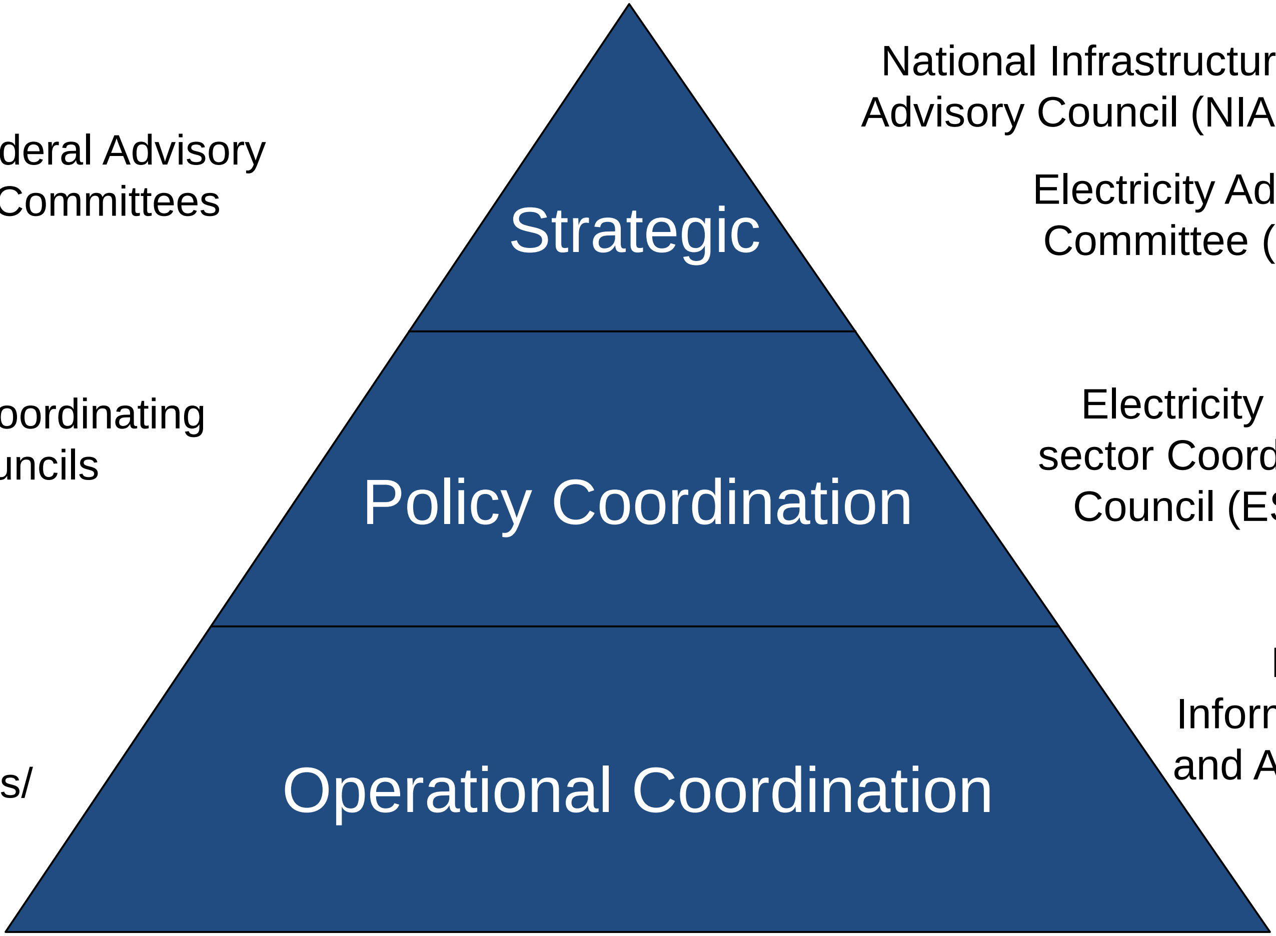
Electricity Information Sharing and Analysis Center (E-ISAC)

For Liberty Eclipse Exercise
December 8, 2016

TLP: GREEN

RESILIENCY | RELIABILITY | SECURITY

CIP Relationships



Federal Advisory Committees

National Infrastructure Advisory Council (NIAC)

Electricity Advisory Committee (EAC)

Strategic

Sector Coordinating Councils

Policy Coordination

Electricity Sub-sector Coordinating Council (ESCC)

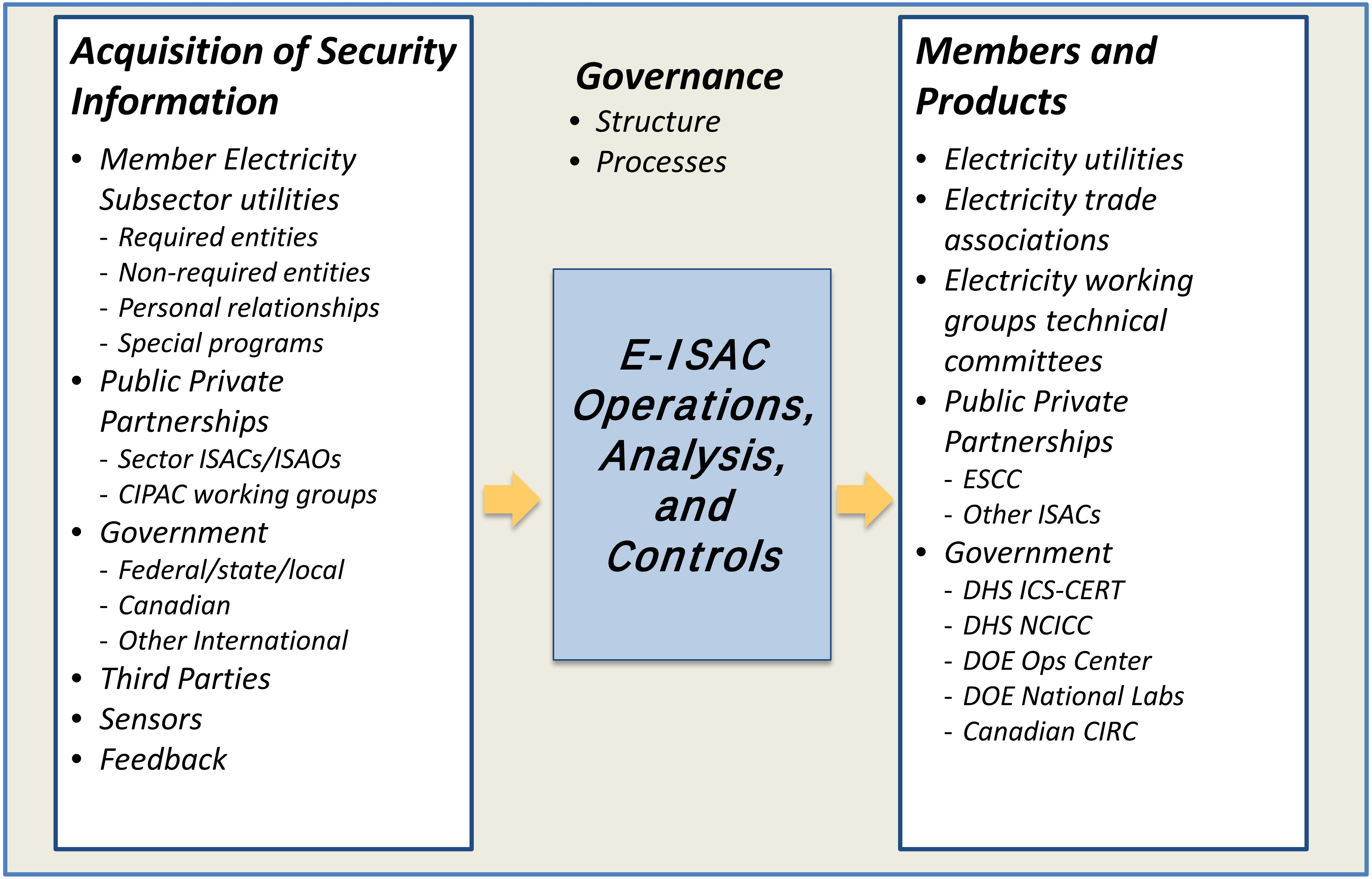
Information Sharing and Analysis Centers/ Organizations

Operational Coordination

Electricity Information Sharing and Analysis Center (E-ISAC)

E-ISAC
ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Value Chain



Acquisition of Security Information

- *Member Electricity Subsector utilities*
  - *Required entities*
  - *Non-required entities*
  - *Personal relationships*
  - *Special programs*
- *Public Private Partnerships*
  - *Sector ISACs/ISAOs*
  - *CIPAC working groups*
- *Government*
  - *Federal/state/local*
  - *Canadian*
  - *Other International*
- *Third Parties*
- *Sensors*
- *Feedback*

Governance

- *Structure*
- *Processes*

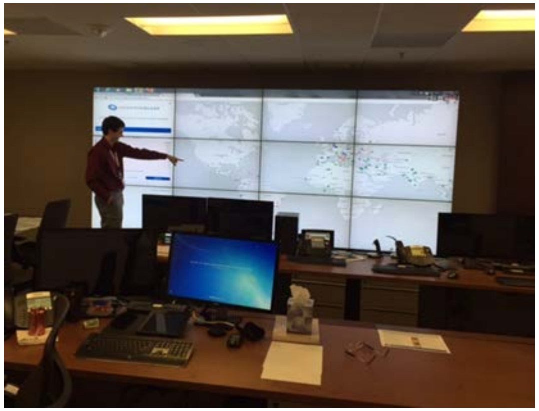
E-ISAC Operations, Analysis, and Controls

Members and Products

- *Electricity utilities*
- *Electricity trade associations*
- *Electricity working groups technical committees*
- *Public Private Partnerships*
  - *ESCC*
  - *Other ISACs*
- *Government*
  - *DHS ICS-CERT*
  - *DHS NCICC*
  - *DOE Ops Center*
  - *DOE National Labs*
  - *Canadian CIRC*

Capabilities

- Via NERC's BPSA team, real-time monitoring of the Grid
- Contracted with commercial providers to monitor the external IP ranges and domain names of all registered BPS entities
  - Botnet infection / mail server compromise / C2 nodes
  - Phishing / domain name spoofing / website spoofing
- Cyber Risk Information Sharing Program (CRISP)
  - Advanced threat awareness with entity notification
  - Multiple sources of information
  - Provides IOCs/Snort rules for non-CRISP participants within a week of detection



- Physical threat awareness program
  - Design Basis Threat / surveillance / improvised explosives / UAS / active shooter situations
- Cyber and physical threat analysis
  - Monthly education presentations, weekly sector summaries
- TLP Green / Amber / Red notifications via the E-ISAC portal

NCCIC Integration

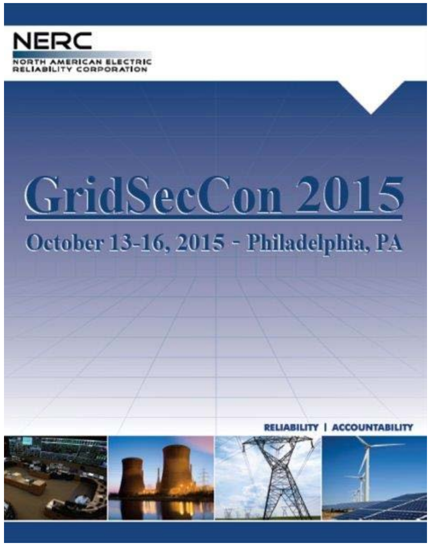
- The E-ISAC maintains a presence at the National Cybersecurity and Communications Integration Center (NCCIC), a DHS-operated 24/7 watch floor near Washington, D.C.
  - Top Secret, real-time, operations center
  - Hub for classified threat and vulnerability work
- E-ISAC cleared personnel analyze the threat and vulnerability components seen by the intelligence community and make an initial determination of potential impacts on the BPS

Staff Organization

- E-ISAC staff is oriented around five primary groups:
  - Programs & Engagement Team
  - Watch Operations Team
  - Cyber Analysis Team
  - Physical Analysis Team
  - CRISP Team
- New staff being hired
  - Focus is on filling out the Operations, Analysis & Physical Teams

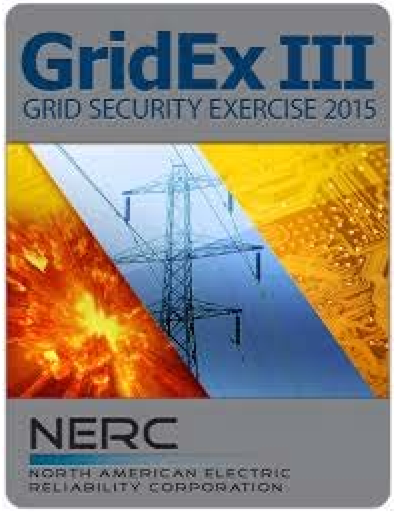
Exercises and Events

- Grid Security Conference (GridSecCon) 2015
  - October 17-21, 2016
  - Quebec City - Complete


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
GridSecCon 2015
October 13-16, 2015 - Philadelphia, PA
RELIABILITY | ACCOUNTABILITY

- GridEx IV
  - November, 2017
  - Two days of distributed play
  - Executive TTX
  - Multiple ways to participate

  - STG Series - Classified


GridEx III
GRID SECURITY EXERCISE 2015
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Today's Threatscape

- Threats include our vulnerabilities
- Opportunities include our strategic strengths – use them
- Small vectors can mean big impacts
- Out of the way target sets can be advanced actor attractive

What it means

- From protection to risk acceptance and management
- Risk prioritization and security collaboration
- Life is not just at the edge, its within our network environments
- Own system awareness, and all hands understanding are key

Questions and Answers