SAND2007-7996P

IRS Visit – SNL Overview
Information Technologies (IT) Exchange

Constantine "Dino" Pavlakos
Sandia National Laboratories
December 2007

Sandia National Laboratories

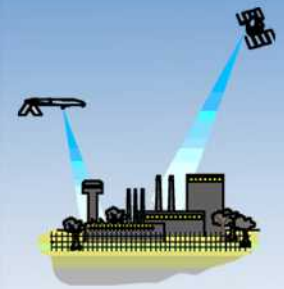
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Management Groups

Integrated Technologies and Systems

Three Management Units:

- Energy, Resources, and Nonproliferation
- Homeland Security
- Defense Systems and Assessments



Nuclear Weapons

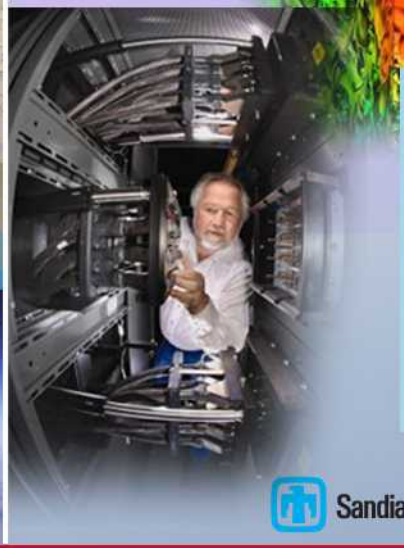
One Management Unit:

- Nuclear Weapons

Laboratory Transformation

Two Management Units:

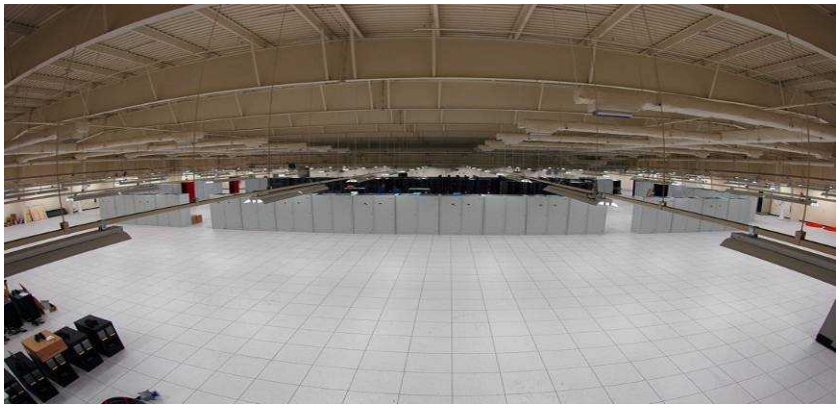
- Integrated Enabling Services
- Science, Technology, and Engineering



Sandia National Laboratories

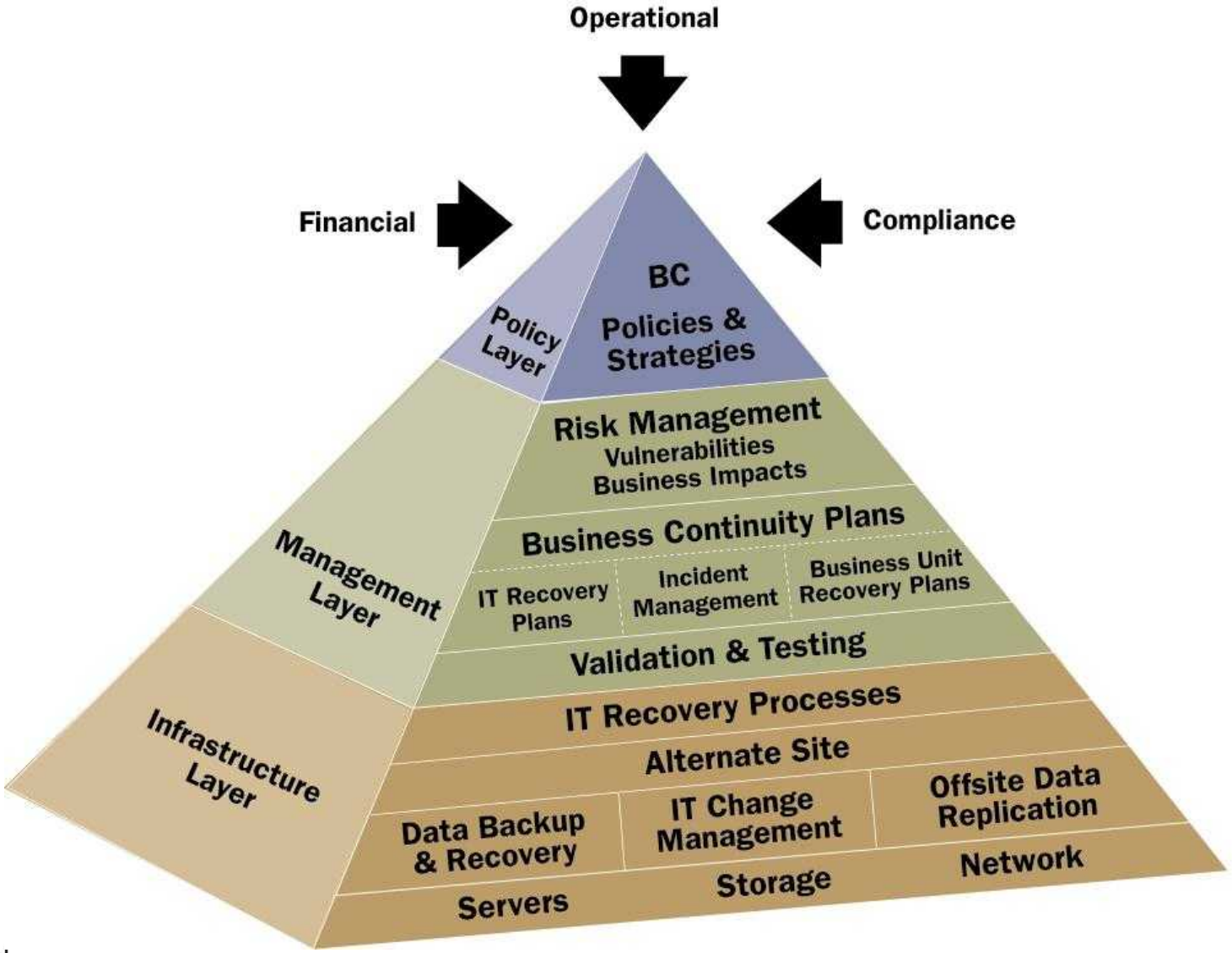
Lots of experience with complex IT environments

- Infrastructure deployment, operation & support
- Thousands (~36,000) of distributed desktops, workstations, laptops, etc. -- enterprise & engineering / scientific
- Enterprise services (~800 servers) and high performance computing (hundreds of teraflops)
- Networking -- classified, unclassified, open; ~25,000 drops
- Facilities: power & cooling
- Two SNL sites (NM & CA)
- NNSA Tri-lab computing environment
- Cyber security



Sandia National Laboratories

Building DR/BC Into The Enterprise



Sandia National Laboratories

Sandia IT Continuity Strategy

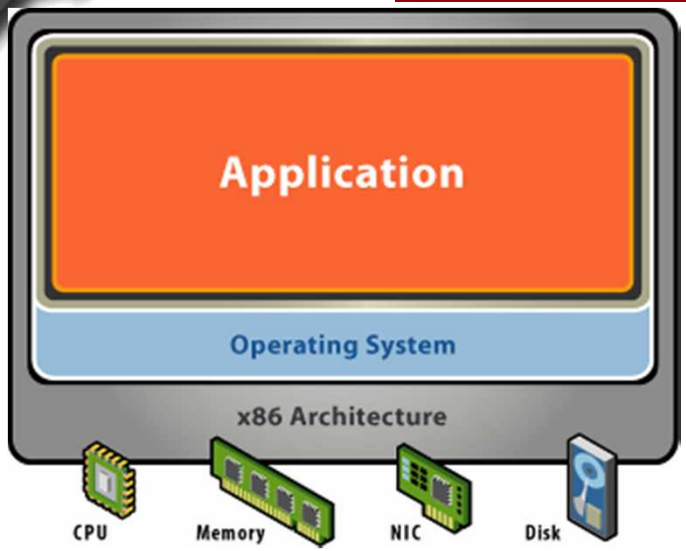
Recovery with Reasonable Spending Before Disruption

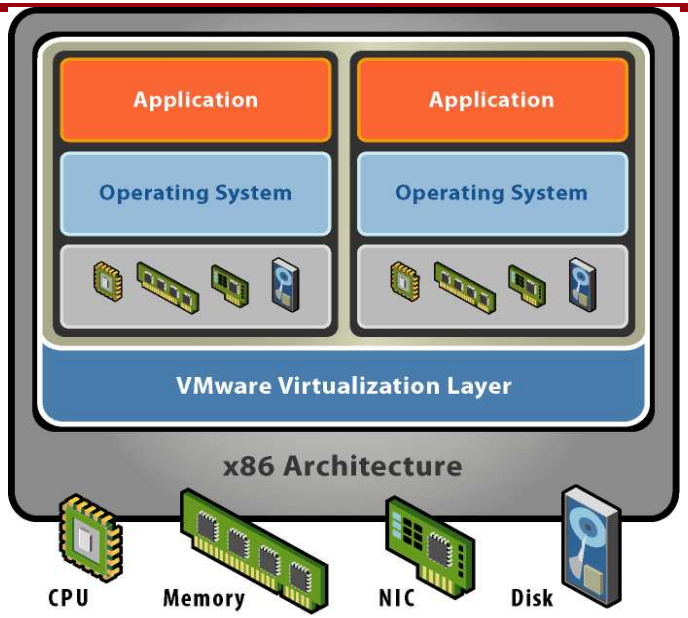
- Alternate recovery site determined - Sandia Livermore
  - Using established data center owned by Sandia
- Recovery based on tiering process
  - Tier 0 (security, safety) auto failover at alternate site
  - Tier 1 (mission essential applications based on Business Impact Assessment) equipment ready
  - Tier 2+ (operate and enhance) equipment will be quick-shipped based on needs
- Data stores, operating systems, applications will be replicated to alternate recovery site
- Recovery plans developed by owners and tested on recurring basis
- Recovery costs built-in to IT services and applications

Sandia IT Continuity Strategy
Current State

- Alternate recovery site established at Sandia Livermore
- Tier 0 services (security, safety) auto failover implemented
- Replication software in pilot phase
- Recovery plans
  - Software implemented
  - Recovery plan template designed
  - Recovery plans for Tier 0 services in progress
  - Tabletop tests in progress

SNL IT starting to explore & make use of Virtualization





Before Virtualization:

- Single OS image per machine
- Software and hardware tightly coupled
- Running multiple applications on same machine often creates conflict
- Result: Underutilized resources
- Inflexible and costly infrastructure

After Virtualization:

- **Breaks dependencies** between the BIOS, OS, and Applications from hardware
- Allows many applications to share same physical hardware
- VM's are **hardware-independent:** they can be provisioned anywhere

Sandia National Laboratories

Phase 1: Currently operating ~115 virtual machines within our Enterprise Services.

Application Performance Analysis, Monitoring and Troubleshooting

Pre-deployment

- **Test web applications *prior* to deployment to determine:**
  - If they can accommodate the expected number of users
  - The upper limit of these systems for capacity planning

Post-deployment

- **Monitor response time and availability *from a user perspective***
- **Trigger action from response team when thresholds are exceeded**

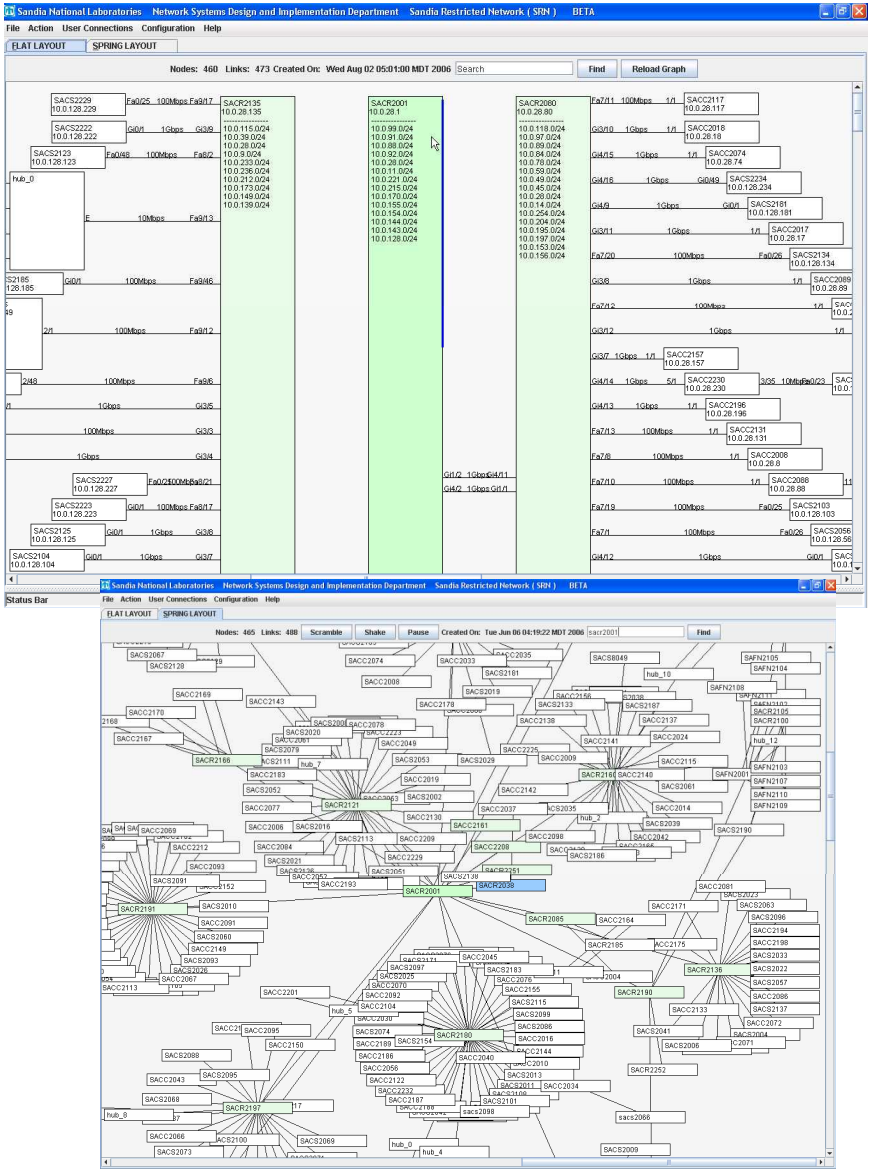
Troubleshooting

- **Provide response team with data and analysis to support trouble resolution**

DRIfT -- Dynamically Rendered Infrastructure Topology

DRIfT provides

- unified network visualization and real-time situational awareness
- enabling IT staff to dynamically create a single view with servers, critical network elements and links and the operational state of the combined view.
- Its primary purpose is to render network diagrams dynamically for rapidly changing networks
- and to provide an interface from which additional information can be obtained and visualized.



Sandia National Laboratories

DRIfT -- Dynamically Rendered Infrastructure Topology

- **IRS interested in Sandia's DRIfT capabilities to diagram/visualize network topology, alarms and events, utilization.**
- **Government Use Notice (license) issued to Enterprise Networks/IRS for DRIfT software on 10/29/2007.**
  - IRS POCs: John.S.Chambliss@irs.gov, steven.morgan@irs.gov
- **DRIfT 4.0 was released 12/3/07. Is to be delivered to IRS.**
- **SNL and IRS share common network modeling and simulation capabilities.**
  - IRS and Sandia both use OPNET's Virtual Network Environment Server to create/maintain a data model of their enterprise networks. (Primary data source for DRIfT.)
  - Both agencies use network simulation tools by OPNET technologies, ITGURU software family.
  - IRS can readily incorporate DRIfT into their environment.
  - Same tools to perform network configuration audits for regulatory compliance e.g. NIST 800-53.

Cyber Security at Sandia National Laboratories

- **Cyber security is integral to Sandia's computing environment**
  - Networks
    - Wired and wireless intrusion detection
    - Bi-directional packet captures
      - 30 day "look back" of all traffic to/from the internet
    - Firewall event monitoring and reporting
  - Desktops and Servers
    - Vulnerability and penetration testing
      - IIS
      - Tenable
      - "Hands on" testing
    - Remote updates/patching and configuration management
  - E-discovery
    - E-mail
    - Web logs
    - Forensic examinations
  - Rapid Response Security Team
    - Subject matter experts from all cyber disciplines form event-specific teams
      - Full decision making authority appropriate for the threat at hand
      - Team's membership varies based upon current event
        - Ensures appropriate experts are engaged

Cyber Security Technology

- **Two-Factor Authentication**
  - Fully deployed to all elevated privileged accounts
  - Smartcard integration into Active Directory
  - CryptoCard integration into Radius and MIT Kerberos
- **PKI Initiatives**
  - Deploying Credent Technologies solutions for laptop/desktop and removable media
  - Key player in DOE PKI environment. Locally manage one of the DOE Certificate Authorities.

Cyber Security Monitoring & Analysis

- **Vulnerability assessments & Penetration testing**
  - ISS RealSecure
  - NMAP
  - Nessus/Tenable
  - Metasploit
  - CoreImpact
- **E-discovery and Forensics**
  - EnCase e-discovery suite
    - ENCE-certified examiners
  - Forensics ToolKit
  - Reverse Engineering
    - IDAPro
- **Intrusion detection**
  - SNORT signature-based IDS
    - Industry-standard and in-house developed rules
  - Full packet capture
    - 11tb on-line storage for packet captures
  - StealthWatch
    - Behavioral IDS
  - AirDefense wireless IDS

Information Systems Analysis Center (5600)
Information Assurance

- **Threat modeling and assessment**
  - Supported by unique capabilities in multi-domain red teaming
    - "Red teaming = authorized adversary-based assessment for defensive purposes"
    - Method-based approaches to structuring and conducting assessment means actionable information for decision makers
- **Communications security analysis and design**
  - Cryptographic R&D
  - Secure communications solutions reduce risk in critical systems
- **Secure network architectures**
  - Improves system/mission survivability in hostile environments through security-driven design
- **Control systems security**
  - Specialized knowledge in process/automation control systems including those used for electricity, oil & gas, manufacturing, building controls and physical protection/monitoring systems
- **Tool development for advanced IA**
  - Supports improved information/situational awareness
  - Provides stronger insight into system weaknesses, consequences
  - Assists in development of mitigations
- **Custom hardware solutions**
  - Improves trust in COTS-based systems
  - Component fabrication at Sandia

Information Systems Analysis Center (5600)
Modeling & Simulation

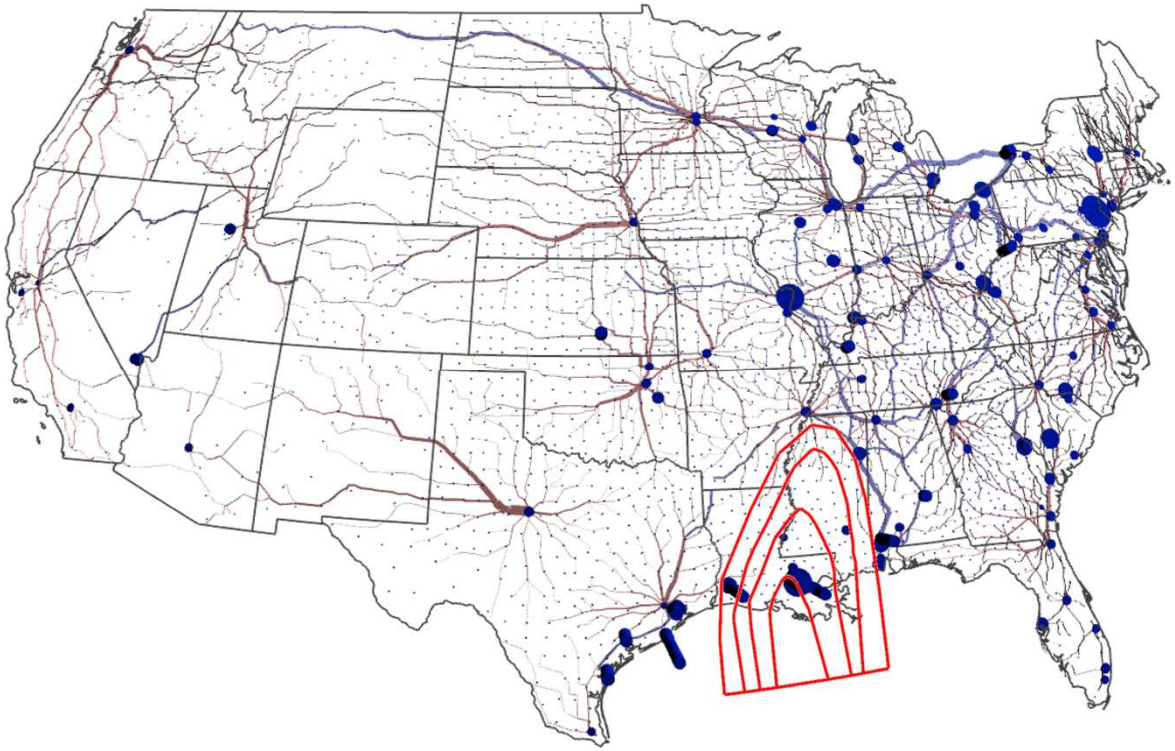
- **Networked Information System Analysis**
  - Modeling & Simulation
    - Model development at various levels of abstraction
      - System devices
      - System architecture
      - System traffic
      - System environment (including adversary or attacker impacts on system)
    - Scenario development to target specific analysis questions
      - System security
      - System reliability
      - System performance
    - Post simulation data analysis
  - Scenario Development
    - Identify scenarios requiring analysis
      - Device failures
      - Attacks on system
    - Develop models at level of abstraction to answer target analysis questions
  - Networked information system simulations can be combined with broader system simulations (co-simulation & federation)

U.S. Economic Resiliency

Briefing to the U.S. House Committee on Homeland Security

October 10, 2007

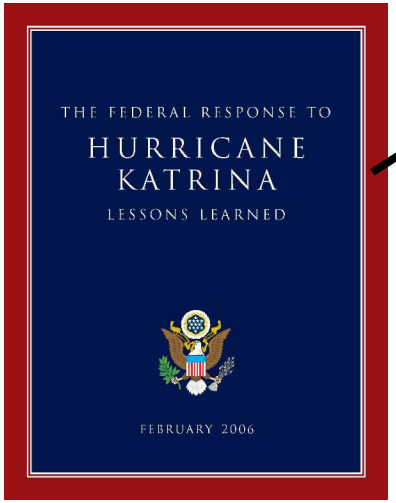
Mark A. Ehlen, Ph.D.
Economist, NISAC ● Team Lead, Computational Economics Group
National Infrastructure Simulation & Analysis Center (NISAC)
Department of Homeland Security
Office of Infrastructure Protection



Los Alamos
Sandia National Laboratories

NISAC

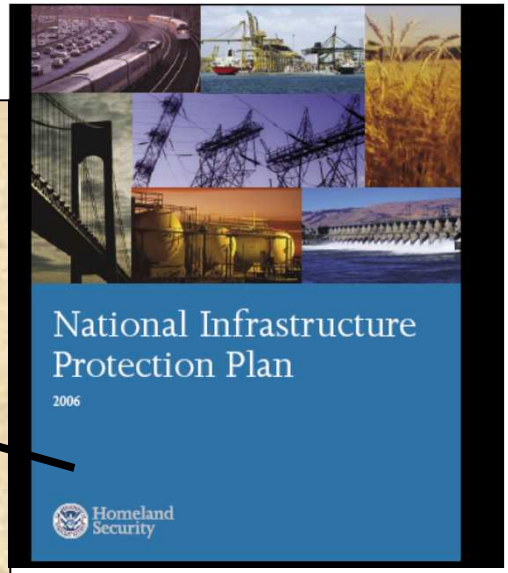
NISAC is Recognized as a Valuable National Resource



- Hurricane Katrina Lessons Learned Recommendations:
- 78. DHS should revise the National Response Plan…optional actions will be based on reports from…the National Infrastructure Simulation and Analysis Center (NISAC)…
- 82. DHS should expand the National Infrastructure Simulation and Analysis Center's (NISAC) Modeling and Analysis capability to allow more robust and accurate systems modeling.
- 83. The National Economic Council should form an Impact Assessment Working Group to provide an overall economic impact assessment of major disasters, including the Departments of Homeland Security, Treasury, Commerce, Energy (Energy Information Administration) and Labor as well as the President's Council of Economic Advisers…The various economic modeling expertise of the members of the Impact Assessment Working Group should be incorporated into the NISAC models.

- From National Infrastructure Protection Plan:
- The NISAC is chartered to develop advanced modeling, simulation, and analysis capabilities for the Nation's CI/KR. These tools address physical and cyber dependencies and interdependencies in an all-hazards context. These sophisticated models enhance the Nation's understanding of CI/KR dependencies and interdependencies, and better inform decisionmakers in the areas of policy analysis, investment, prevention and mitigation planning, education, training, and crisis response…

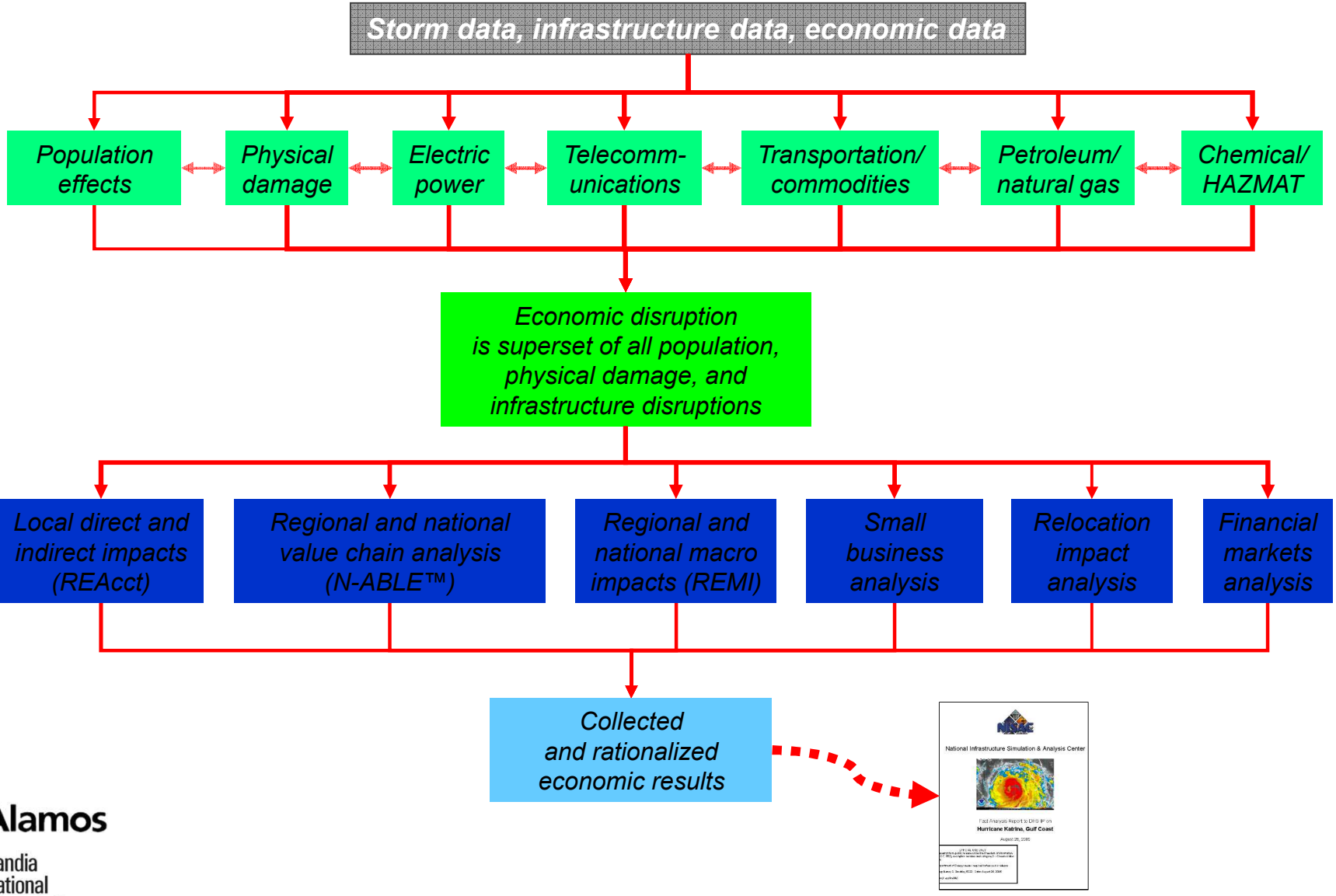
- Modeling and simulations through the NISAC will help quantify national and international dependency and interdependency, as well as their resulting consequences.



National Laboratories

Los Alamos

How Economic Analysis fits within the Broader NISAC



Los Alamos

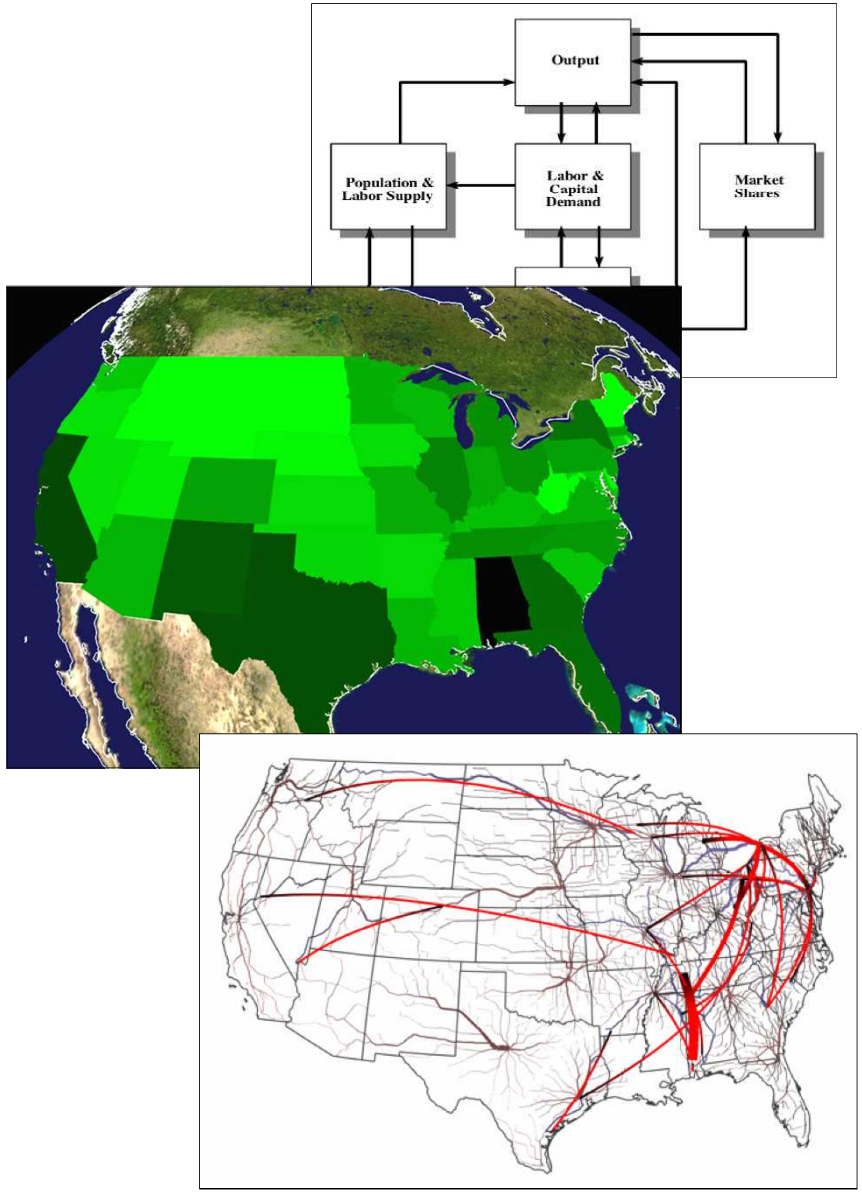
Sandia National Laboratories

History and Path of NISAC Economic Analysis

- Analyses
- **Have conducted over 100 detailed economic impact studies, e.g.,** natural disasters**: hurricanes, earthquakes, pandemic influenza;** man-made**: terrorist attacks (e.g., chem/bio), port closures, rail transport shutdowns, air traffic shutdowns, commodity futures markets**

- Models
- **Use a suite of microeconomic, mesoeconomic, and macroeconomic tools for both fast reach-back, longer term studies, and development of new NISAC models (e.g., the U.S. petrochemicals supply chain).**

- Current Capability Development
- **Tools and analytical approaches that can help define, measure, and design homeland security policy for** economic resiliency



Los Alamos
Sandia National Laboratories

NISAC Economic Toolkit

Approach	Description	Benefits / Best Use	Example Studies
Data Analysis	**Application of multiple socio-economic data sources to specific problem**	**Short analysis period; high-fidelity answers for impacts where economic consequence paths are basic.**	**Chlorine Phase 1**
REAcct	**Input-Output model modified to man-made or natural disaster-based infrastructure disruptions, in which economy returns to baseline**	**Short analysis period; consequence paths are widespread; methodology that can be applied across NISAC projects**	**Pre-landfall hurricane analyses**
REMI / IMPLAN	**Large-scale, state-level / county-level macroeconomic models of the U.S.**	**Long-term impacts due to structural changes in the economy. Highly validated models.**	**Katrina, Pandemic Influenza, MANPAD Senior Officials Exercise**
System Dynamics	**Systems-of-equations approach to modeling deterministic dynamics in a complex system**	**Large-scale problems where infrastructure disruptions influence the economy in short time durations**	**Pandemic influenza**
N-ABLE™	**High-fidelity stochastic, dynamic agent-based economic modeling of the U.S. economy**	**National economic impacts, where impacts need to be known with great fidelity.**	**Chlorine Phase 2** **National milk supply chain; international tire supply chain, U.S. border security; petrochemicals industry, manufactured foods**

Sandia National Laboratories

Los Alamos

IPAWS is the Nation's next-generation emergency warning capability

- Department of Homeland Security program begun in 2004 to improve public alert & warning in partnership with NOAA*, the FCC*, & other public/private stakeholders.
- Evolving "system of systems"
  - Emergency Alert System (EAS) upgrades
  - National Warning System (NAWAS) enhancements
  - **New pilots and systems:**
    - Digital EAS (DEAS) program with APTS* and others
    - **Web Alert and Relay Network (WARN) pilot with Sandia and others**
    - Geo-Targeted Alerting System (GTAS) program with NOAA and others

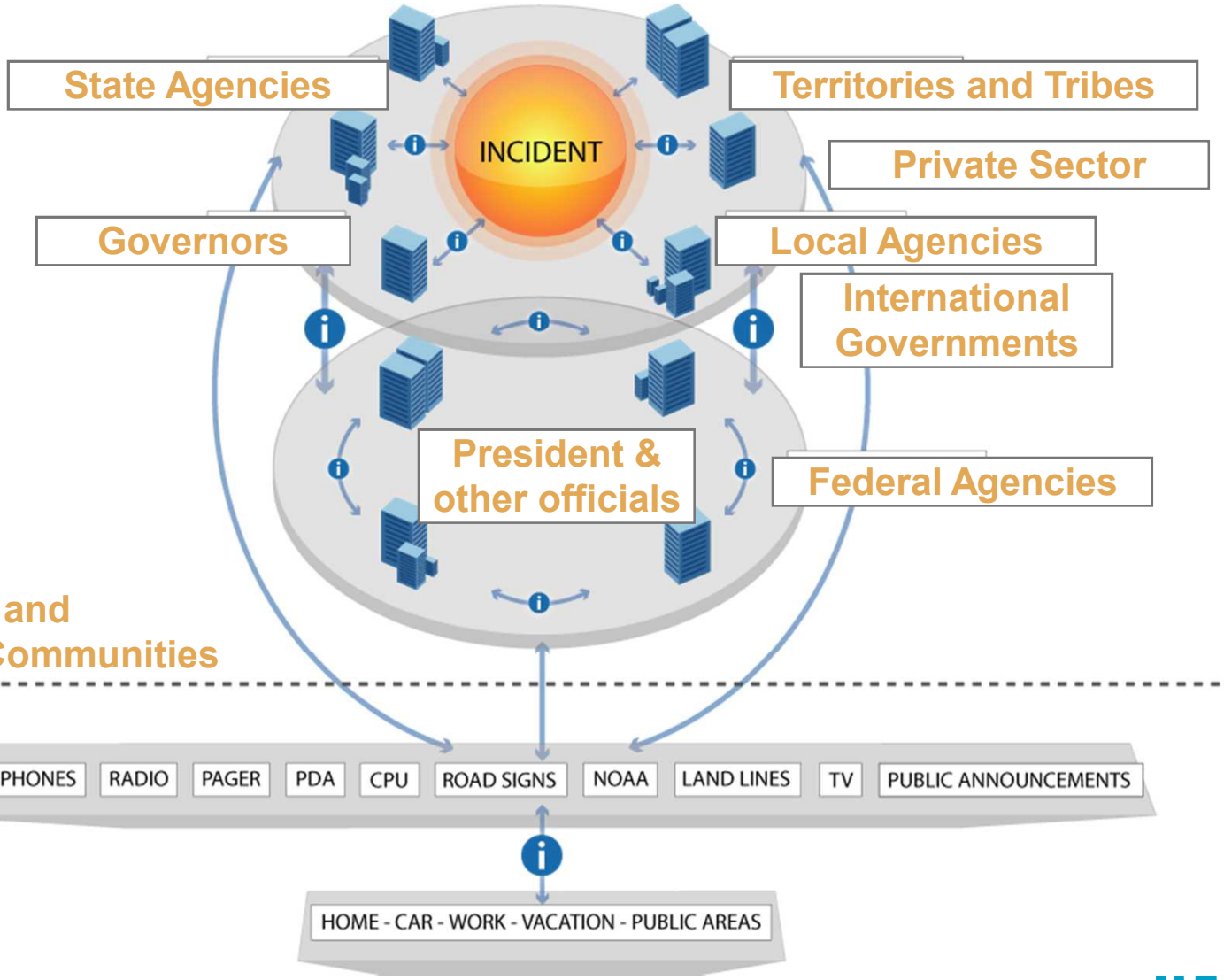
"DHS should establish an integrated public alert and warning system in coordination with all relevant departments and agencies."

- Hurricane Katrina Lessons Learned Report (2006)

* NOAA = National Oceanic and Atmospheric Administration
FCC = Federal Communications Commission
APTS = Association of Public Television Stations

Sandia National Laboratories

The end vision of IPAWS is to deliver coordinated messages over more channels to more people, anywhere, anytime.



Sandia National Laboratories

IPAWS Overview

IPAWS will transform the national Emergency Alert System (EAS)

Current EAS	IPAWS Goal
❖ 12% of listening population during the day ❖ 1% at night	❖ 85% of the listening population in 10 minutes
❖ Audio-only alerts, distributed via television and radio	❖ Voice, text, or video to all Americans, including those with disabilities or who cannot understand English

IPAWS Connecting Communities

How do we connect such independent, distributed sets of resources?

Federal Agencies

Authentication Boundary

Satellite and IP Network

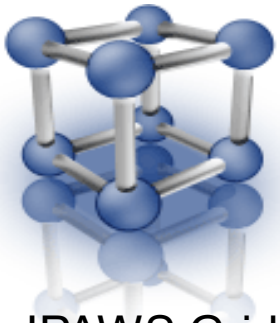
Internet & Landline Services

Authentication Boundary

Authentication Boundary

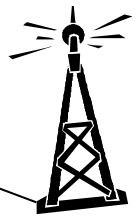
Local EOC

Authentication Boundary



IPAWS Grid

Authentication Boundary



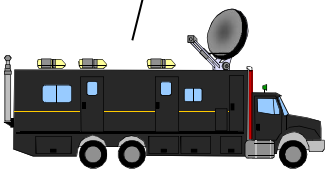
Radio

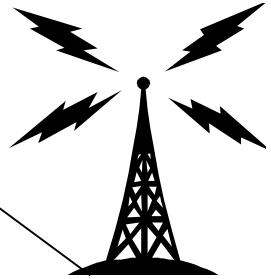
Authentication Boundary

Authentication Boundary

Authentication Boundary

State EOC





Television

Mobile IPAWS Coordination Center

Commercial Satellite Services

Commercial Mobile Services

Sandia National Laboratories

Sandia's Role

- **Design, set up, and operate pilot alert program for 2007 hurricane season**
  - Initial capability deployed 1 August 2007
- **Develop and pilot new architecture for next hurricane season**
  - Understand needs/requirements of users
  - Develop secure architecture for sending messages (internal/public)
  - Develop standards (OASIS*)
  - Certify vendors for interoperability
  - Multiple year effort to develop architecture and roll it out nationally

Sandia National Laboratories

* Organization for the Advancement of Structured Information Standards

Other areas of SNL R&D/expertise

- Data Analysis & Visualization
- Informatics
- Data Intensive Computing