Objective

• Develop a distributed peer-based framework to provide secure information exchange internally in critical infrastructure to increase security and resiliency of grid operation

Solution

• Securely communicate edge data (legacy and modern protocols) in a reliable and trustworthy way
• Provide security value-add through progressive enhancement
• Build on successes of prior efforts and provide easily integrated and field-tested solutions
• Release an extensible platform that provides increased awareness of communications and enables security protections

Challenges

• Meet availability and timeliness constraints while operating inline and enhancing security
• Provide a flexible, adaptable, and transparent deployment that provides immediate value-add with no operational impact
• Provide a solution that adds real value to Utility deployments today and enables future game-changing functionality in the future
• Leverage successes of emerging related efforts while balancing the need for stable, well-tested solutions

Status

• Design Implementation
• Customer Interaction and Feedback
• Beginning Development

Project Interaction

• Leverage integration and interoperation with past GPA efforts such as SIEGate
• Build on foundational exploration of projects like LEMNOS
• Build upon ICS protocol support and protocol semantic reasoning of Bro IDS
• Derive value from comparison against commercial related offerings