement phases.
Protecting AMI

**System Wide Security**
- Multi-Layer Encryption to the Endpoint
- Tamper Prevention and detection
- Time-Windowed Commands
- Pass-through devices
- Behavior Monitoring

**Meter Security**
- Non-Repudiation
- Modifications must originate from Headend
- All Modifications are logged
- No commands accepted from the field network
Protector customer data

• Data collected from the AMI meters is the same as data collected from traditional meters. Smart meters have no visibility within the home.

• All data is encrypted from the home to the Headend and digitally verified before being collected.

• Per policy, TPU does not release customer data without prior written consent from the customer. This is published on our website along with the Customer compliant process and is located Here.
SECC is a nonprofit organization that works to learn the wants and needs of energy consumers in North America, encourages the collaborative sharing of best practices in consumer engagement among industry stakeholders, and educates the public about the benefits of smart energy and energy technology.