Harmonizing ICS Security and Compliance
Moderator: Mike Assante, SANS Institute
Panelists:
Matt Davis, Ernst & Young
Perry Pederson, The Langer Group LLC
Josh Sandler, Duke Energy
Compliance vs. Security

Perry Pederson
The Langner Group
Washington DC | Hamburg | Munich
Definitions

**Compliance**: (1a) the act or process of complying to a desire, demand, proposal, or regimen or to coercion. (1b) conformity in fulfilling official requirements. (2) a disposition to yield to others.

**Security**: (1) the quality or state of being secure. (4a) something that secures : protection. (4b1) measures taken to guard against espionage or sabotage, crime, attack, or escape. (4b2) an organization or department whose task is security.
"The goal of this work is to dispel the belief that compliance with security standards provides assurance that system security goals are met.”

Jennifer Bayuk

“People, has compliance burned your brains?!!! We are NOT doing it to impress an auditor; we are doing it to stop an attacker!”

Anton Chuvakin

“CIOs must stop being rule followers who allow compliance to dominate business decision making and become risk leaders who proactively address the most severe threats to their enterprises.”

John A. Wheeler
RIPE Compliance Metrics

Robust Industrial Control Systems Planning and Evaluation

The Loviisa NPP in Finland is first to complete full annual cycle using RIPE

CSF Profile Comparison

- Target Profile
- Current Profile

- System Inventory
- Network Architecture
- Data Flow
- Workforce Information
- Training
- Policies and SOP
- System Procurement
- Plant Planning

100
80
60
40
20
0
QOTD References