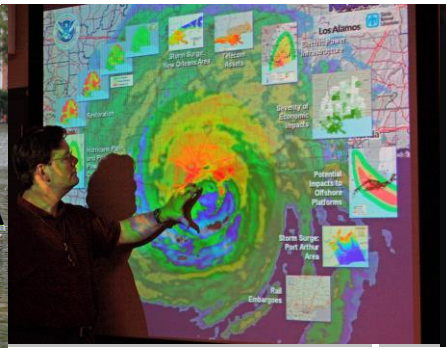
Exceptional service in the national interest

Sandia National Laboratories





Federally-funded R&D Centers: partners in cyber and infrastructure security

Lori Parrott

Sandia National Laboratories

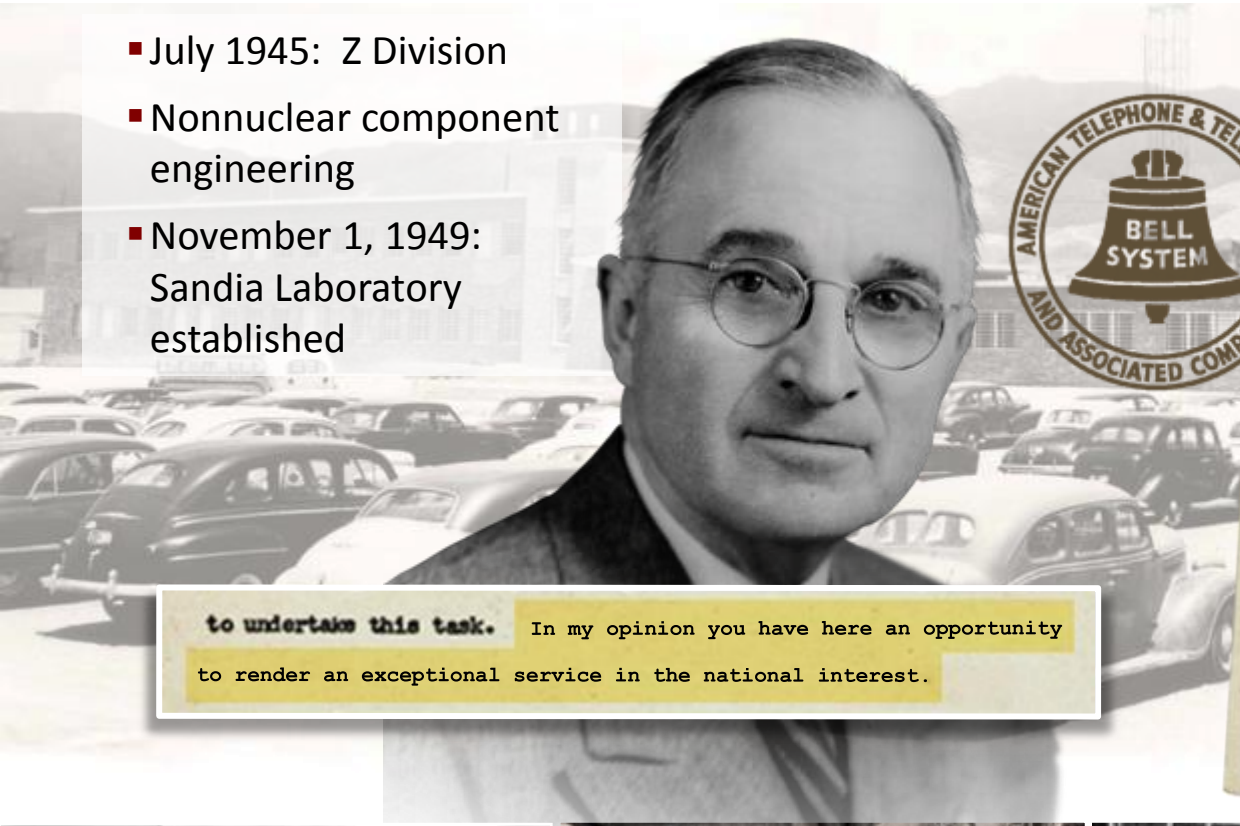
U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

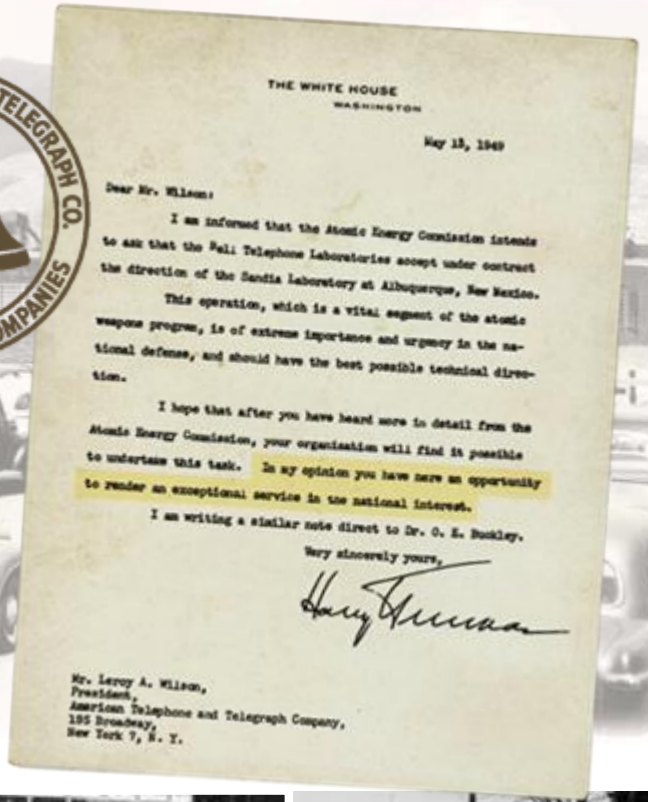
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Sandia's History

Exceptional service in the national interest

- July 1945: Z Division
- Nonnuclear component engineering
- November 1, 1949: Sandia Laboratory established





THE WHITE HOUSE
WASHINGTON

May 13, 1949

Dear Mr. Wilson:

I am informed that the Atomic Energy Commission intends to ask that the Bell Telephone Laboratories accept under contract the direction of the Sandia Laboratory at Albuquerque, New Mexico.

This operation, which is a vital segment of the atomic weapons program, is of extreme importance and urgency in the national defense, and should have the best possible technical direction.

I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

I am writing a similar note direct to Dr. C. E. Buckley.

Very sincerely yours,

Harry Truman

Mr. Leroy A. Wilson,
President,
American Telephone and Telegraph Company,
195 Broadway,
New York 7, N. Y.

to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

At a glance: 10,600 employees, 6 locations

Sandia National Laboratories

Albuquerque, New Mexico

Livermore, California

Kauai, Hawaii

Waste Isolation Pilot Plant, Carlsbad, New Mexico

Pantex Plant, Amarillo, Texas

Tonopah, Nevada

Energy & Climate

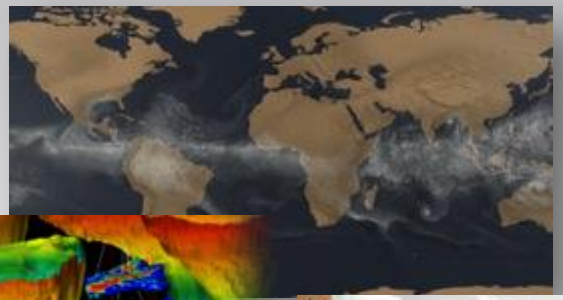
Sandia National Laboratories

Energy Research

ARPAe, BES Chem Sciences, ASCR, CINT, Geo Bio Science, BES Material Science

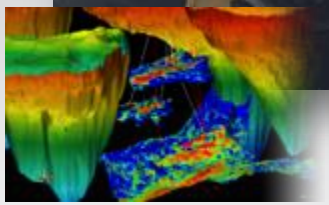
Climate & Environment

Measurement & Modeling, Carbon Management, Water & Environment, and Biofuels



Nuclear Energy & Fuel Cycle

Commercial Nuclear Power & Fuel, Nuclear Energy Safety & Security, DOE Managed Nuclear Waste Disposal

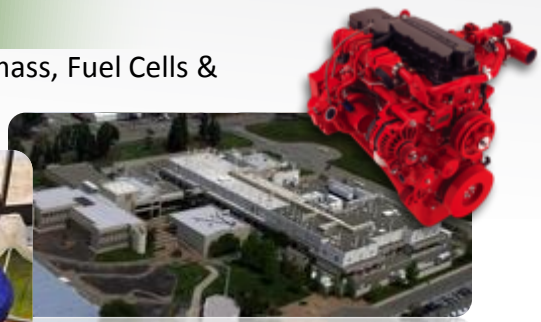


Renewable Systems & Energy Infrastructure

Renewable Energy, Energy Efficiency,
Grid and Storage Systems

Transportation Energy & Systems

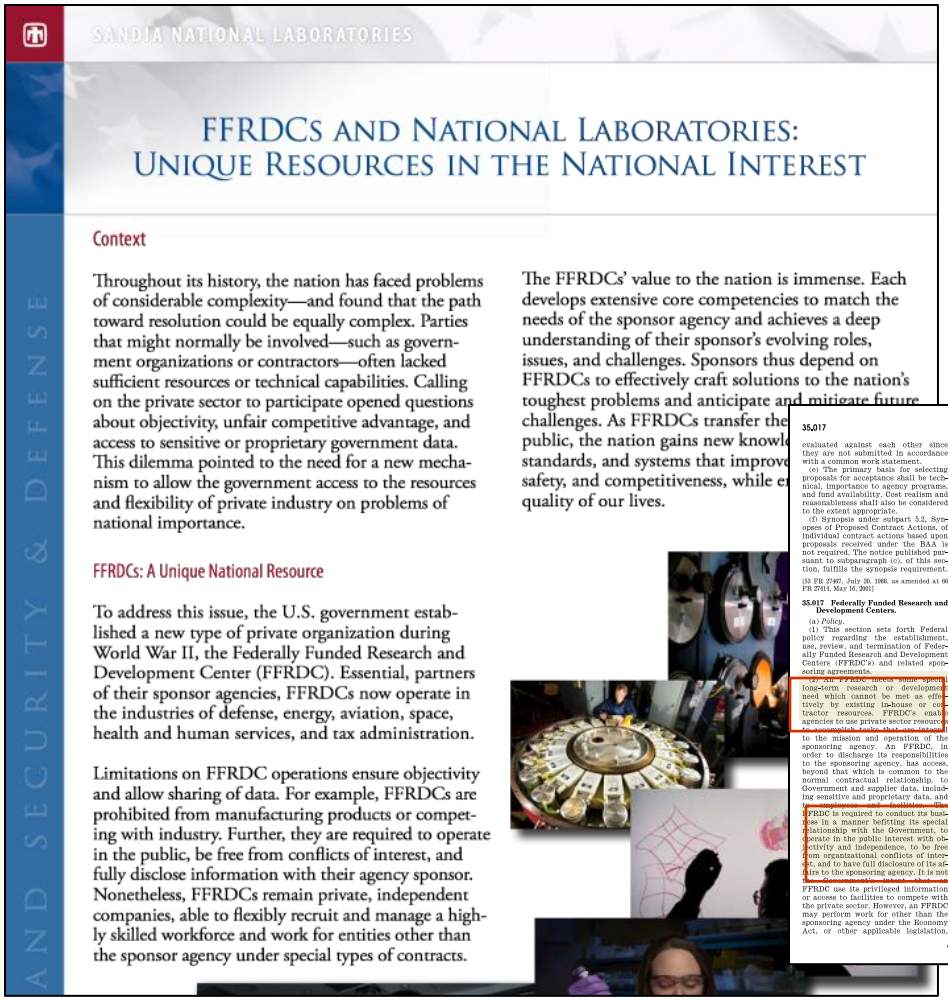
Vehicle Technologies, Biomass, Fuel Cells & Hydrogen Technology



International, Homeland, & Nuclear Security

Sandia National Laboratories

Federally Funded R&D Centers: unique resources for government, university, industry partnerships



SANDIA NATIONAL LABORATORIES

AND SECURITY & DEFENSE

FFRDCs AND NATIONAL LABORATORIES: UNIQUE RESOURCES IN THE NATIONAL INTEREST

Context

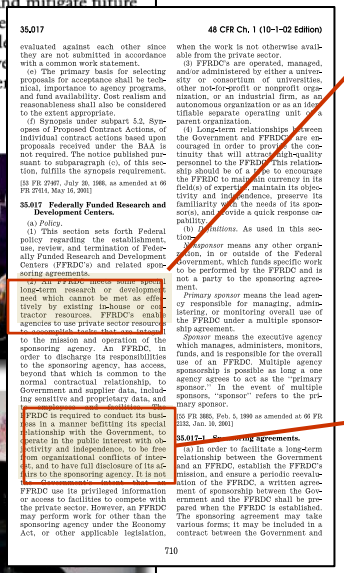
Throughout its history, the nation has faced problems of considerable complexity—and found that the path toward resolution could be equally complex. Parties that might normally be involved—such as government organizations or contractors—often lacked sufficient resources or technical capabilities. Calling on the private sector to participate opened questions about objectivity, unfair competitive advantage, and access to sensitive or proprietary government data. This dilemma pointed to the need for a new mechanism to allow the government access to the resources and flexibility of private industry on problems of national importance.

FFRDCs: A Unique National Resource

To address this issue, the U.S. government established a new type of private organization during World War II, the Federally Funded Research and Development Center (FFRDC). Essential, partners of their sponsor agencies, FFRDCs now operate in the industries of defense, energy, aviation, space, health and human services, and tax administration.

Limitations on FFRDC operations ensure objectivity and allow sharing of data. For example, FFRDCs are prohibited from manufacturing products or competing with industry. Further, they are required to operate in the public, be free from conflicts of interest, and fully disclose information with their agency sponsor. Nonetheless, FFRDCs remain private, independent companies, able to flexibly recruit and manage a highly skilled workforce and work for entities other than the sponsor agency under special types of contracts.

The FFRDCs' value to the nation is immense. Each develops extensive core competencies to match the needs of the sponsor agency and achieves a deep understanding of their sponsor's evolving roles, issues, and challenges. Sponsors thus depend on FFRDCs to effectively craft solutions to the nation's toughest problems and anticipate and mitigate future challenges. As FFRDCs transfer the public, the nation gains new knowl standards, and systems that improve safety, and competitiveness, while e quality of our lives.



35.017 48 CFR Ch. 1 (10–1–02 Edition)

evaluated against each other since they are not submitted in accordance with a common work statement.

(e) The primary basis for selecting proposals for acceptance shall be technical, importance to agency programs, and fund availability. Cost realism and reasonableness shall also be considered to the extent appropriate.

(f) Synopsis under subpart 5.2. Synopses of Proposed Contract Actions, of individual contract actions based upon proposals received under the BAA is not required. The notice published pursuant to subparagraph (c), of this section, fulfills the synopsis requirement.

[58 FR 27467, July 20, 1993, as amended at 66 FR 27464, May 16, 2001]

35.017 Federally Funded Research and Development Centers.

(a) *Policy.*

(1) This section sets forth Federal policy regarding the establishment, use, review, and termination of Federally Funded Research and Development Centers (FFRDC's) and related sponsoring agreements.

(2) An FFRDC meets some special long-term research or development need which cannot be met as effectively by existing in-house or contractor resources. FFRDC's enable agencies to use private sector resources to accomplish tasks that are integral to the mission and operation of the sponsoring agency. An FFRDC, in order to discharge its responsibilities to the sponsoring agency, has access, beyond that which is common to the normal contractual relationship, to Government and supplier data, including sensitive and proprietary data, and

(3) [illegible] FFRDC is required to conduct its business in a manner befitting its special relationship with the Government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency. It is not [illegible] FFRDC use its privileged information or access to facilities to compete with the private sector. However, an FFRDC may perform work for other than the sponsoring agency under the Economy Act, or other applicable legislation, when the work is not otherwise available from the private sector.

(3) FFRDC's are operated, managed, and/or administered by either a university or consortium of universities, other not-for-profit or nonprofit organization, or an industrial firm, as an autonomous organization or as an identifiable separate operating unit of a parent organization.

(4) Long-term relationships between the Government and FFRDC's are encouraged in order to provide the continuity that will attract high-quality personnel to the FFRDC. This relationship should be of a type to encourage the FFRDC to maintain currency in its field(s) of expertise, maintain its objectivity and independence, preserve its familiarity with the needs of its sponsor(s), and provide a quick response capability.

(b) *Definitions.* As used in this section—

Agency sponsor means any other organization, in or outside of the Federal Government, which funds specific work to be performed by the FFRDC and is not a party to the sponsoring agreement.

Primary sponsor means the lead agency responsible for managing, administering, or monitoring overall use of the FFRDC under a multiple sponsorship agreement.

Sponsor means the executive agency which manages, administers, monitors, funds, and is responsible for the overall use of an FFRDC. Multiple agency sponsorship is possible as long a one agency agrees to act as the "primary sponsor." In the event of multiple sponsors, "sponsor" refers to the primary sponsor.

[65 FR 2395, Feb. 5, 1999 as amended at 66 FR 2132, Jan. 10, 2001]

35.017–1 Sponsoring agreements.

(a) In order to facilitate a long-term relationship between the Government and an FFRDC, establish the FFRDC's mission, and ensure a periodic reevaluation of the FFRDC, a written agreement of sponsorship between the Government and the FFRDC shall be prepared when the FFRDC is established. The sponsoring agreement may take various forms; it may be included in a contract between the Government and

710

48 CFR 35.017 Federally Funded Research and Development Centers (1990)

"An FFRDC meets some special long-term research or development need which cannot be met as effectively by existing in-house or contractor resources."

"The FFRDC is required to conduct its business in a manner befitting its special relationship with the Government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency."

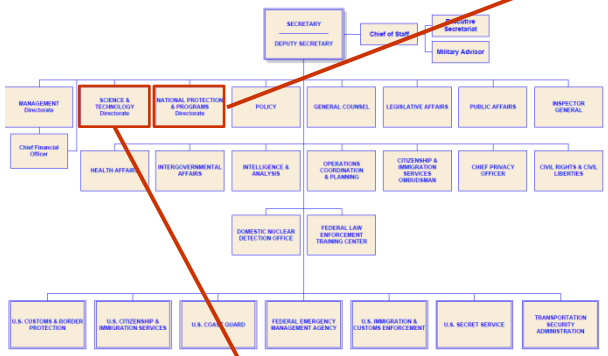
Sandia has a long history in “cyber” and information assurance.

- Significant impact on national cyber missions
  - Derivation from and complement to our NW activities
  - Multiple national sponsors
- History of providing adversarial threat assessment
  - U.S. nuclear command-and-control systems
  - Sandia’s enterprise & classified networks
- Synergy among research, programs, operations, and CI
- Sandia differentiators:
  - FFRDC: Does what industry/academia can’t, won’t, or shouldn’t
  - Deep understanding of the interplay between threats, vulnerabilities, and consequences
  - Systems perspective in contested environments
  - Key investments: Emulytics™, data sciences and machine learning, microelectronics design and fabrication, and materials

DHS cyber programs are concentrated in two areas: S&T and NPPD.

Sandia National Laboratories

DHS's cybersecurity mission:
Strengthening the security and resilience of cyberspace



National Protection and Programs Directorate (NPPD)

Office of Cybersecurity and Communications (CS&C)

- Network Security Deployment
- Federal Network Resilience
- National Cyber Communications Integration Center
- Stakeholder Engagement & Cyber Resilience
- [blank]

Sandia's role: Creation of national cyber capabilities

Science & Technology Directorate (S&T)

Homeland Security Advanced Research Projects Agency (HSARPA)

- [blank]
- Cyber Security
- [blank]
- [blank]

Sandia's role: R&D, red team assessments, and tech transfer support for Sandia-developed cyber technologies

Sandia helps DHS transition cybersecurity technologies to enterprise consumers

Sandia National Laboratories

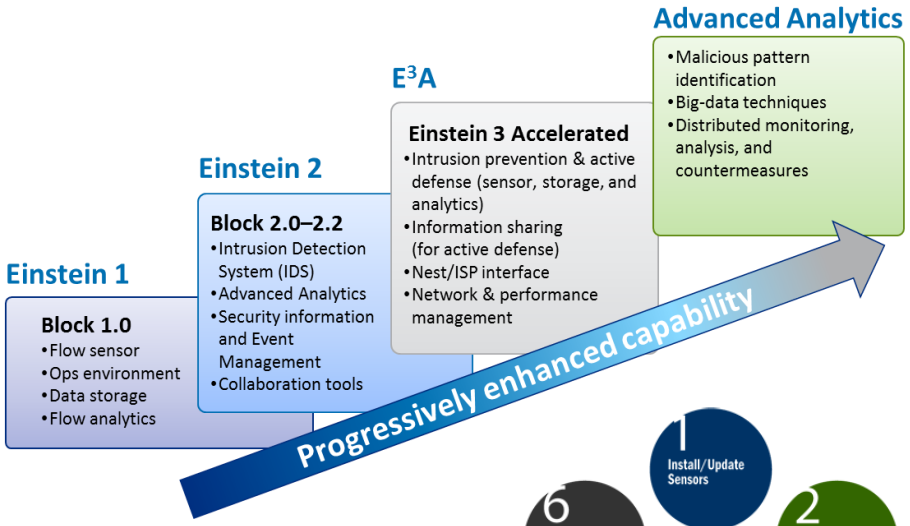
- Sandia helps the S&T Directorate commercialize cyber technologies through its Transition to Practice (TTP) program.
- Test and evaluate technologies from DOE national laboratories to help mature them and prepare them for commercialization.

CodeSeal: Tamper-proof trust anchors that protects critical software from malware and other security gaps

Sandia's NPPD work has focused on the National Cybersecurity Protection System.

DHS has deployed the National Cybersecurity Protection System (NCPS).

- Focus on
  - Detection
  - Analytics
  - Information sharing
  - Prevention/response to cyber threats
- Delivery through
  - Einstein (E^3A)
  - Continuous Diagnostics and Mitigation (CDM)
  - Enhanced Cybersecurity Services (ECS)



CDM process

Cyber security and information assurance activities support DHS's mission of securing government and critical infrastructures

Sandia National Laboratories

- **Supply Chain Risk Management (SCRM)**
  - Develop risk assessment tools; conduct risk- and vulnerability-assessments; develop risk mitigation strategies; threat analysis
  - Identify and evaluate risks for CFIUS studies
- **Continuous Diagnostics & Mitigation (CDM)**
  - Evaluate performance impacts of cloud/mobile computing on various CDM solutions; propose improvements
  - Analyze Trusted Internet Connections (TIC) for vulnerabilities and performance improvements
- **Control Systems Security**
  - Develop and implement firmware analysis toolkits
  - Perform incident analysis of control logic and firmware
  - Provide specialized incident response and training
- **Transition government technology solutions to commercial entities**
  - Independent assessments and evaluations of government developed tools and solutions
  - Demonstrate CODESEAL technology to armor security functions against reverse engineering

Sandia's efforts are enabling cybersecurity for critical infrastructure.

Sandia National Laboratories

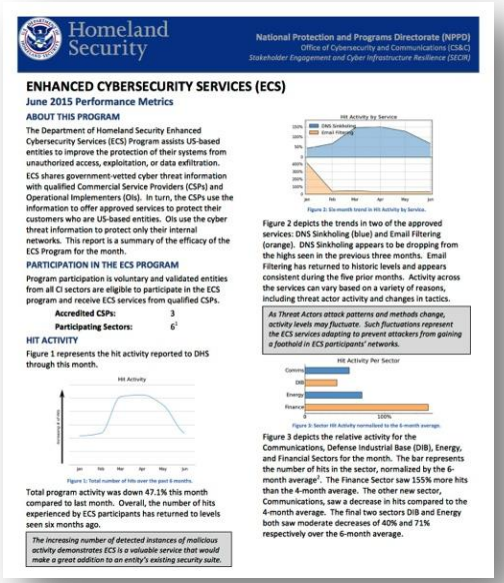
Securing Critical Infrastructure Control Systems

- Developing deep technical capabilities for Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Device-level analysis toolkits for reverse-engineering behavior and discovering vulnerabilities

SIEMENS SCADA device

Enhanced Cybersecurity Services

- Supporting senior DHS leadership by assessing the effectiveness (e.g., threats discovered/blocked) of ECS capabilities
- Aiding outreach to critical infrastructure owners/operators to increase voluntary participation



Homeland Security

National Protection and Programs Directorate (NPPD)
Office of Cybersecurity and Communications (CS&C)
Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR)

ENHANCED CYBERSECURITY SERVICES (ECS)

June 2015 Performance Metrics

ABOUT THIS PROGRAM

The Department of Homeland Security Enhanced Cybersecurity Services (ECS) Program assists US-based entities to improve the protection of their systems from unauthorized access, exploitation, or data exfiltration.

ECS shares government-vetted cyber threat information with qualified Commercial Service Providers (CSPs) and Operational Implementers (OIs). In turn, the CSPs use the information to offer approved services to protect their customers who are US-based entities. OIs use the cyber threat information to protect only their internal networks. This report is a summary of the efficacy of the ECS Program for the month.

PARTICIPATION IN THE ECS PROGRAM

Program participation is voluntary and validated entities from all CI sectors are eligible to participate in the ECS program and receive ECS services from qualified CSPs.

Accredited CSPs:	3
Participating Sectors:	6

HIT ACTIVITY

Figure 1 represents the hit activity reported to DHS through this month.

Hit Activity

Figure 1: Total number of hits over the past 6 months.

Total program activity was down 47.1% this month compared to last month. Overall, the number of hits experienced by ECS participants has returned to levels seen six months ago.

The increasing number of detected instances of malicious activity demonstrates ECS is a valuable service that would make a great addition to an entity's existing security suite.

Hit Activity by Service

Figure 2: Six-month trend in Hit Activity by Service.

Figure 2 depicts the trends in two of the approved services: DNS Sinkholing (blue) and Email Filtering (orange). DNS Sinkholing appears to be dropping from the highs seen in the previous three months. Email Filtering has returned to historic levels and appears consistent during the five prior months. Activity across the services can vary based on a variety of reasons, including threat actor activity and changes in tactics.

As Threat Actors attack patterns and methods change, activity levels may fluctuate. Such fluctuations represent the ECS services adapting to prevent attackers from gaining a foothold in ECS participants' networks.

Hit Activity Per Sector

Comm.
DIB
Energy
Finance
100%

Figure 3: Sector Hit Activity normalized to the 6-month average.

Figure 3 depicts the relative activity for the Communications, Defense Industrial Base (DIB), Energy, and Financial Sectors for the month. The bar represents the number of hits in the sector, normalized by the 6-month average[2]. The Finance Sector saw 155% more hits than the 4-month average. The other new sector, Communications, saw a decrease in hits compared to the 4-month average. The final two sectors DIB and Energy both saw moderate decreases of 40% and 71% respectively over the 6-month average.

Sandia's cross-cutting capabilities and infrastructure are advancing DHS's cyber mission.

Sandia National Laboratories

Emulating the NCPS

- Existing gap: At-scale test environment for evaluating new cybersecurity approaches and technologies to inform NCPS investments
- Sandia effort: Extending Emulytics™ platform to model the NCPS with enough fidelity to try out new technologies and approaches
  - Applying this to exploratory efforts (e.g., key escrow), and technology evaluations (e.g., countermeasures)

SCIF Space

- In process of leasing SCIF space in close proximity to DHS/NPPD/CS&C
- Will support ~8 detailees and cooperative R&D with DHS and other labs/contractors

National Infrastructure Simulation and Analysis Center

NISAC Modeling and Analysis Goals

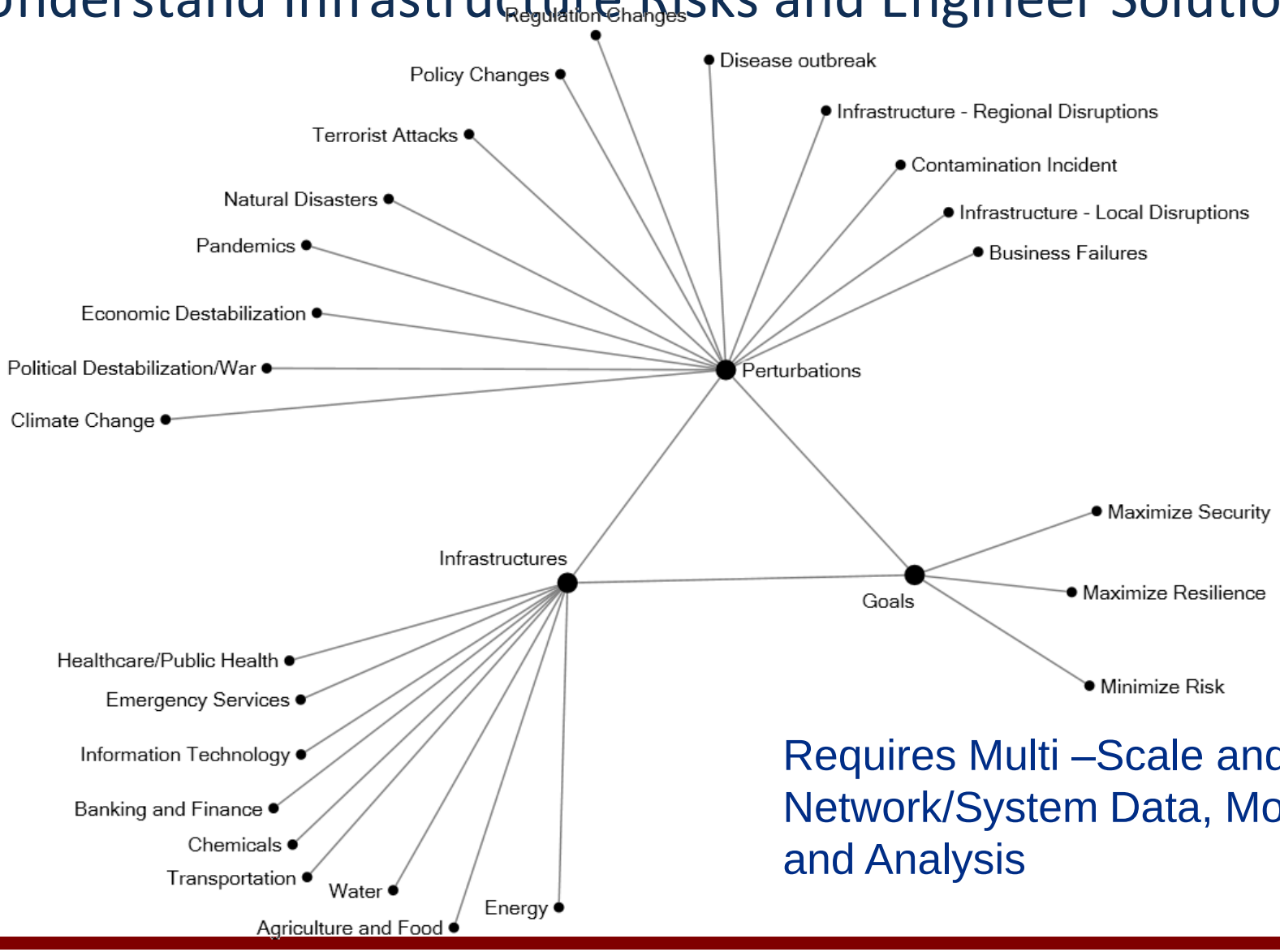
Sandia National Laboratories

Provide fundamentally new modeling and simulation capabilities for the analysis of critical infrastructures, their interdependencies, vulnerabilities, and complexities

Aiding decision makers with

- *policy assessment,*
- *mitigation planning,*
- *education & training,*
- *near real-time assistance to crisis response organizations*

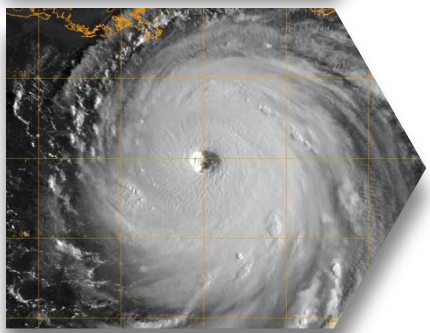
Long-term Applied Research Goal: Understand Infrastructure Risks and Engineer Solutions

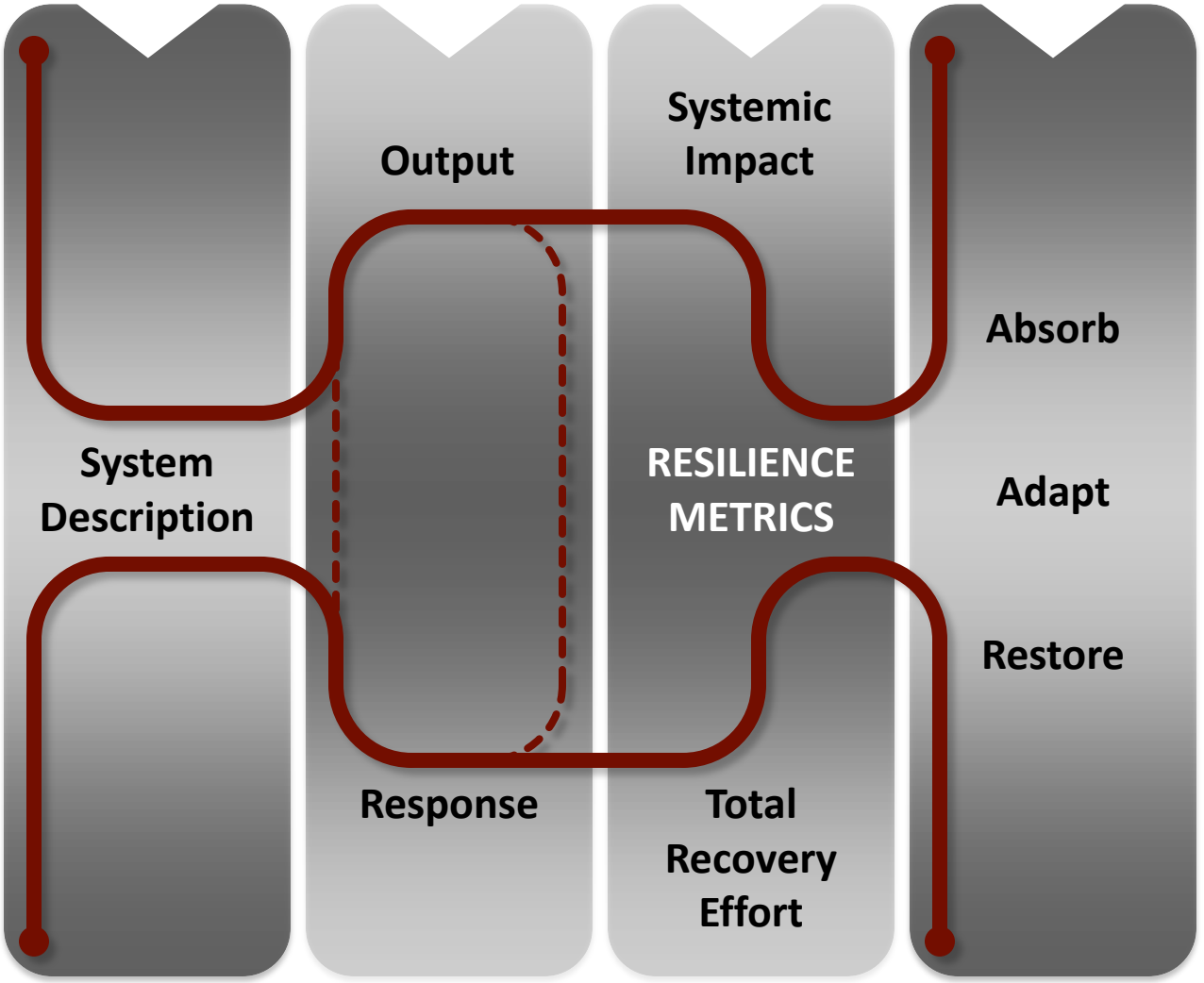


Requires Multi –Scale and Multi-Network/System Data, Modeling and Analysis

Infrastructure Resilience Analysis Methodology provides a Quantitative approach for assessing and improving resilience.

Sandia National Laboratories



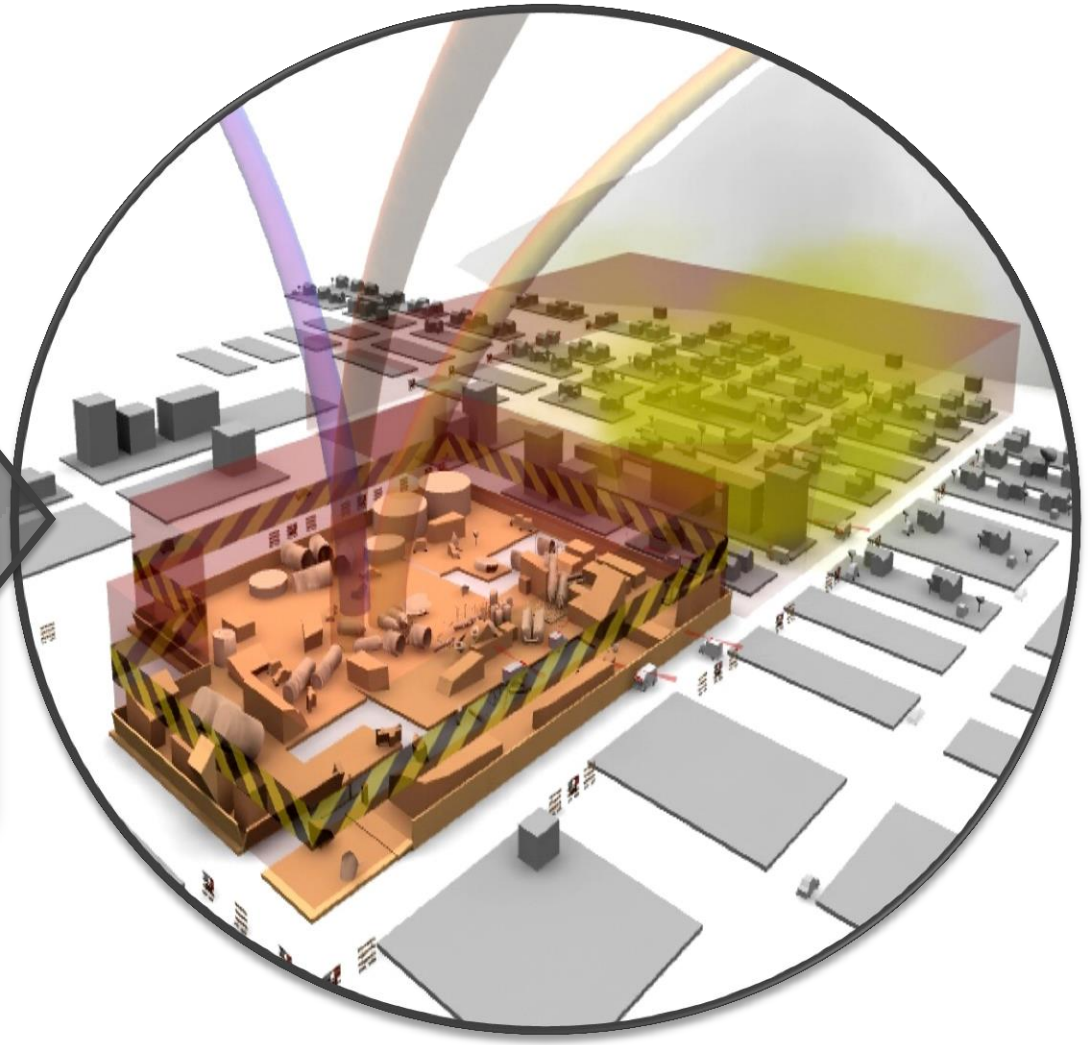


Chemical Criticality estimates the regional and national-level economic impacts of a terrorist attack at a single chemical facility.

Sandia National Laboratories

Sandia's work helps DHS answer these questions…

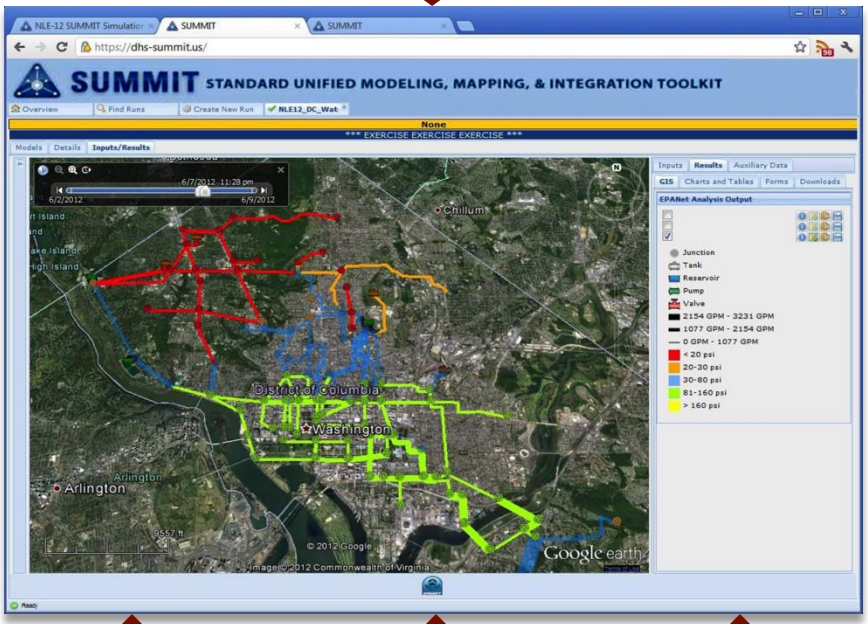
- **What is an economically critical chemical facility?**
- **Can a chemical incident cause significant economic impacts?**
- **Should DHS regulate chemical facilities based on their economic criticality?**



Drinking Water Resilience Project will provide water infrastructure risk and prioritization at the regional and national level supporting DHS emergency situational awareness.

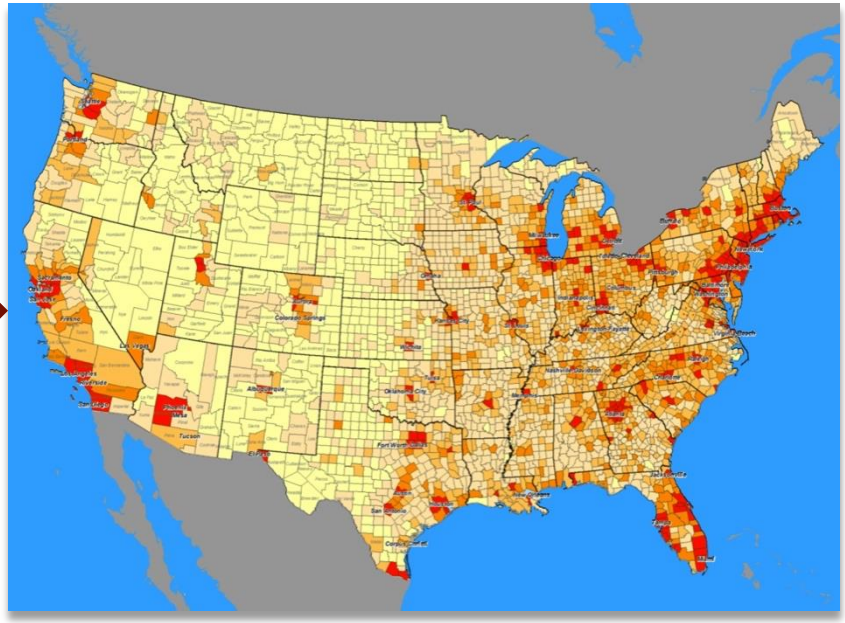
Sandia National Laboratories

Water Utility Inputs for Local Risk Assessments



J100 Engine | **Database** | **Supporting Models & Data**

Infrastructure Prioritization for Regional and National Risk Assessments



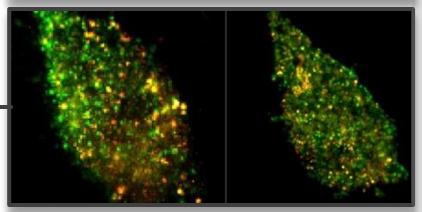
Resilient Cities provides technical expertise to help cities better address the shocks and stresses of the 21st Century.

Sandia National Laboratories

SYSTEM-specific

- Energy
- Water
- Transportation
- Medical
- Food




SHOCKS

Building Disaster
Disease Outbreak
Earthquake
Fire
Flooding
Heat Wave
Hurricane
Landslide
Terrorism
Torrential Rain
Transit Disaster
Violent Protest

STRESSES

Coastal Erosion
Crime
Education
Emigration
Energy Supply/Demand
Food Supply
Immigration
Inequality
Sea Level Rise
Sinking Lands
Unemployment
Waste
Water Safety

CROSS-cutting




- City Critical Function Assessment
- All Shocks & Stresses Risk Assessment
- Human Resilience Analysis
- Emergency Response Exercises / Optimization

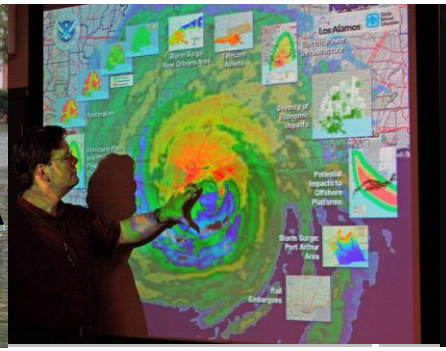
Sandia's programs for cyber and infrastructure security

- **Commitment to the mission**
  - *commitment to prime sponsors and national service*
  - *FFRDC charter of objectivity, independence*
- **Patient intellectual capital**
  - *Continuity of expertise*
- **Anticipation of national needs**
  - *mission-focused research*
- **Facilities to address long-term, large scale problems**
- **Trusted advisor roles:**
  - *sensitive (industry or classified) information*

Exceptional service in the national interest

Sandia National Laboratories





For more information:

- *NISAC: http://www.sandia.gov/nisac/*
- *Resilience and Complex Systems: www.sandia.gov/casosengineering/resilience.html*
- *Cyber Security: www.sandia.gov/missions/defense_systems/cybersecurity.html*

Lori.parrott@sandia.gov

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

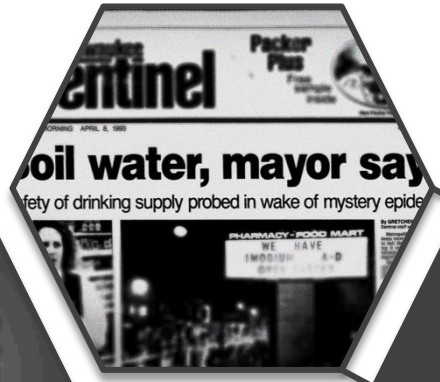
Backups/unused

Sandia National Laboratories

Sandia National Laboratories

Chemical Criticality

DHS/Infrastructure Security Compliance Division (ISCD)

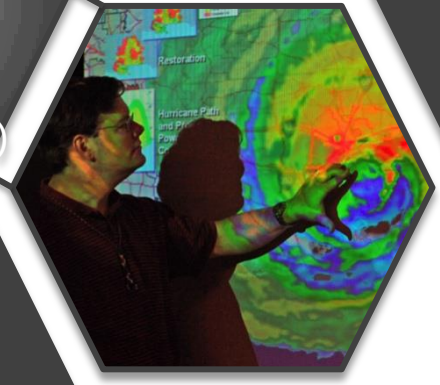


NISAC

DHS/Office of Cyber & Infrastructure Analysis (OCIA)

Drinking Water Resilience Project

DHS/Science & Technology (S&T)



Infrastructure Resilience

DHS/Science & Technology (S&T)

Resilient Cities

SNL/DOE

Tobacco Regulatory Support

FDA/Center for Tobacco Products (CTP)

Sandia National Laboratories

Chemical Criticality

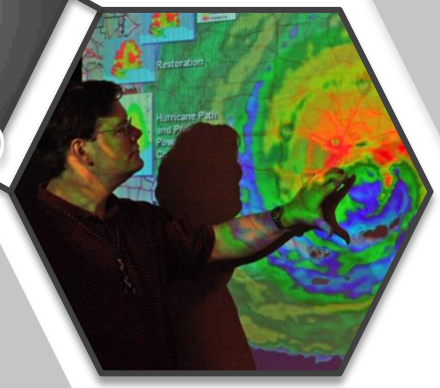
DHS/Infrastructure Security Compliance Division (ISCD)

Drinking Water Resilience Project

DHS/Science & Technology (S&T)

NISAC

DHS/Office of Cyber & Infrastructure Analysis (OCIA)



Infrastructure Resilience

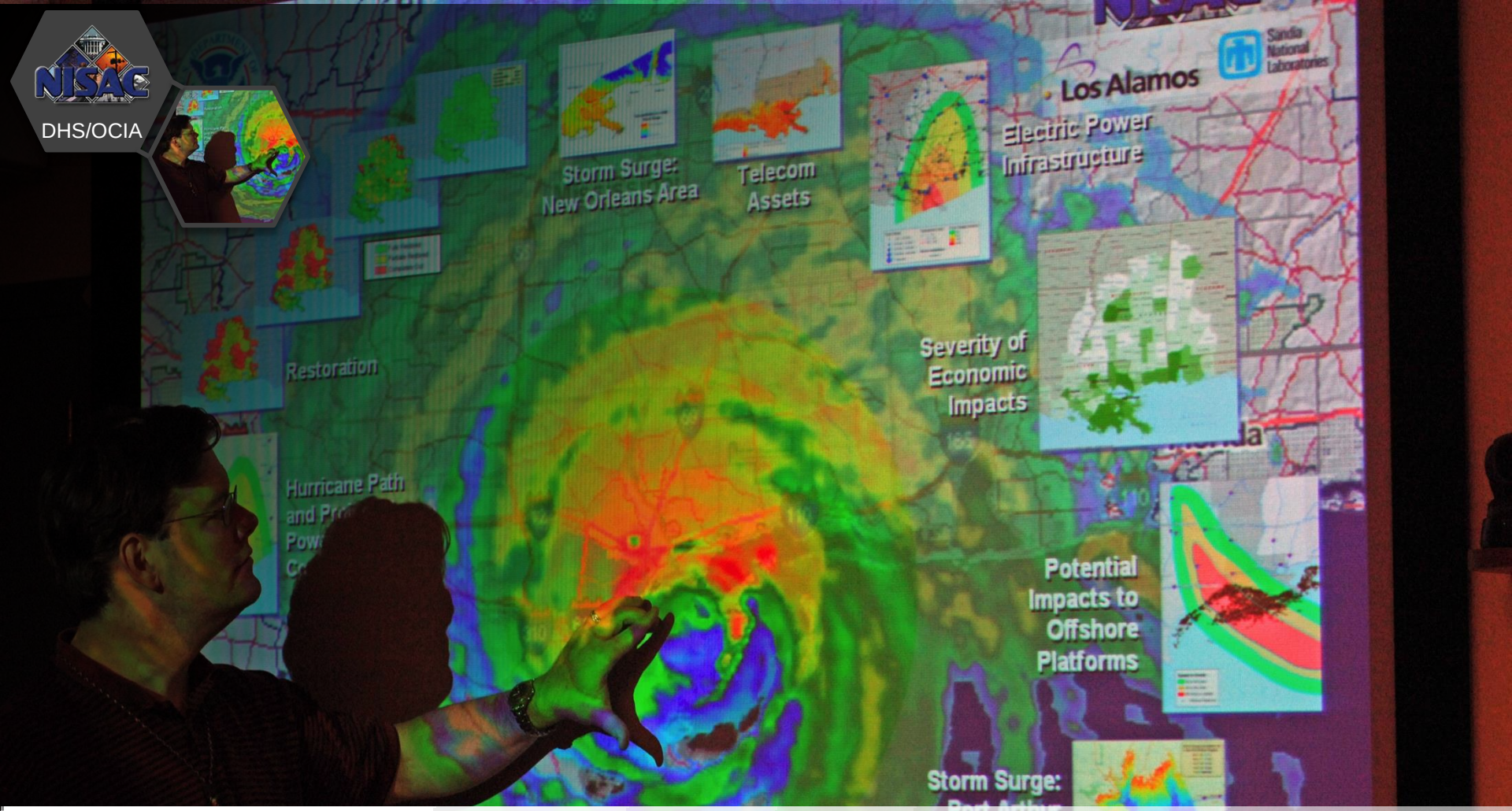
DHS/Science & Technology (S&T)

Resilient Cities

SNL/DOE

Tobacco Regulatory Support

FDA/Center for Tobacco Products (CTP)



Hurricane Katrina 2005

- **NISAC provided comprehensive and integrated situational awareness to the White House, DHS, and the federal government**
- **A computer network was developed to assist evacuees at the Houston Astrodome to locate family members**
- **A computer server was used to help map safe convoy routes during the evacuation**
- **NISAC provided technical expertise in economic analyses and continues to lead a multi-lab effort looking at water decontamination issues in New Orleans**

Sandia National Laboratories

Chemical Criticality

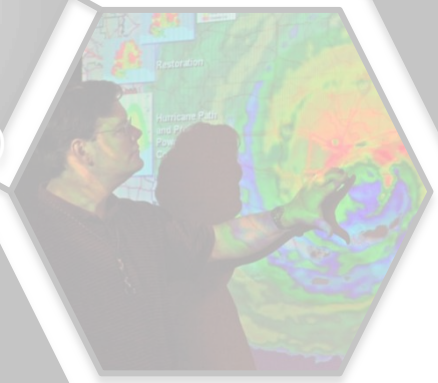
DHS/Infrastructure Security Compliance Division (ISCD)

NISAC

DHS/Office of Cyber & Infrastructure Analysis (OCIA)

Drinking Water Resilience Project

DHS/Science & Technology (S&T)



Infrastructure Resilience

DHS/Science & Technology (S&T)

Resilient Cities

SNL/DOE

Tobacco Regulatory Support

FDA/Center for Tobacco Products (CTP)

West, TX Chemical Plant Explosion 2013

West Fertilizer Company building was destroyed, 60–80 homes destroyed, 50–75 homes damaged, 50-unit apartment building destroyed, West Middle School damaged, 16 deaths, 160 injuries.

Norfolk, VA Flooding 2015

Hampton Roads area had major tidal flooding, water levels built to about six feet at high tide. Sandia worked with Norfolk as a test-bed to showcase resilience analysis capabilities for flooding.

Sandia National Laboratories

Chemical Criticality

DHS/Infrastructure Security Compliance Division (ISCD)

NISAC

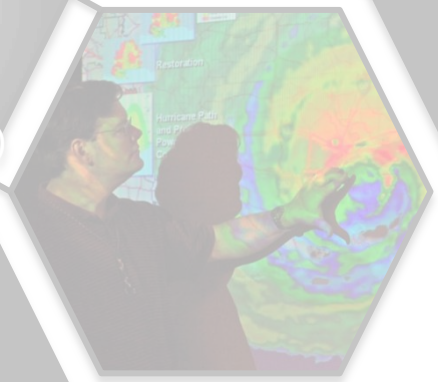
DHS/Office of Cyber & Infrastructure Analysis (OCIA)

Drinking Water Resilience Project

DHS/Science & Technology (S&T)

Infrastructure Resilience

DHS/Science & Technology (S&T)



Resilient Cities

SNL/DOE

Tobacco Regulatory Support

FDA/Center for Tobacco Products (CTP)

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

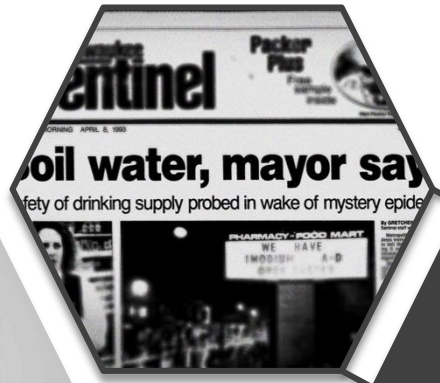
Sandia National Laboratories

Chemical Criticality

DHS/Infrastructure Security Compliance Division (ISCD)

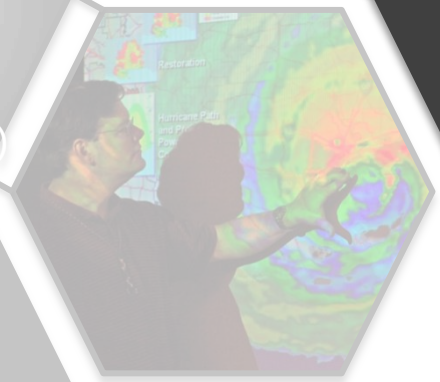
NISAC

DHS/Office of Cyber & Infrastructure Analysis (OCIA)



Drinking Water Resilience Project

DHS/Science & Technology (S&T)



Infrastructure Resilience

DHS/Science & Technology (S&T)

Resilient Cities

SNL/DOE

Tobacco Regulatory Support

FDA/Center for Tobacco Products (CTP)

Sandia National Laboratories

Chemical Criticality

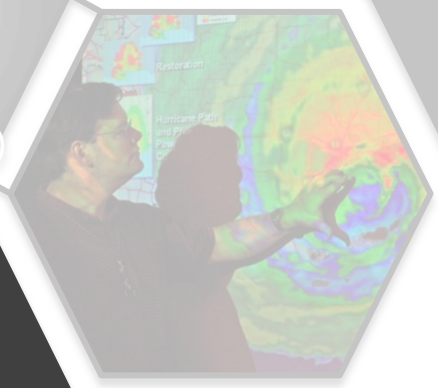
DHS/Infrastructure Security Compliance Division (ISCD)

NISAC

DHS/Office of Cyber & Infrastructure Analysis (OCIA)

Drinking Water Resilience Project

DHS/Science & Technology (S&T)



Infrastructure Resilience

DHS/Science & Technology (S&T)

Resilient Cities

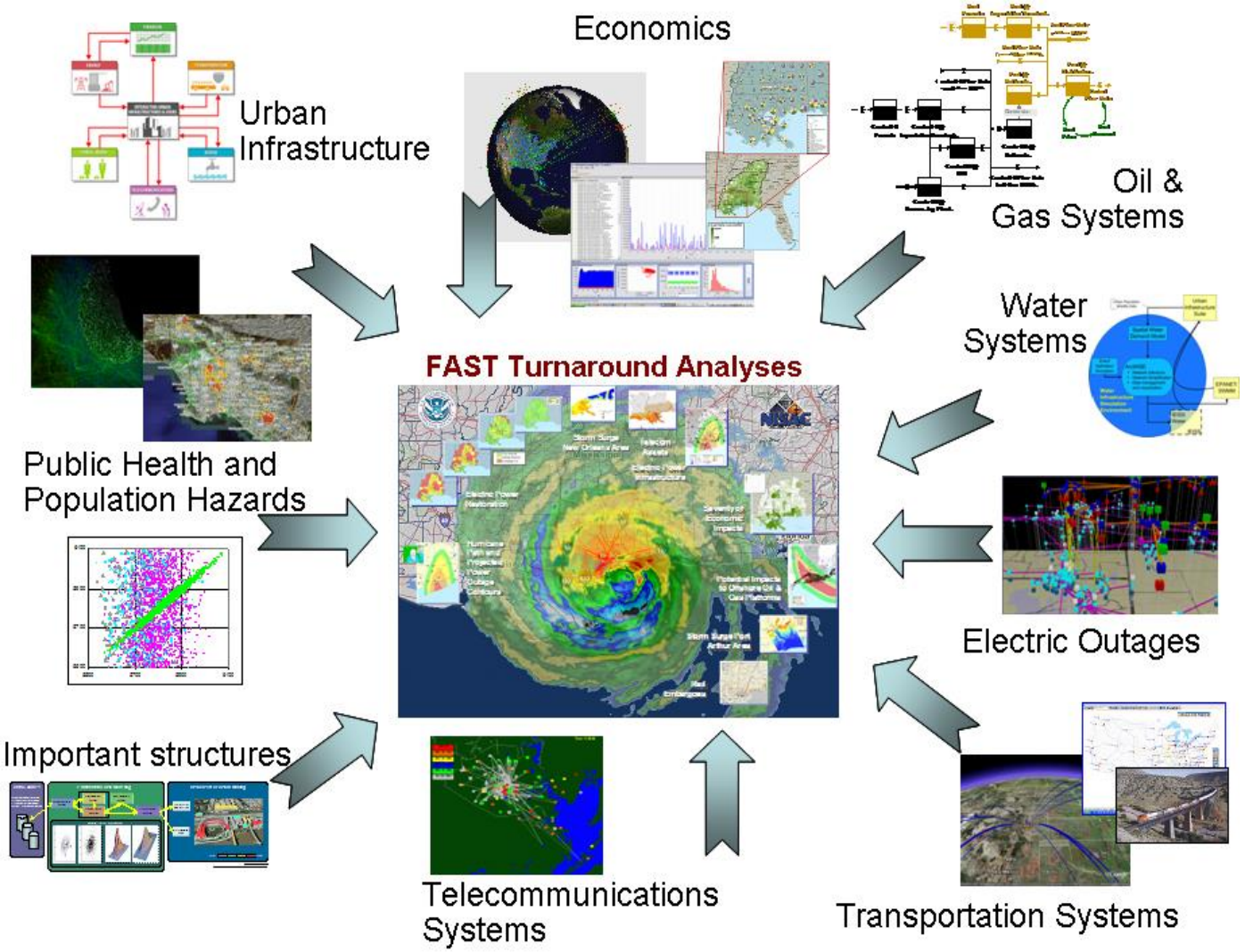
SNL/DOE

Tobacco Regulatory Support

FDA/Center for Tobacco Products (CTP)

Integration of Multidisciplinary Skill Sets & Expertise

Sandia National Laboratories



Infrastructure
Resilience
DHS/S&T

Hurricane Sandy 2012

A power outage resulted in a 200 patient evacuation from NYU Langone Medical Center in New York City – Sandia developed a systems-based model called "Hospital Evacuation during Infrastructure Disruptions" to prevent a repeat scenario.