To Compliance and Beyond!
Nice place to live, not visit

Wish You Were Here

Compliance
Compliance ≠ Security

Hypothetical Example

- Name an entity CIP Senior Manager
- Perform risk based assessment
- Identify zero critical assets
- Rinse and repeat annually

- This example results in compliance with little added security
Security ≠ Compliance

**Hypothetical Example # 2**

- Lock down every computing asset
- Implement Data Diodes on every routable connection
- Completely island all command and control assets on a single net
- Assume all of your cyber assets are secure / exempt from the standards
- Assume the corporate compliance department has you covered

- This example results in security with low likelihood of compliance
Ensure Balance

- Do not over invest in one and ignore the other
- Pursue both compliance and security
- Architect security or compliance investments to compliment the other
- Utilize Continuous Compliance tools or Active Policy Enforcement tools
How do you get there?

- People
- Money
- Training
- Tools
How do you get there?

- Tool Examples
  - Directory policy enforcement
  - Access requirement enforcement
  - Default / Shared account enforcement
  - Document management enforcement
  - Compliance management enforcement
  - Change management enforcement
  - Network Cyber access enforcement
Questions