

# NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

## Consequence Modeling and Analysis

Kevin L. Stamber, Ph. D.

Infrastructure Systems Research, Analysis, &  
Applications

Sandia National Laboratories

[klstamb@sandia.gov](mailto:klstamb@sandia.gov)

Bryan T. Richardson

Critical Infrastructure Systems  
Sandia National Laboratories

[btricha@sandia.gov](mailto:btricha@sandia.gov)



U.S. Department of Energy  
Office of Electricity Delivery  
and Energy Reliability



Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

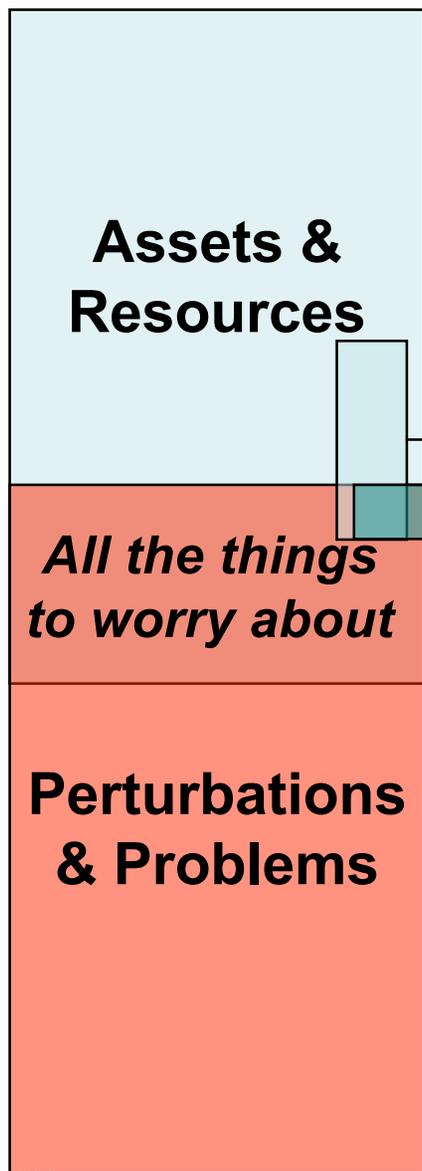


- Are the consequences quantifiable in a way that is relevant to the stakeholder's business/operational roles?
- What are the consequences of the impacts in terms of the stakeholder's business/operational roles?
- Are the consequences of the impacts locally, regionally, or nationally significant?
- Where could mitigations be implemented to lower the consequences?

# Overview

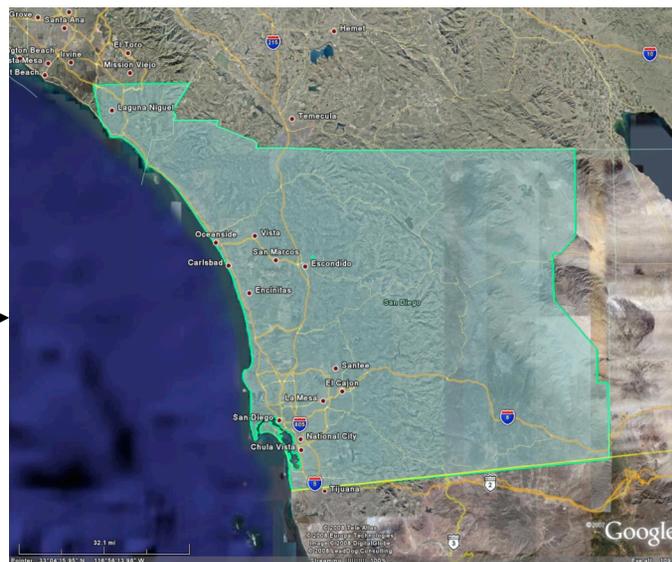
- Consequence Analysis: Method and Application
- Consequence Metrics
- Risk, Consequence, and Actors
- Identifying Key Stakeholders
- Consequence Estimation
  - Approach
  - Results

## Consequence Analysis: Method and Application



Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture <sup>1</sup> Department of Health and Human Services <sup>2</sup>	Agriculture and Food
Department of Defense <sup>3</sup>	Defense Industrial Base
Department of Energy	Energy <sup>4</sup>
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security Office of Infrastructure Protection	Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Telecommunications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard <sup>5</sup>	Transportation Systems <sup>6</sup>
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

### Assets Relevant to Public Interest and Impact in Question

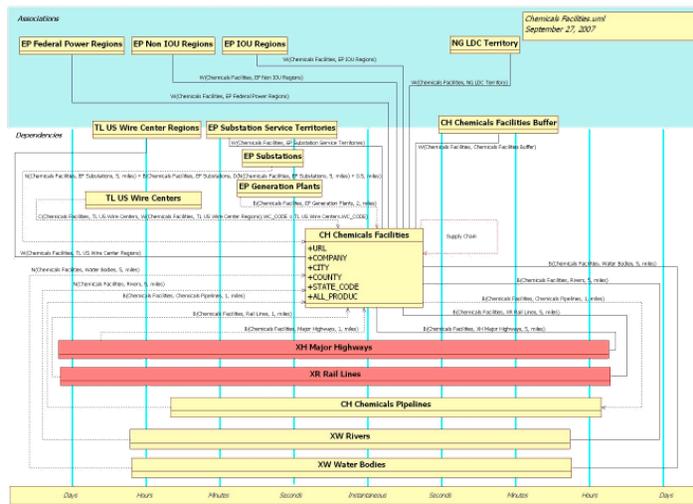


Area of Projected Impact

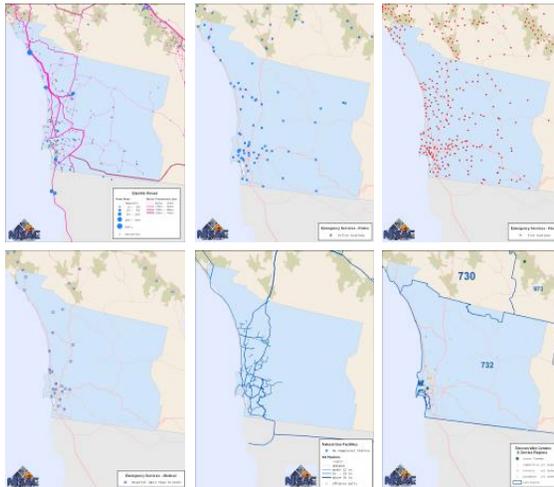
## Consequence Analysis: Method and Application



Disruptive Effect



Indirect Infrastructure Consequences



Direct Infrastructure Consequences



Economic Impact

# Consequence Metrics

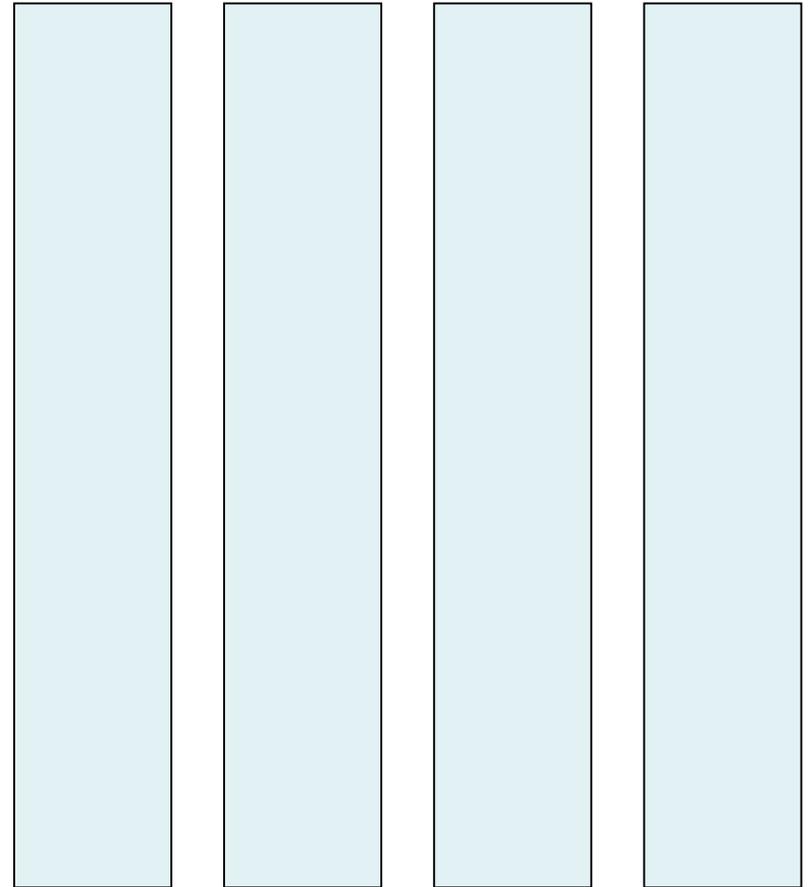
- Some are readily quantified
  - Casualties
  - Economic loss
- Others, not so much
  - Psychological Impacts
  - Confidence in Government
  - Loss of Governance
- Even the readily quantified require clear definition
  - Casualties: Deaths? Injuries? Both?
  - Economic loss: Over what time frame?
- Combination of the readily quantified can be a nightmare
  - How much is a life worth? Are you willing to commit it to print?

# Risk, Consequence and Actors

- Risk = Threat \* Vulnerability \* Consequence
- Keep this in mind as we discuss the variety of actors involved in understanding how infrastructure fits together
  - Vertical Actors
  - Horizontal Actors
  - Vertical Endpoint Actors
  - Diagonal Actors

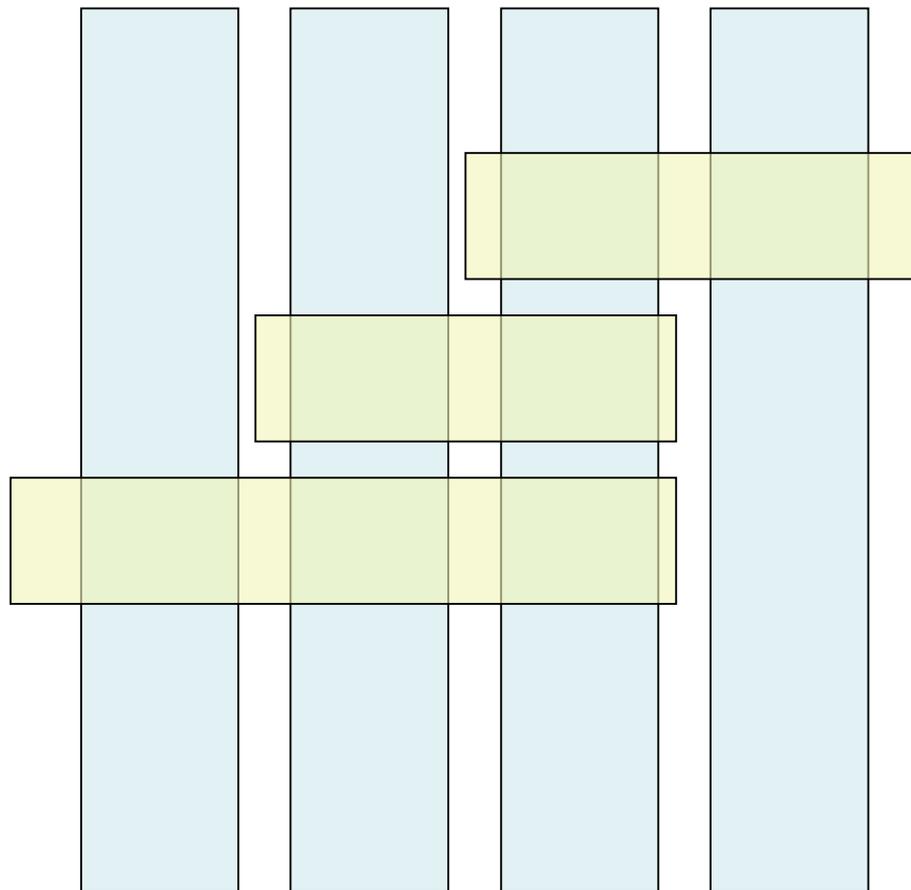
# Risk, Consequence and Actors

- Vertical Actors
  - Represent the structure of the flow of infrastructure service from source to ultimate customer
    - GenCos
    - TransCos
    - Vertically Integrated Utilities
    - ISOs/RTOs
    - Security Coordinators
    - Utility Sector Self-Regulatory Entities
  - Are likely interdependent entities
    - Within an infrastructure, sharing assets/contractual rights of way
    - Across infrastructures, serving as ultimate customers of one another



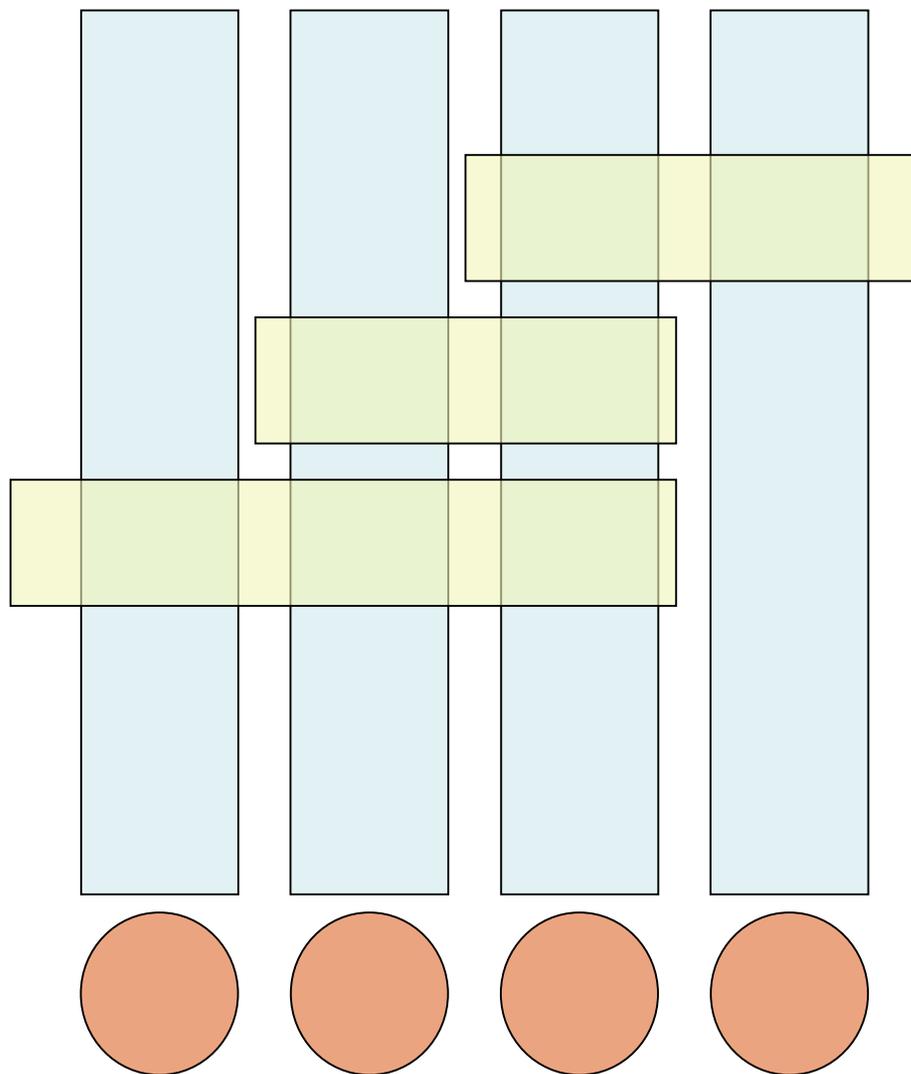
# Risk, Consequence and Actors

- Horizontal Actors
  - Represent the vendors which provide support and capability which enables a Vertical Actor
    - Hardware manufacturers
      - “system hardware” (e.g., generators, switches, wiring, poles, transformers)
      - “system control hardware” (e.g., computers, real-time monitoring equipment)
    - Software vendors



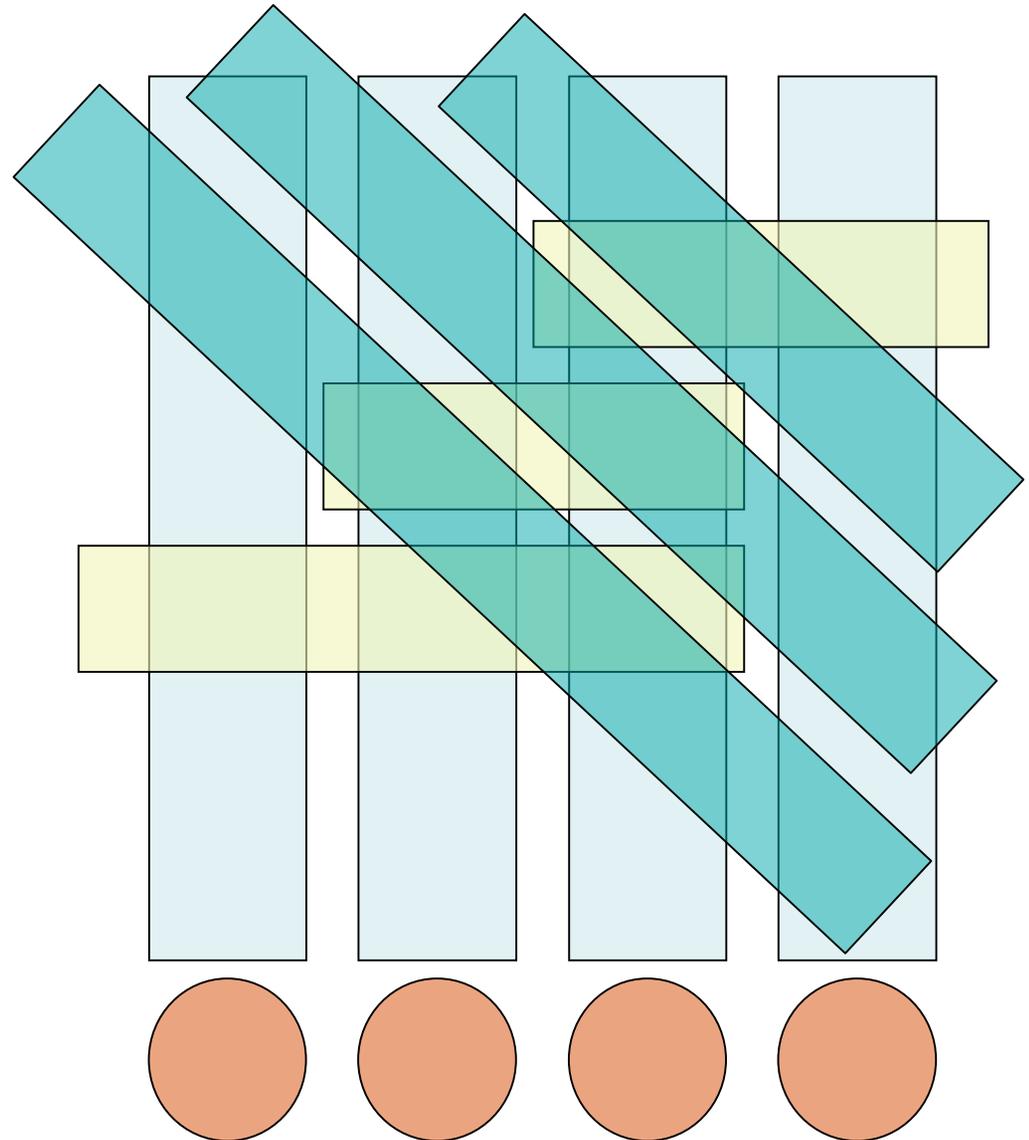
# Risk, Consequence and Actors

- Vertical Endpoint Actors
  - Represent the ultimate customer of a Vertical Actor
    - Can be a gateway for Vertical or Horizontal Actors



## Risk, Consequence and Actors

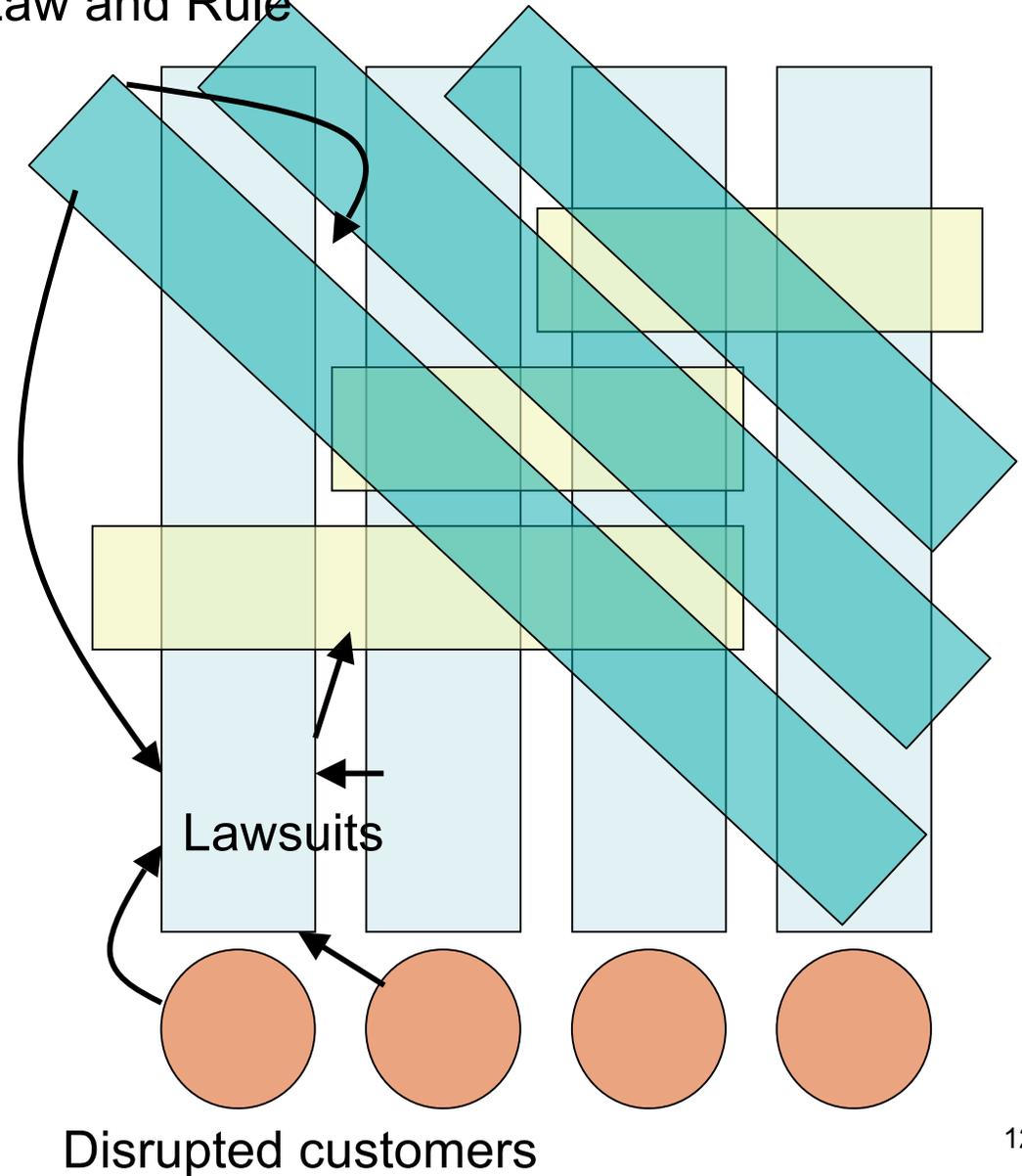
- Diagonal Actors
  - Represent entities who either reduce or increase impediments to collaboration among Vertical and Horizontal Actors
  - Those who reduce impediments are Positive Action Diagonal
  - Those who increase impediments are Negative Action Diagonal
  - Some actors alternate between the two states
  - Examples
    - Researchers
    - Their funding entities
    - Insurers and Reinsurers
    - Regulatory Authorities
    - Legislative Bodies



## Identifying Key Stakeholders

- When the vulnerability is ubiquitous among like actors
  - Consequence is the driving metric in identifying those stakeholders who face the greatest risk
  - Consequences more than direct as cascading effects lead to larger consequences
    - Many of these larger consequences are drags on economic and system performance
  - Therefore it is important to look at the relative level of consequence among like actors
    - for our discussion, among Vertical Actor utilities

New Law and Rule

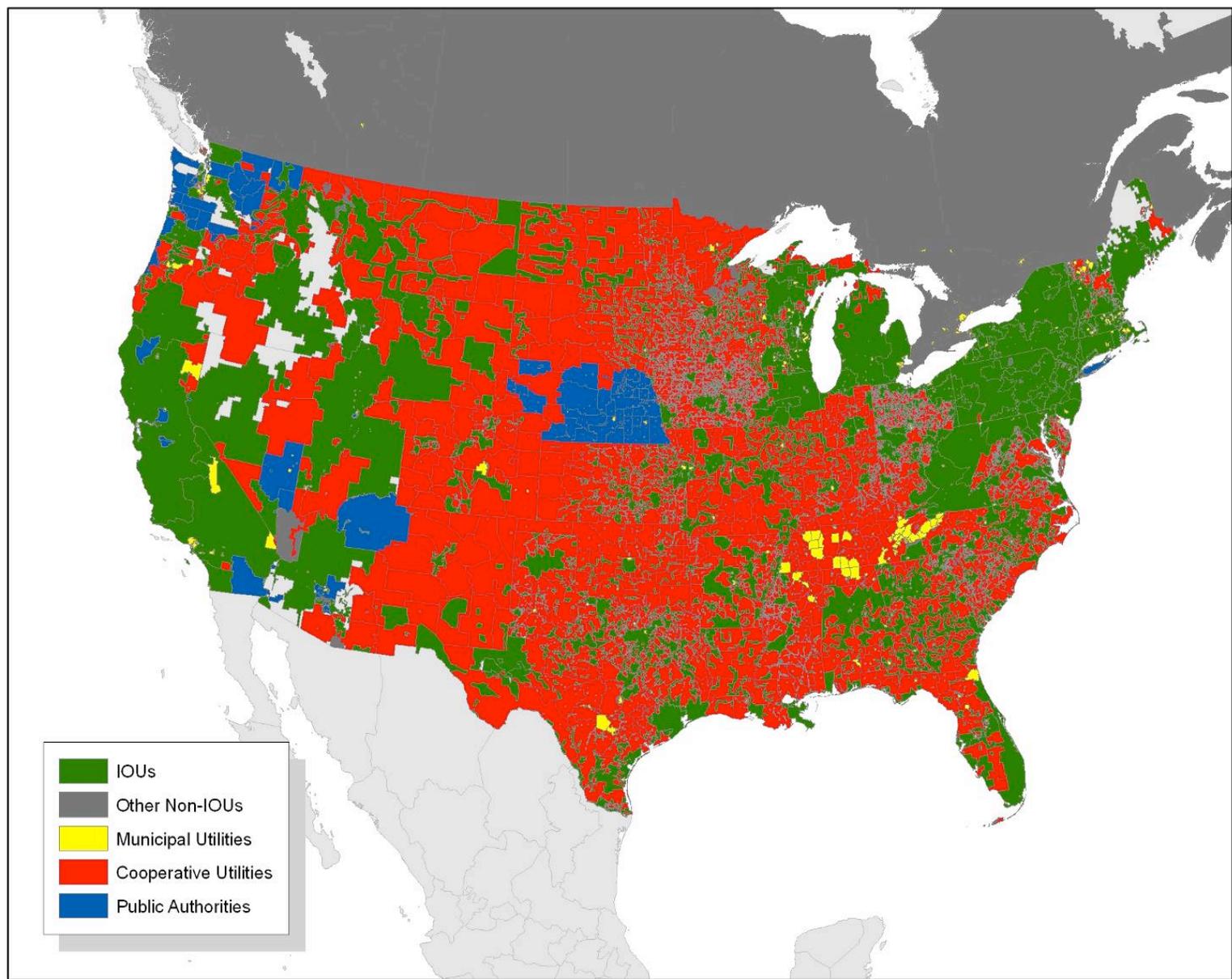


# Identifying Key Stakeholders

- **Acknowledgment**
  - Analysis performed using tools developed for the National Infrastructure Simulation and Analysis Center (NISAC)
    - a program of the Assistant Secretary for Infrastructure Protection, Department of Homeland Security
    - a core partnership of Sandia National Laboratories and Los Alamos National Laboratory
    - Contact Information: Gerald Frazier, IP/IASD/NISAC Program Office, 703-235-3603, [gerald.frazier@dhs.gov](mailto:gerald.frazier@dhs.gov)



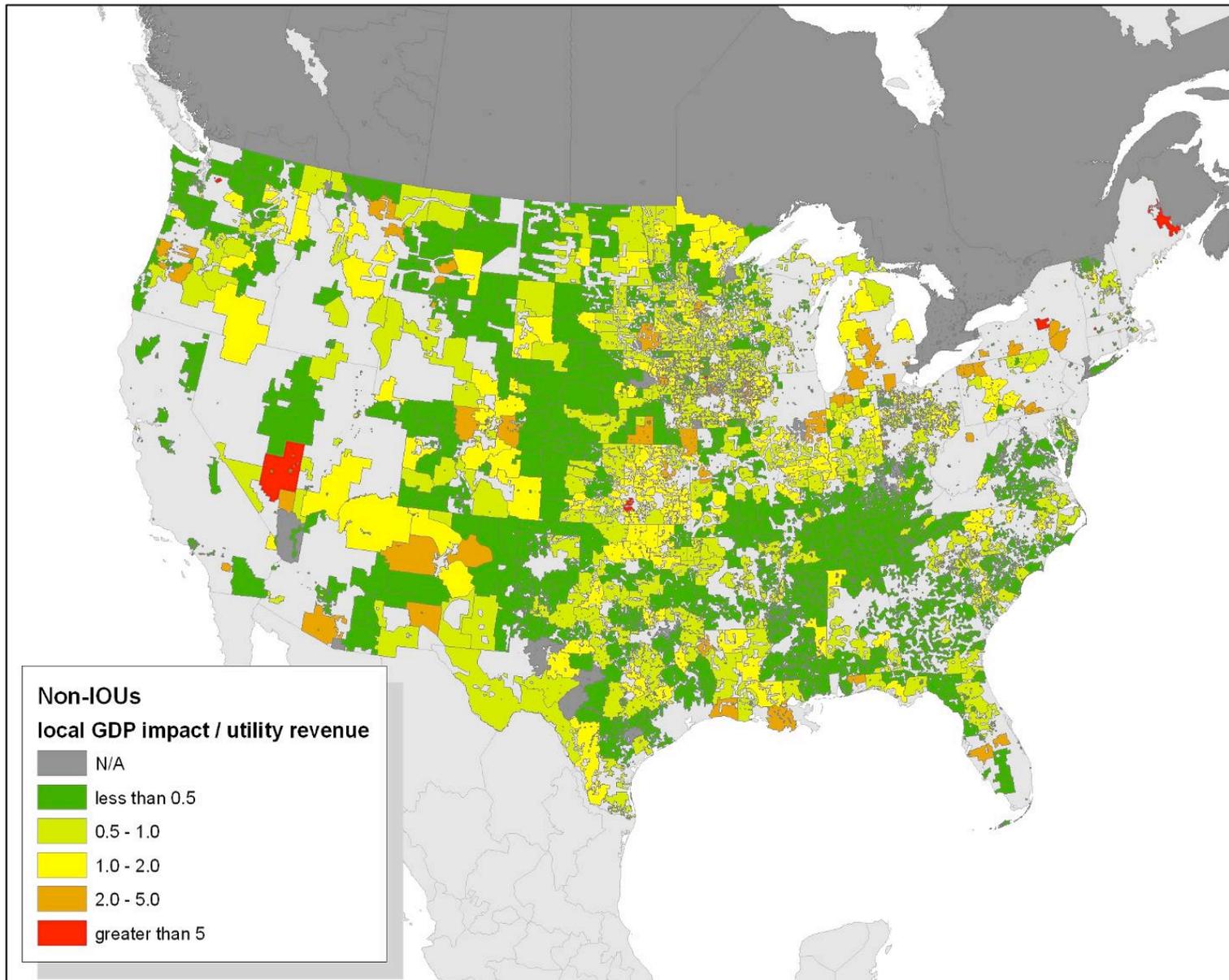
## Identifying Key Stakeholders



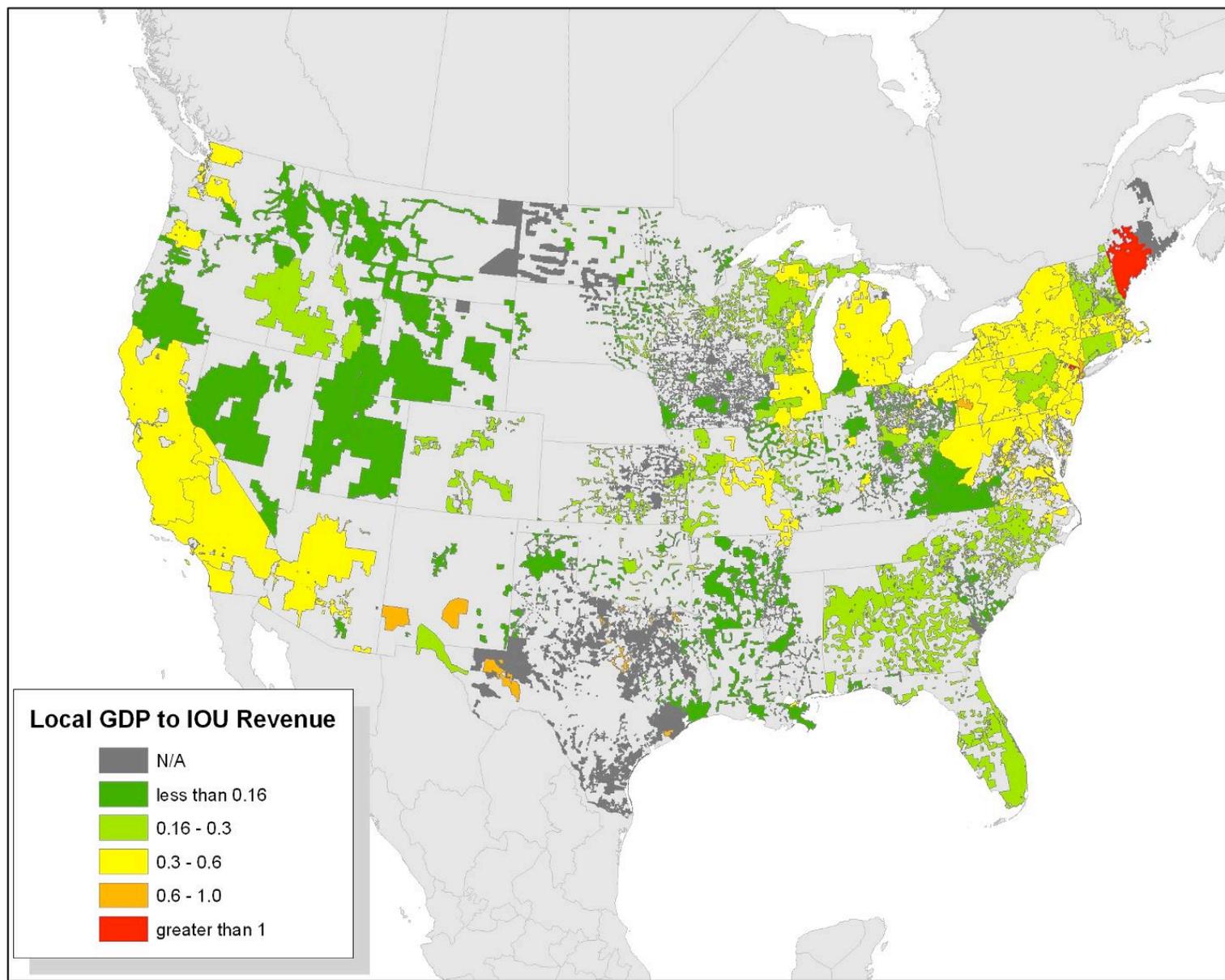
# Identifying Key Stakeholders

- For Non-IOUs
  - Examine the value of direct and indirect business disruption lasting one day for the entirety of the Non-IOUs service territory relative to the annual operating revenue of the Non-IOU
- For IOUs
  - Examine the value of direct and indirect business disruption lasting one day for the entirety of the Interconnection containing the IOUs service territory relative to the annual operating revenue of the IOU
- Data sources used
  - Utility service territories, revenue data (Platts)
  - Economic and employment data (Census, BEA)

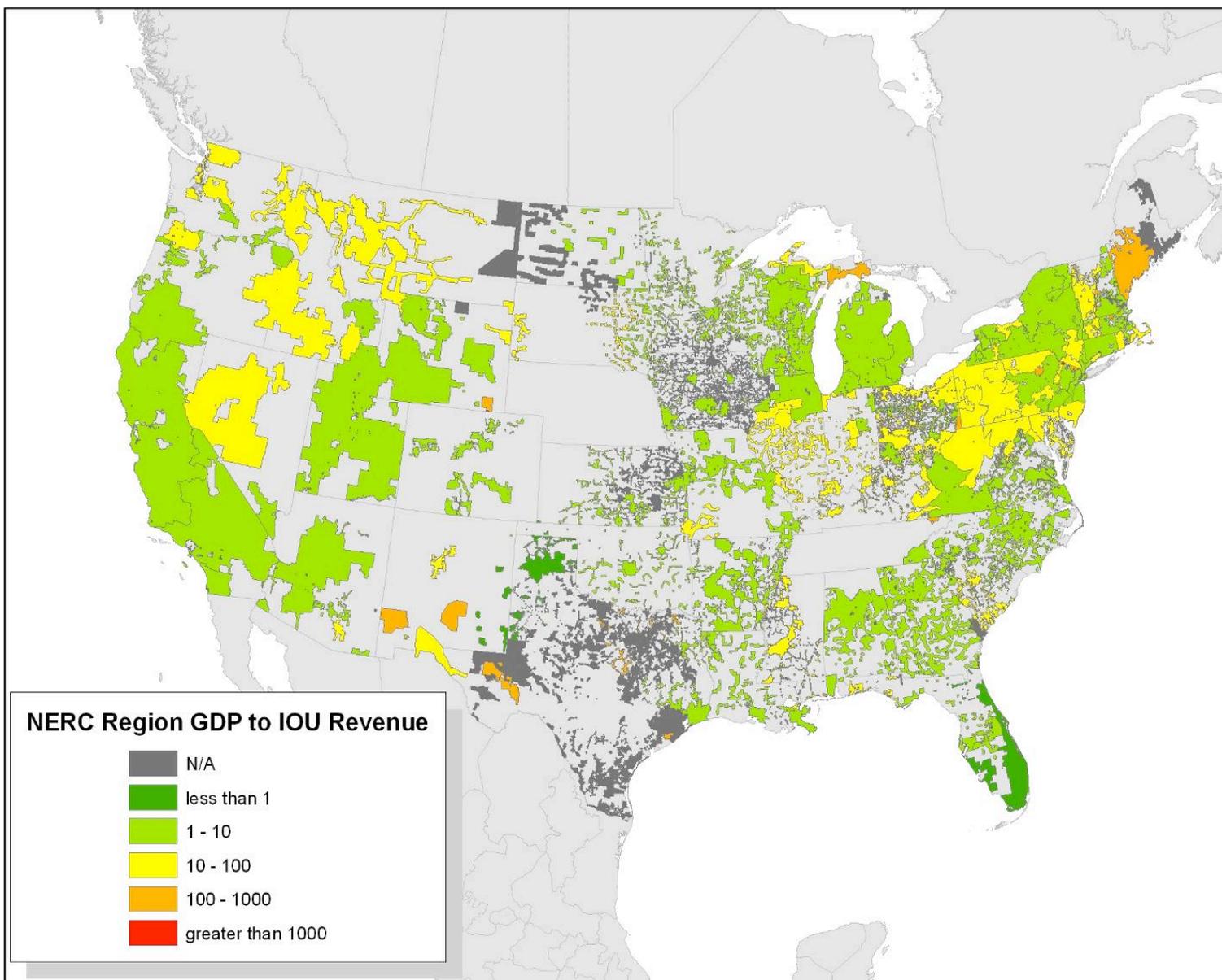
## Identifying Key Stakeholders



## Identifying Key Stakeholders



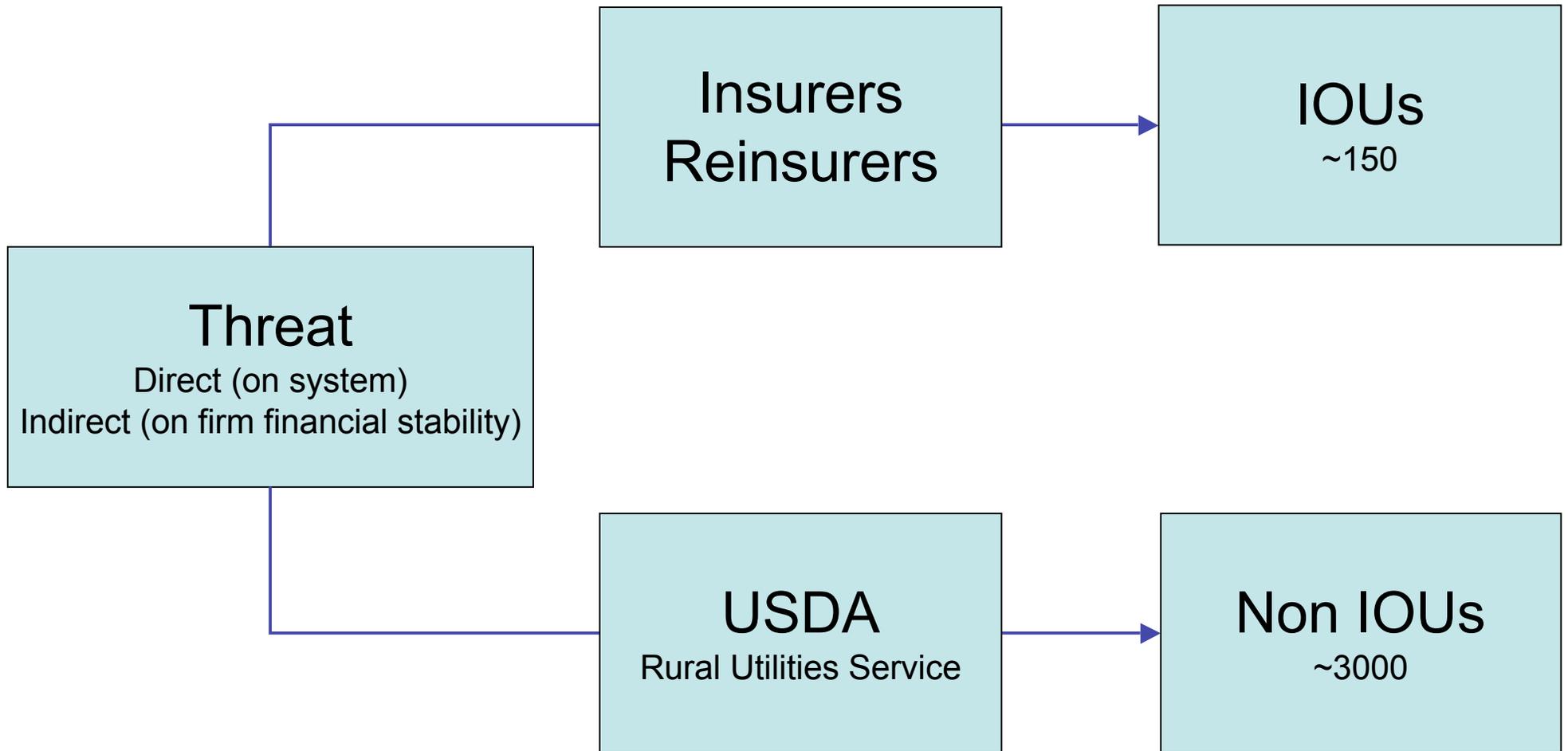
# Identifying Key Stakeholders



# Identifying Key Stakeholders

- **Sample Investor-Owned Utility**
  - Annual Revenue ~ \$2B
  - Single-Day Direct and Indirect Business Disruption Impacts for Service Territory over \$1B
  - Single-Day Direct and Indirect Business Disruption Impacts for WECC over \$10B
- **As that which we've discussed is both ubiquitous and repetitive**
  - Modelling and simulation has shown that other kinds of disruptions can be worse
    - Perception of reduced reliability
    - Leads to high-value customer departure
    - Leads to reduced revenue
    - Leads to distribution of O&M over smaller customer base (higher rates)

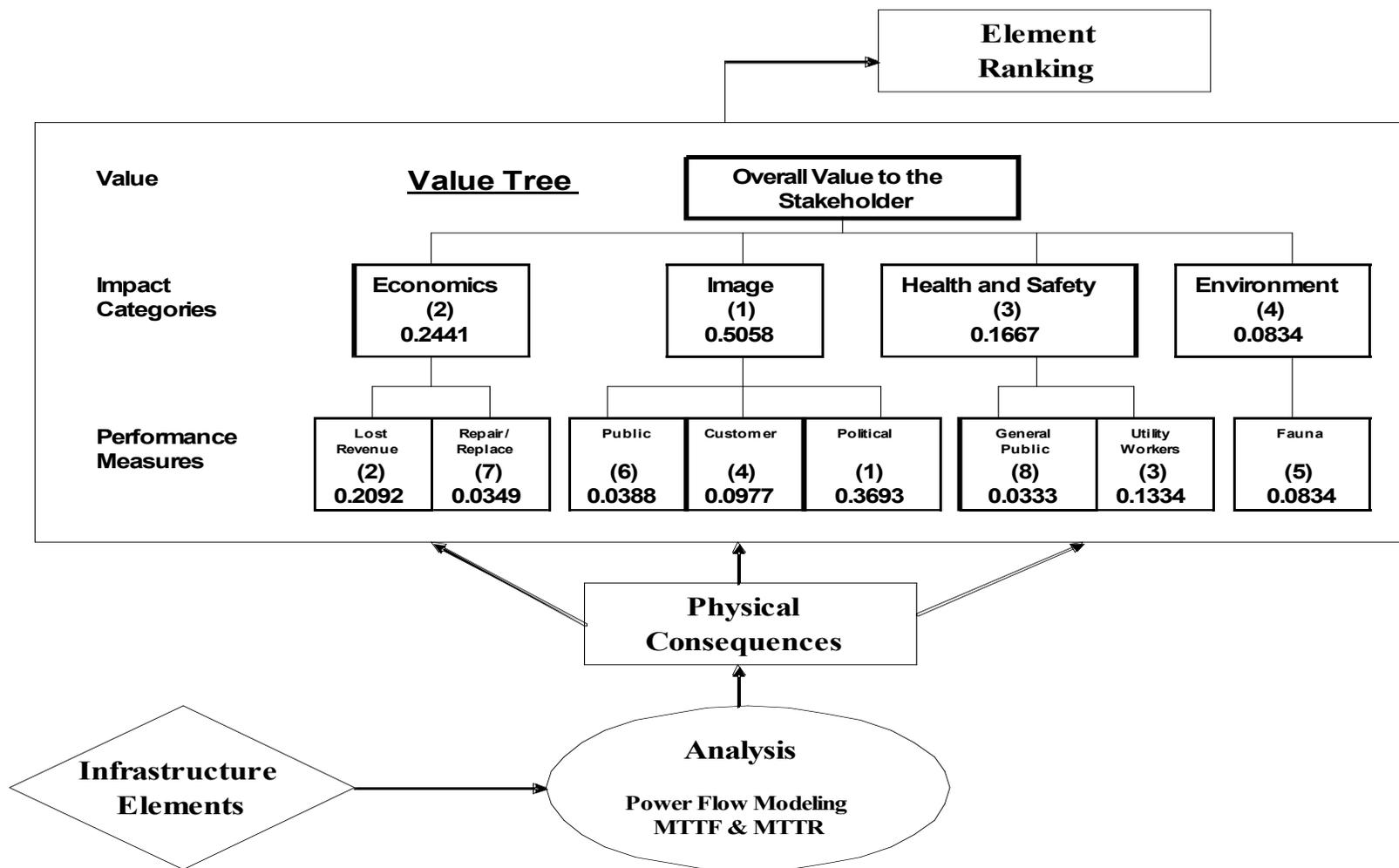
## Identifying Key Stakeholders



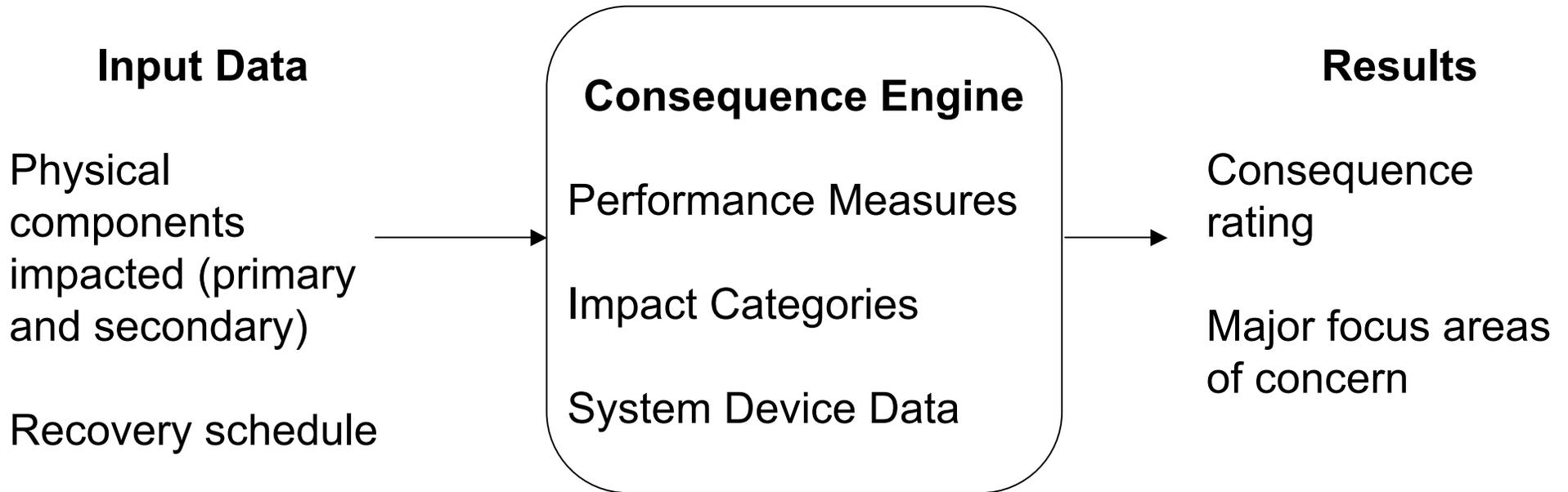
# Consequence Estimation

- Stakeholders have a need to base consequence on metrics they care about
  - Economics, public image, health and safety, etc.
- Physical impacts must somehow be mapped to metrics
- Metrics most likely will not be equally important to everyone and in every situation
  - Can use pairwise comparison techniques to weigh metrics
- As impacts occur, metrics and specific system data could be used to calculate a **numerical value** for consequence
- Metrics could also highlight areas of concern within the system that mitigations could be applied to

# Approach for Consequence Estimation



# Approach for Consequence Estimation



## Rogue Software Scenario Consequence Results

File System Help
Consequence Modeling Tool
\_ □ ×

**System Status: 0.2691**      **Total Cost of Outage: \$6768174**

This category represents the third priority for counter terrorism efforts. These locations are normally less vulnerable because they are either less susceptible or less valuable than the terrorist desire.

Risk Analysis

Component
System Health Levels
Performance Levels
Constructed Scales

**G22**      **Total Cost of Component Loss: \$991458**

This category represents the third priority for counter terrorism efforts. These locations are normally less vulnerable because they are either less susceptible or less valuable than the terrorist desire.

**Affected Components:**

Component: L1      **Amount Load Shed: 100%**

Component: L2      **Amount Load Shed: 100%**

Number of Residential Customers Affected:

Number of Commercial Customers Affected:

Number of Small/Medium Industrial Customers Affected:

Number of Large Industrial Customers Affected:

Name:

Type:

Description:

Threat Level:

Outage Time:

Cost to Repair:

Default Utility Worker Level:

Default Fauna Level:

Number of Residential Customers:

Number of Commercial Customers:

Number of Small/Medium Industrial Customers:

Number of Large Industrial Customers:

Performance Measure	Level
Economics - Lost Revenue	Hundreds of Thousands of Doll...
Economics - Repair/Replace	Tens of Thousands of Dollars
Image - Public	Repeated publications in nation...
Image - Customer	No impact
Image - Political	Low political influence on indust...
Health & Safety - General Public	No impact
Health & Safety - Utility Workers	Low safety impact on worker as...
Environment - Fauna	No impact

# Summary

# Questions?