Southern Company

Information Sharing

Tom Wilson
Chief Information Security Officer

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association

Who We Are:

Southern Company is one of America's premier energy companies

Southern Company

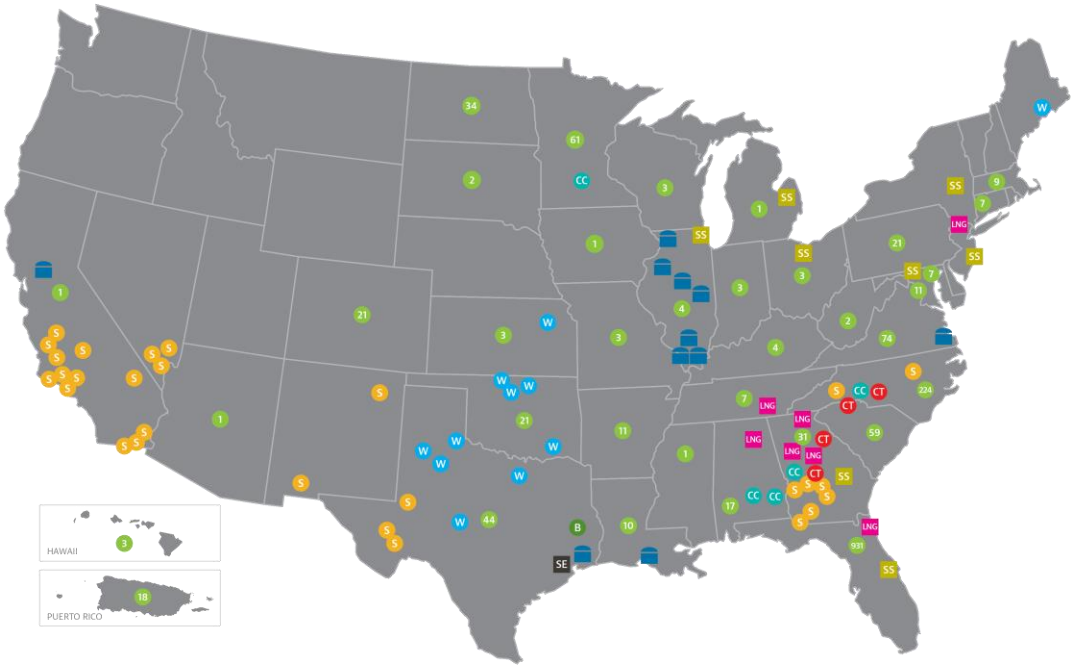
We provide clean, safe, reliable, affordable energy and customized solutions

Service territories

- Electric
- Gas

Gas pipelines

- Southern Natural Gas
- Southern Company Gas
- Pipeline projects



Southern Power

- Combined-cycle facility [1]
- Peaking facility
- Biomass facility
- Solar facility
- Wind facility

Southern Company Gas

- LNG facilities
- Sequent Energy Management
- SouthStar
- Natural gas storage

PowerSecure

- Owned and managed sites per state

[1]In November 2018, Southern Power agreed to sell its combined-cycle facility in Mankato, Minnesota.

Capabilities in **50 States**

7 Electric & Natural Gas Utilities

9 Million Customers

Approximately **29,000** Employees

Approximately **44,000 MW** of Generating Capacity

US Electric Sector Approaches to Grid Resiliency

REGULATIONS

Physical

Cyber

Resiliency

INDUSTRY GOVERNMENT PARTNERSHIPS

Electricity Subsector Coordinating Council (ESCC)

Electricity Information Sharing and Analysis Center (E-ISAC)

Partnerships with federal, state, and local governments

INDUSTRY PROGRAMS

Incident Response

Mutual Assistance

Spare Equipment

EXERCISES

GridEx V

Grid Security Exercise 2019

Why Information Sharing?

- **Early Detection of Threats:** Allow organizations to detect the threat sooner in their operational kill chain
- **Situational Awareness:** Increase situational awareness for individual organizations and the sector
- **Best Practices/Lessons Learned:** Improve overall security posture by learning from the practices of others

"Given the risks these threats present, it is increasingly important that organizations share cyber threat information and use it to improve their security posture."

- NIST SP 800-150 Guide to Cyber Threat Information Sharing

How to Process Information?

What to Share/Collect

- Indicators of Compromise (IOCs) which have a short- and medium-term value
- Tactics, Techniques, and Procedures (TTPs) - which are more difficult for an adversary to change - offer a longer-term value.
- Industry benchmarks to aid in understanding and improving investment and performance

How to Use Information

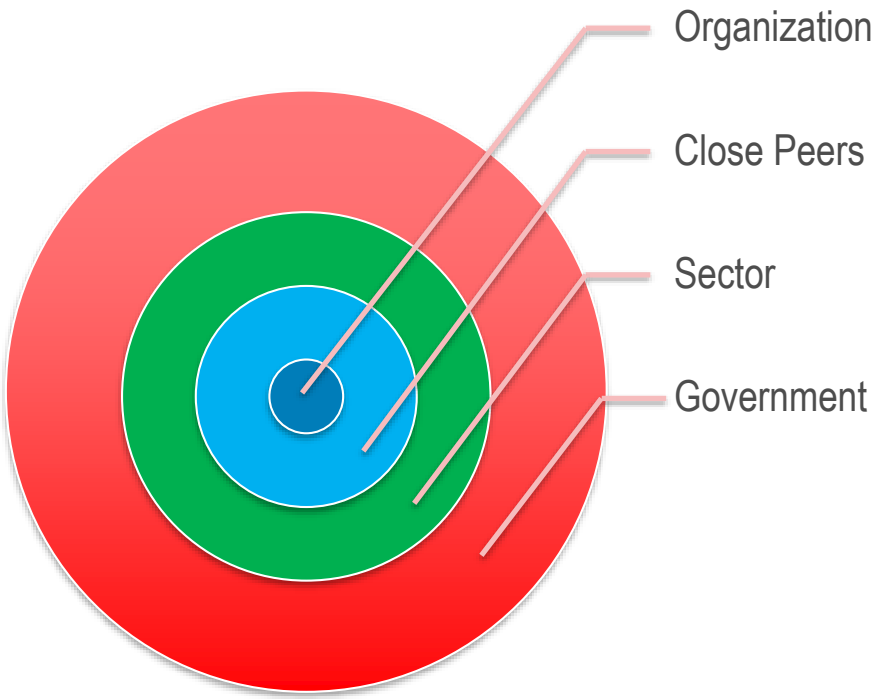
- Track threat actors, campaigns, and indications/warnings
- Create strategic intelligence for executive decision making
- Conduct routine collaboration and analysis

Timely, Vetted, Relevant, Accurate, Factual, and Actionable Information

(Command and Control*)

Circles of Trust

- Information sharing is fostered by trust, collaboration, and relationship building.
- Create a close circle of trusted individuals to leverage each other's capabilities.
- Meet with people in person, peer groups, and sector communities.
- Encourages sharing of business, process and technology enhancements.
- Provides for the ability to share organizational milestones and benchmark comparisons among peers.



Energy Sector: Information Trust Groups

U.S. Government

Industry

Third Parties

Collaboration Opportunities

Sharing Focus Areas and Scope

- **Cross Sector Peers**
  - Local
  - Consortiums, committees and conferences
- **Sector Peers**
  - Local
  - Trusted
  - Small industry consortiums
  - Broad national industry
  - International industry
- **Information Sharing Analysis Centers / Organizations (ISAC/ISAO)**
  - Sector
  - Sectors aligned by adversary or other commonalities
- **Government**
  - Sector-specific agency
  - Law enforcement
  - Intelligence community

Traffic Light Protocol (TLP) is a great framework for information handling designations.

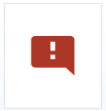
Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf

GridEx V: U.S. Government Information Sharing

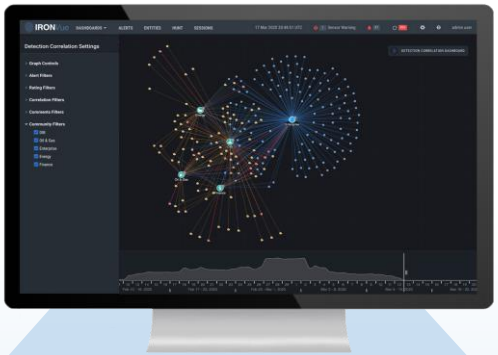
- Hosted **representatives** from government agencies
- Gain better understanding of Southern Company operations, response and recovery to different types of incidents
- Continued fostering relationships with the business units and corporate (physical) security
- Leverage lessons learned from GridEx to advance operational collaboration and development of joint (public-private) playbooks

Small Utilities, Small Supply Chain



Malicious Notifications

Weekly Collective Defense Report



Large Utilities, Supply Chain Enterprise

IronSensor (metal)

IronSensor for AWS

IronSensor for Azure

IronSensor for VMWare

IronNet

Intelligence Sharing

ISACs, Governments, etc.

Cyber Operations Center (CyOC)

- Continuous Overwatch
- Threat Intelligence
- Secure Communications

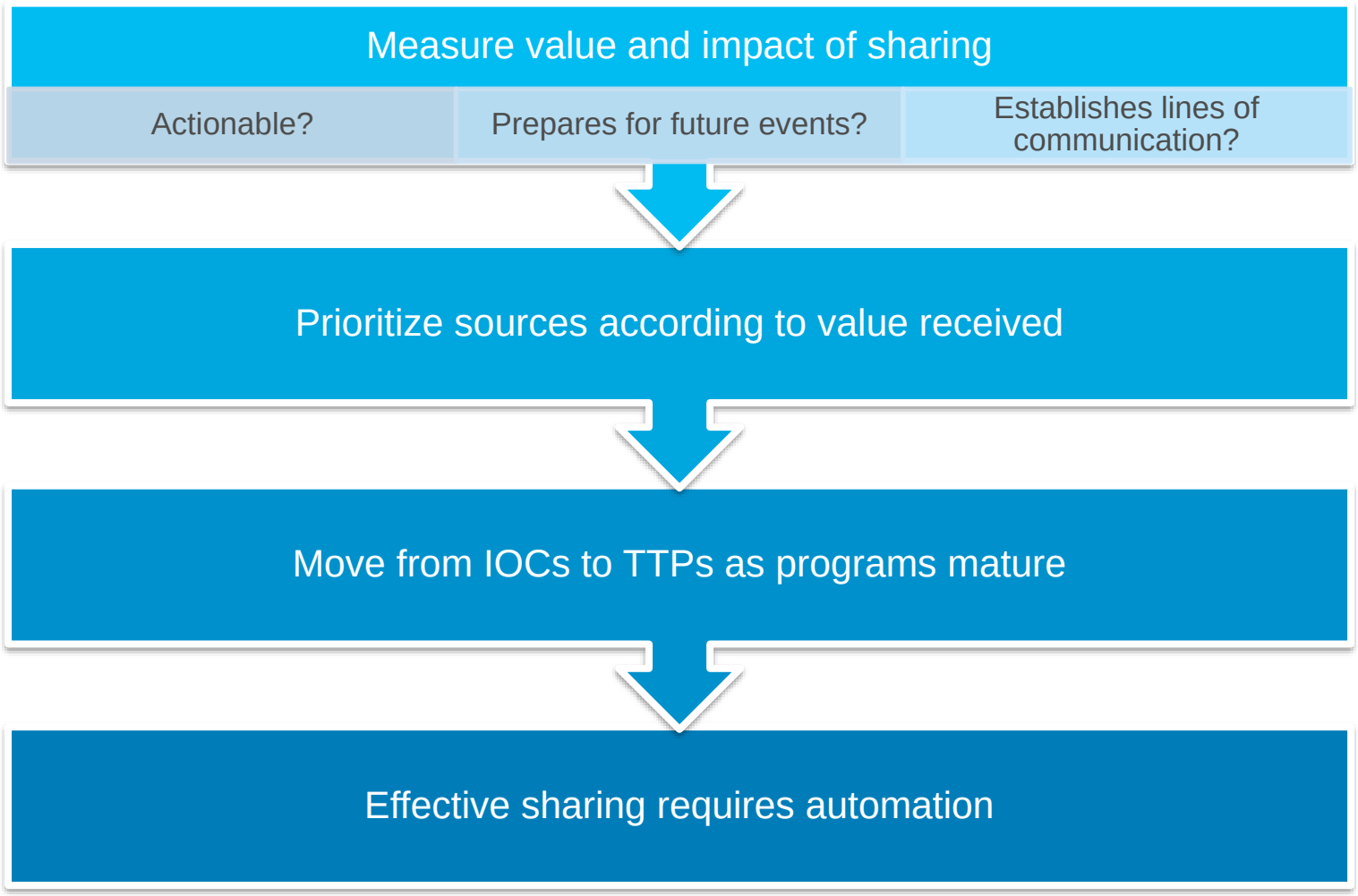
Countries, Sector Domes

Oil & Gas, Finance, Healthcare, International, etc.

IronNet Initiative – An Alternative to Traditional Information Sharing

- Sector and cross-sector visibility, sharing and collaboration
- Situational awareness of shared anomalies to investigate
- Security Operations Center (SOC) efficiency / focus through collaboration
  - prioritize threats confirmed at peers
  - deprioritize threats noted by peers

Lessons Learned and Best Practices



Plans Moving Forward

Business	• Awaiting future opportunities for in-person collaboration
Process	• Continued tabletop and playbook development • Refine processes based on lessons learned
Technology	• Increased automation and tool support for sharing • Data correlation tied to actionable intelligence

Final Thoughts…

Mission

- Improve security ecosystem within and across companies and governments
- Reduce adversary dwell time in targeted environments.
- Shorten the mean time to recovery after an incident.

Recommendations

- Information sharing across all organizational levels – information security analysts, information security leaders, management, and staff
- Create “circles of trust” to increase sharing and collaboration
- Share and adopt best practices, leveraging benchmarks where appropriate
  – create wins while growing and maturing


Southern Company