SAND2015-10336PE

Exceptional service in the national interest

Sandia National Laboratories

11/24/2015

NSTAC Big Data Analysis Subcommittee

National Cyber Defense High Performance Computing & Analysis: Concepts, Planning and Roadmap

Sandia Report SAND2010-4766, Unlimited Release, Printed September 2010

Curtis M Keliiaa, Jason R. Hamlet

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

Introduction to SNL

U.S. DEPARTMENT OF ENERGY

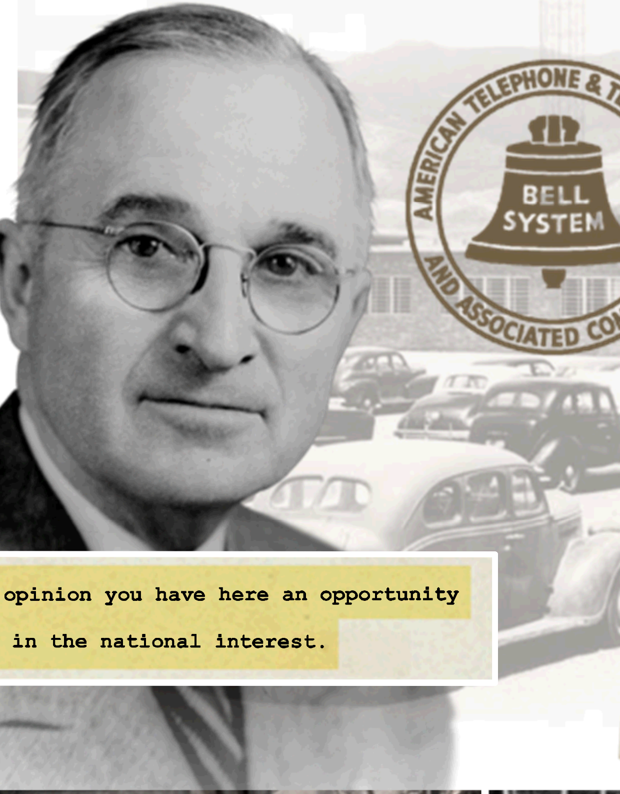
NNSA National Nuclear Security Administration

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

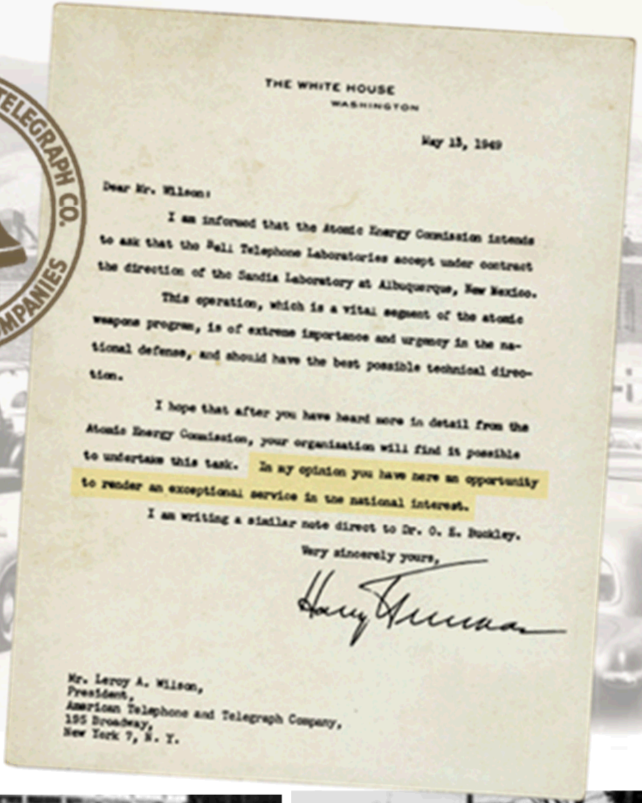
Sandia’s History

Exceptional service in the national interest

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



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



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.

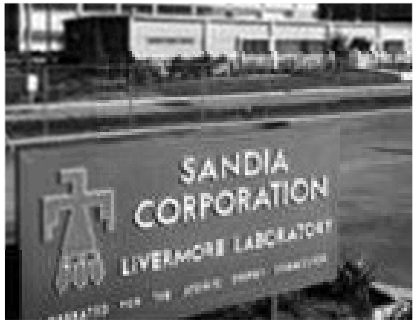
I hope that after you have heard more in detail from the Atomic Energy Commission, your organization will find it possible to undertake this task. In my opinion you have here an opportunity to render an exceptional service in the national interest.

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

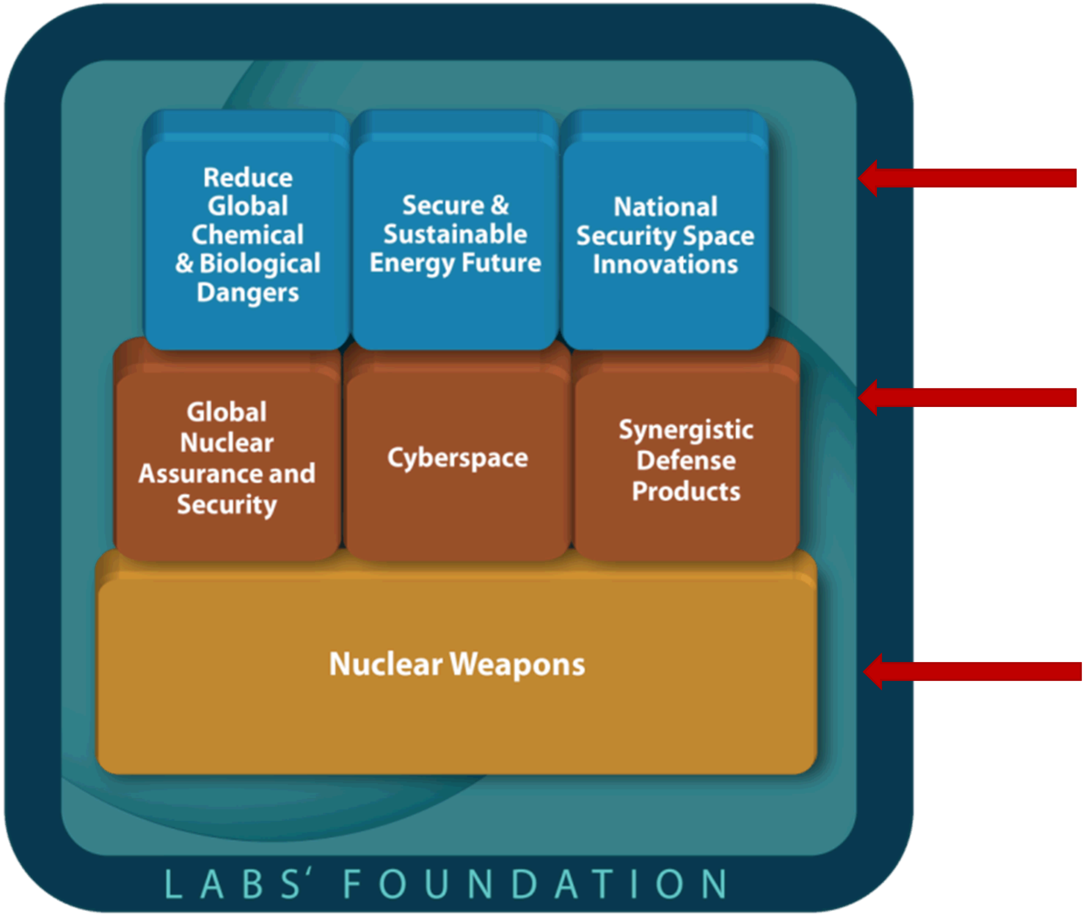
Very sincerely yours,

Harry Truman

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



National Security Mission Areas


Reduce Global Chemical & Biological Dangers
Secure & Sustainable Energy Future
National Security Space Innovations
Global Nuclear Assurance and Security
Cyberspace
Synergistic Defense Products
Nuclear Weapons
LABS' FOUNDATION

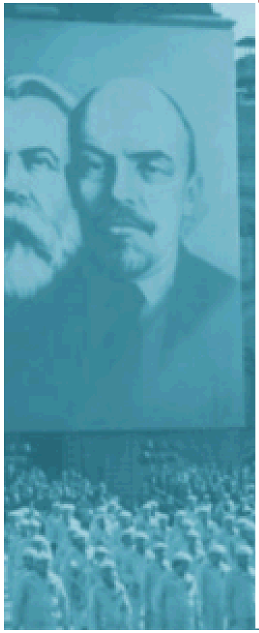
- Top row: Critical to our national security, these three mission areas leverage, enhance, and advance our capabilities.
- Middle row: Strongly interdependent with NW, these three mission areas are essential to sustaining Sandia's ability to fulfill its NW core mission.
- Bottom row: Our core mission, nuclear weapons (NW), is enabled by a strong scientific and engineering foundation.

Sandia Addresses National Security Challenges

1950s

Nuclear weapons

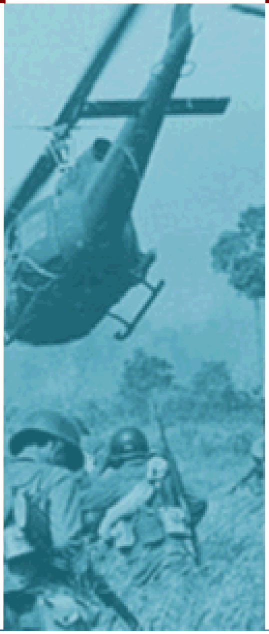
Production and manufacturing engineering



1960s

Development engineering

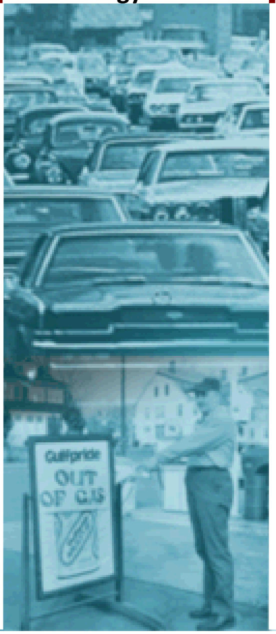
Vietnam conflict



1970s

Multiprogram laboratory

Energy crisis



1980s

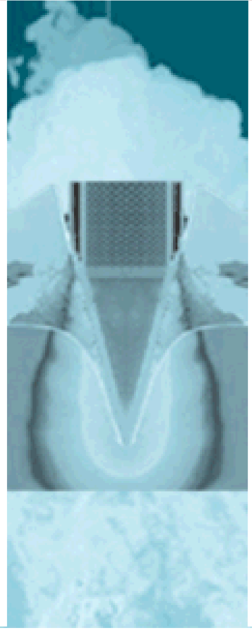
Missile defense work

Cold War

1990s

Post–Cold War transition

Stockpile stewardship



2000s

START
Post 9/11

National security

2010s

LEPs
Cyber, biosecurity proliferation

Evolving national security challenges

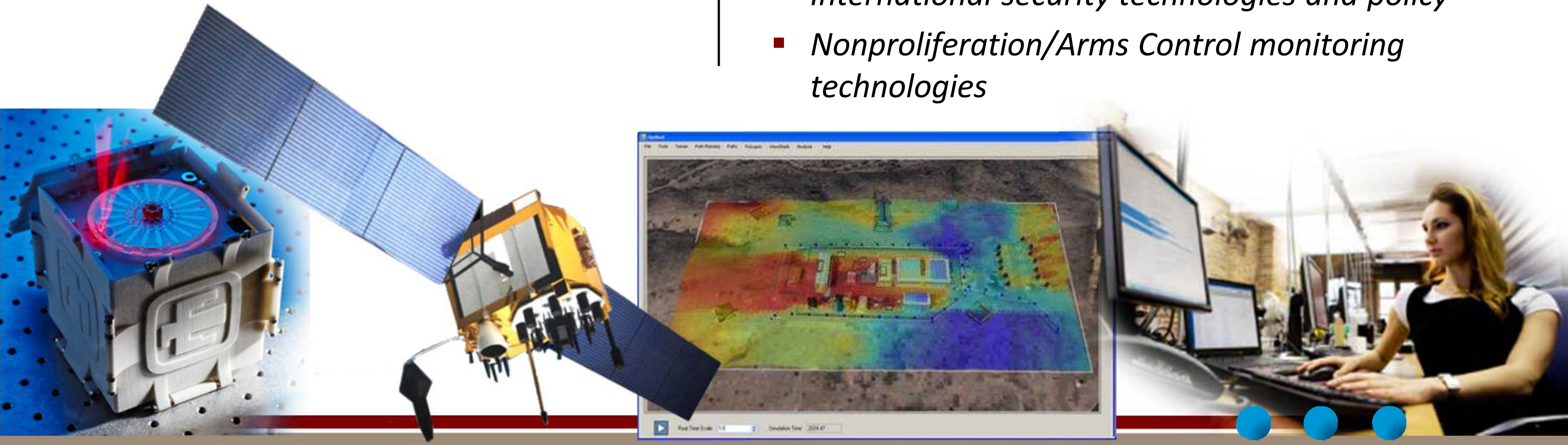
International, Homeland, and Nuclear Security

Program Areas

- Global Security
- IHNS Remote Sensing & Verification
- WMD Counterterrorism and Response
- Homeland Security
- Cyber and Infrastructure Security
- Homeland Defense and Force Protection

Capabilities

- *Nuclear, radiological, biological, explosives, and chemical science and engineering*
- *System analysis, engineering, and integration*
- *Physical and cyber security methods, technologies, and systems*
- *Predictive modeling and simulation of interdependent systems*
- *Decontamination and restoration approaches and technologies*
- *International security technologies and policy*
- *Nonproliferation/Arms Control monitoring technologies*



Current Sandia Activities

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

High Performance Computing

Funding profiles for Scientific Computing at Sandia:

1. NNSA Advanced Simulation and Computing (ASC)
2. Institutional Computing program
3. DOE Office of Science, Advanced Scientific Computing Research (ASCR)

ASC Tri-Lab Networks/Systems at SNL, LANL and LLNL:

- Continuous Access to Large Compute Systems
- Over 3 Petaflops + 4 Security Environments + Over 1.3B Processor Hrs/Yr

Operations:

- Scientific Computing Platforms – Cielo, Trinity, Sequoya, Sierra
- System Acquisition, Maintenance & Operations
- High Speed Parallel File Systems
- High Performance Parallel Networks
- Multi-Petabyte Data Archive Systems
- Facilities Improvements
- User Support Personnel
- Analysts & Code Development

Sandia National Laboratories

Exceptional service in the national interest

U.S. DEPARTMENT OF ENERGY

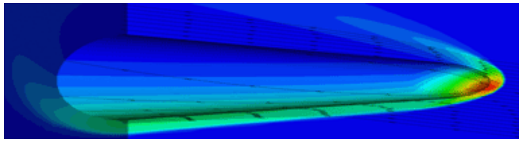
NNSA National Nuclear Security Administration

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

Center for Computing Research

Cybersecurity research focused on cross-cutting challenges and enabling capabilities:

- Streaming algorithms to process large data streams
- Algorithms to find patterns in large graphs
- Machine learning techniques to detect adversarial behavior (e.g. phishing emails)
- Quantum Information Systems
- Cognitive Science
- Neural Networks
- Cyber Emulytics
- Exascale Computing
- Remote sensing challenges
- Cybersecurity Engineering Research Institute (CERI) Collaboration with Industry and Academia



Sandia National Laboratories

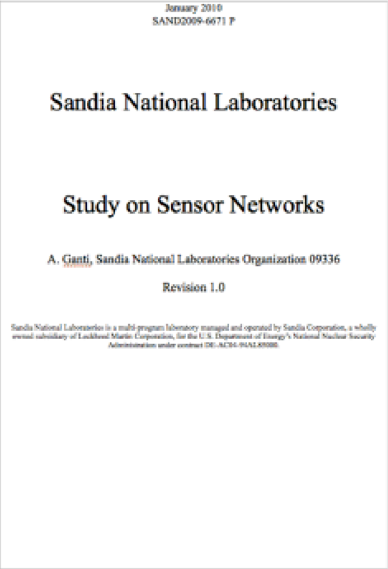
Exceptional service in the national interest

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

2010 Report Progression



January 2010
SAND2009-6671 P

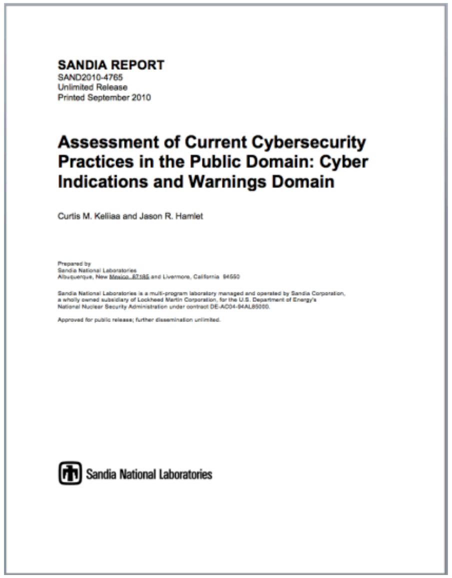
Sandia National Laboratories

Study on Sensor Networks

A. Ganti, Sandia National Laboratories Organization 09336

Revision 1.0

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.



SANDIA REPORT
SAND2010-4765
Unlimited Release
Printed September 2010

Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain

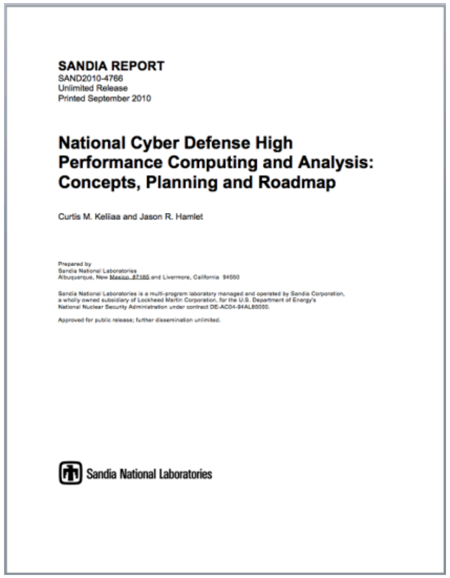
Curtis M. Keliiaa and Jason R. Hamlet

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories



SANDIA REPORT
SAND2010-4766
Unlimited Release
Printed September 2010

National Cyber Defense High Performance Computing and Analysis: Concepts, Planning and Roadmap

Curtis M. Keliiaa and Jason R. Hamlet

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

The September 2010 report illustrates a national cyber dilemma that threatens the very fabric of government, commercial and private use operations worldwide. Much is written about "what" the problem is, and though the basis for the paper is an assessment of the problem space, we target the "how" solution space of the wide-area national information infrastructure through the advancement of science, technology, evaluation and analysis with actionable results intended to produce a more secure national information infrastructure and a comprehensive national cyber defense capability.

Sandia
National
Laboratories

Exceptional service in the national interest

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

Problem Statement and Overview

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

Cybersecurity Domain Priority Wide Area Problems

Cyber & Infrastructure Security

Sandia National Laboratories

Seven Priority Wide-Area Problems:

1. Disjointed Response to Wide-Area and Multi Target Attack
2. Widely Dispersed and Fragmented Detection and Notification Capabilities
3. Ill-defined Government, Commercial, and Academic Roles and Responsibilities
4. Divided and Rigid Wide-Area Cyber Protection Posture
5. Unresolved Wide-Area Common and Shared Risks
6. Fragile Interdependent Wide-Area Critical Access and Operations
7. Unresolved Attribution of Attack and Compromise

Sandia National Laboratories

Exceptional service in the national interest

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

Big Data * Cybersecurity

- Volume
- Velocity
- Variety
- Variability
- Complexity

Unprecedented Data Availability * Adversarial Threat

Sandia National Laboratories

Exceptional service in the national interest

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

Cyberspace Challenge

Accelerated National Cyber Threat Environment Amid Disruptive Change

Sandia National Laboratories

Exceptional service in the national interest

Extreme Data Future?

↑ **Big Data: Legacy to Cloud/Sensor/Mobile/Quantum**

↑ **HPC: Peta to Exascale**

↑ **ICT: IPv4 (4.3B Depleted 9/24/15) to RF/IPv6 (3.4 *10^{38})**

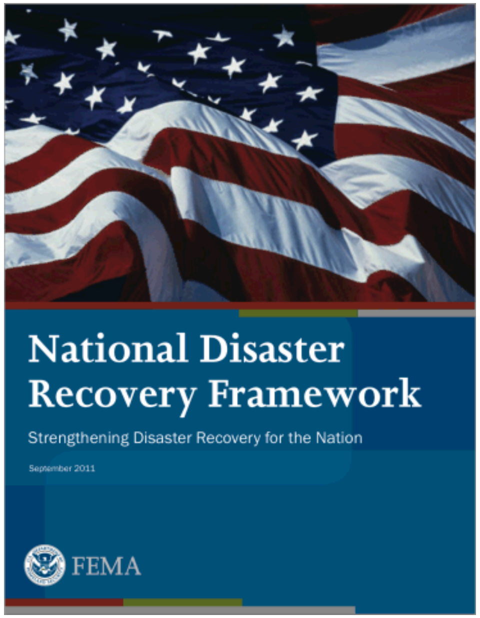
↑ **CIKR: SCADA/ICS to Multi-Domain IoT/Cyber**

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

Cyber Critical Infrastructure Risks & Exposure



National Disaster Recovery Framework

Strengthening Disaster Recovery for the Nation

September 2011

FEMA

- Complexity + Risk + Cost = Greater Exposure
- Big Data * Complexity Increases Time to Respond/Resolve
- High Risk Command & Control – Increases with Automation
- Knowledge, Skills, and Abilities Gap

Assess risk and disaster resilience so that decision makers, responders, and community members can take informed action to reduce risk and increase resilience.

Sandia National Laboratories

Exceptional service in the national interest

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

Cyber Critical Infrastructure Challenges

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems

16 DHS Defined
Critical Infrastructure Sectors

- Big Data Scale Cyberspace Threat to Critical Infrastructure Key Resources (CIKR)
- Accelerated Information and Communication Technology (ICT) Dependence
- Changing Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS)
- Wide Area Operations and Security Coordination
- Increased Need for Cyber Critical Infrastructure Protection, Resilience, & Security

National Security and Emergency Preparedness

Sandia National Laboratories

Exceptional service in the national interest

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

Research Opportunities and Expected Impacts

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 National Laboratories

Trusted Connection and Automated Process Opportunities

Actionable Result: Effective Response to Attack

Challenge: Trusted Internet Connection Defense

Short Term Conceptual Gain:

Distributed Detection, Notification & Response Communication Framework

Long Term Conceptual Gain:

Bio-Technology Aided Attribution & Cyber Deterrence

Sandia National Laboratories

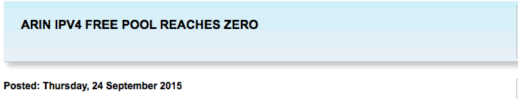
Exceptional service in the national interest

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

Informatics Statistical TCP/IP Anomalous Behavior



ARIN IPV4 FREE POOL REACHES ZERO

Posted: Thursday, 24 September 2015

Source:
https://www.arin.net/announcements/2015/20150924.html

The IPv6 Forum
The New Internet
"Take the Internet where no other network has been before"
Vint Cerf, IPv6 Forum Honorary Chairman

Source:
https://www.Ipv6 forum.org

Sandia National Laboratories

Exceptional service in the national interest

Actionable Result: Near Real Time Notification of Infrastructure Attack

Challenge: Legacy IPv4 and Next Generation IPv6

Short Term Conceptual Gain:

Distributed Sensor Architecture, Cyber Personification Schema

Long Term Conceptual Gain:

Polymorphic Attack Surface, Real Time Provisioned / Deprovisioned & Assured Critical Access & Operations

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

Cybersecurity Mathematical and Statistical Analysis

Actionable Result: Near Real Time Notification of Information Compromise

Challenge: Cybersecurity Informed Defense

Short Term Conceptual Gain:

Value Based Information Protection, & Statistical Language Analysis

Long Term Conceptual Gain:

Artificial Intelligence Aided Dynamic Defense

Sandia National Laboratories

Exceptional service in the national interest

U.S. DEPARTMENT OF ENERGY

NNSA

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

Cybersecurity Complexity Science Analysis

Actionable Result: Agile & Adaptive Defense

Challenge: Defending Against Emerging Threat

Short Term Conceptual Gain:

Behavior Based Entitlement Provisioning, Situational Staged Defense, Rapid Response Service Oriented Architecture

Long Term Conceptual Gain:

Behavioral Autoimmune System, Real Time Containment, Eradication & Recovery From Compromise

Sandia National Laboratories

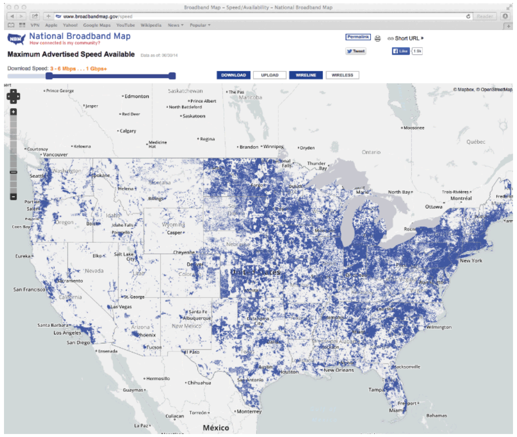
Exceptional service in the national interest

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

Modeling, Simulation and Analysis of Complex Networked Systems



Source:
http://www.broadbandmap.gov/speed

Exceptional service in the national interest

Actionable Result: Identified Shared Cross Domain Risk and Mitigations

Challenge: Informed CIKR National Cyber Defense

Short Term Conceptual Gain:

Latent Dirichlet Allocation (LDA) Based Anomalous Event Detection, Formal Risk-Based Approach to Attribution

Long Term Conceptual Gain:

Dynamically Mitigated Cross Domain Risks

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

HPC Analysis and Correlation Algorithms

INTERNATIONAL, HOMELAND, AND NUCLEAR SECURITY

Sandia National Laboratories

Actionable Result: Minimized Attack Surface and Assured Critical Access and Operations

Challenge: Big Data Correlation for National Cyber Defense

Short Term Conceptual Gain:

Federated Business Continuity Planning

Long Term Conceptual Gain:

Self-Organizing System of Systems, Real Time Containment & Eradication of Attack

Sandia National Laboratories

Exceptional service in the national interest

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

The Sociology and Psychology of Cyber Engagement

Sandia National Laboratories

Actionable Result: Attribution of Attack & Compromise, Identified Gaps and Vulnerabilities

Challenge: Understanding Defender and Attacker Engagement

Short Term Conceptual Gain:

Cyber Adaptive Response Architecture,

Multi-Actor Interactive Gaming

Long Term Conceptual Gain:

Trusted High Performance Cloud Computing, & Socio-Psychological Preemptive Response to Attack

Sandia National Laboratories

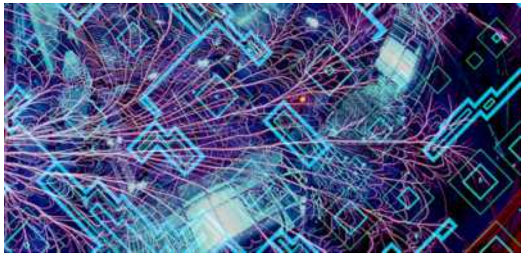
Exceptional service in the national interest

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

Cybersecurity Domain: Actionable Results



Actionable Results to Resolve Big Data Scale Challenges:

- Identification of Gaps and Vulnerabilities
- Identified Cross Domain Risks and Mitigations
- Minimized Attack Surface
- Effective Response to Attack
- Agile and Adaptive Defense
- Near Real-Time Notification of Infrastructure Attack and Information Compromise
- Assured Critical Access and Operations
- Attribution of Attack and Compromise

Sandia National Laboratories

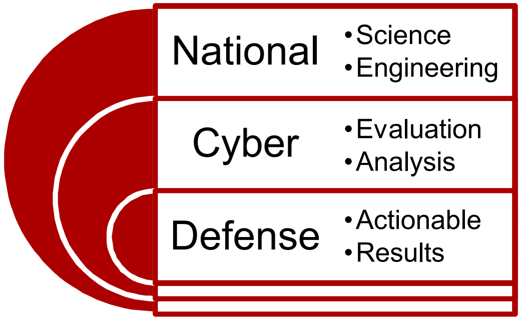
Exceptional service in the national interest

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

Research Direction


National
- Science
- Engineering

Cyber
- Evaluation
- Analysis

Defense
- Actionable
- Results

National Cyber Defense HPC Analysis

- ➢ Trusted Connection & Automated Process Opportunities
- ➢ Informatics Statistical TCP/IP Anomalous Behavior
- ➢ Cybersecurity Mathematical & Statistical Analysis
- ➢ Cybersecurity Complexity Science Analysis
- ➢ Mod, Sim & Analysis of Complex Networked Systems
- ➢ HPC Analysis & Correlation Algorithms
- ➢ The Sociology & Psychology of Cyber Engagement

Sandia National Laboratories

Exceptional service in the national interest

- Research Complexity Science, Mod-Sim of Large Scale Networks & Big Data
  - Enhanced understanding of networked systems
  - Improved graph analysis
  - Identification of network nodes to prevent or slow spread of attack
  - Improved signatures and predictors of attack
  - More timely detection of attack
  - Faster response & resolution of compromise

- Research informatics, statistical anomaly detection, data reduction approaches
  - Combine with distributed sensor networks, and HPC analysis, to enhance attack detection, response, and recovery

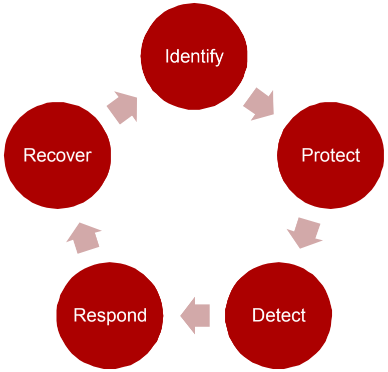
U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

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

Concepts and Planning

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

Cyber Adaptive Response Architecture



National Cyber Defense HPC Analysis

- Trusted Connection & Automated Process Opportunities
- Informatics Statistical TCP/IP Anomalous Behavior
- Cybersecurity Mathematical & Statistical Analysis
- Cybersecurity Complexity Science Analysis
- Mod, Sim & Analysis of Complex Networked Systems
- HPC Analysis & Correlation Algorithms
- The Sociology & Psychology of Cyber Engagement

Sandia National Laboratories

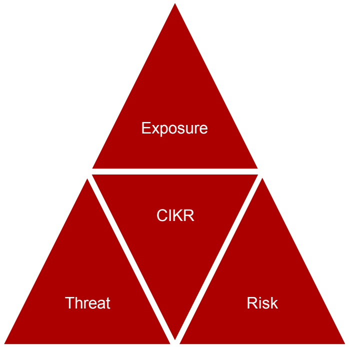
Exceptional service in the national interest

- Three Phase Automated Defense
  - Behavior-based entitlement provisioning
  - Situationally provisioned defensive posture
  - Rapid response virtual service oriented architecture (SOA)
- Command & Control (C&C)
  - Managed entitlements to information assets
  - Managed network & systems configuration
  - Managed services & applications
  - Enhanced assurance boundary
- HPC Analysis Informed Defense
  - Obfuscation & emulation
  - Data provenance & discovery attributes
  - Proactively defined defensive postures
  - Cyber event correlation & cyber response

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

Threat Evaluation Environment



National Cyber Defense HPC Analysis

- Trusted Connection & Automated Process Opportunities
- Informatics Statistical TCP/IP Anomalous Behavior
- Cybersecurity Mathematical & Statistical Analysis
- Cybersecurity Complexity Science Analysis
- Mod, Sim & Analysis of Complex Networked Systems
- HPC Analysis & Correlation Algorithms
- The Sociology & Psychology of Cyber Engagement

- Authorized User Roles & Responsibilities
  - Managed entitlement persona definitions
  - Behavior-based entitlement provisioning
  - Identity credential & access management (ICAM)

- Adversarial Based Threat Analysis
  - Threat case service oriented architecture
  - Level of adversary
  - Level of threat
  - Level of risk & vulnerability

- Predictive & Informatic Analysis
  - Big data HPC analysis informed defense
  - System in the loop
  - Live fire network
  - Managed network defense posture
  - Identification of emerging methods of attack

Exceptional service in the national interest

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

Distributed Analysis Cloud Computing

Security System Network

Sensors Cloud

National Cyber Defense HPC Analysis

- Trusted Connection & Automated Process Opportunities
- Informatics Statistical TCP/IP Anomalous Behavior
- Cybersecurity Mathematical & Statistical Analysis
- Cybersecurity Complexity Science Analysis
- Mod, Sim & Analysis of Complex Networked Systems
- HPC Analysis & Correlation Algorithms
- The Sociology & Psychology of Cyber Engagement

- Cloud/Sensor Network Architecture
  - Integrated sensor networks
  - Distributed sensors
  - Data aggregation & filtering
  - I/O, processing & storage
  - Sensor network control plane
  - Out of band sensor network communications

- Virtualized System, Network, & Security
  - Identification of hostile or rogue nodes
  - Minimize response time
  - Interactive operations

- Hybrid or Custom HPC Analysis
  - Centralized and/or distributed
  - Very large data sets
  - Computationally intensive applications
  - Real & synthetic data aggregation & filtering

Exceptional service in the national interest

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

Coordinated Response Framework

Low
Guarded
Elevated
High
Severe

National Cyber Defense HPC Analysis

- Trusted Connection & Automated Process Opportunities
- Informatics Statistical TCP/IP Anomalous Behavior
- Cybersecurity Mathematical & Statistical Analysis
- Cybersecurity Complexity Science Analysis
- Mod, Sim & Analysis of Complex Networked Systems
- HPC Analysis & Correlation Algorithms
- The Sociology & Psychology of Cyber Engagement

- Cyber Threat Definition Matrix
  - Homeland Security Advisory System Compatibility
- Big Data HPC Analysis
  - Informed Actionable Results
- Baked-In Cyber Security
  - Design Requirement - Concept to Disposition
- Wide Area Consistency
  - Common Schema & Nomenclature
  - Continuity of Operations
- Adoption of State of the Art COTS Technology
  - ICAM/Sensors
  - SOA/OpenStack
  - Cloud/IoT/Mobility
  - Software Defined Networks/IP/NFV/OpenFlow

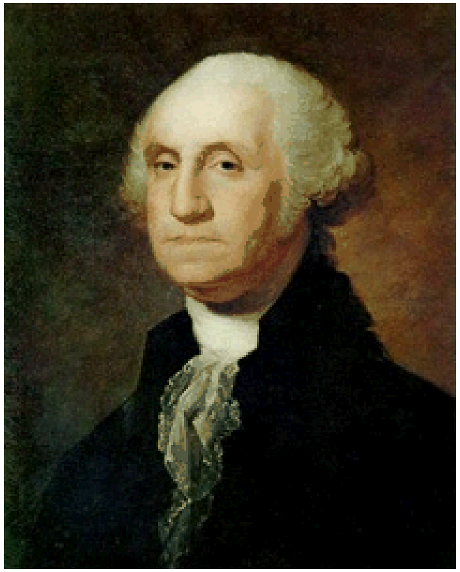
Sandia National Laboratories

Exceptional service in the national interest

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

National Cyber Defense High Performance Computing Analysis



"The time is now near at hand..."
— George Washington, July 2, 1776

Sandia National Laboratories

Exceptional service in the national interest

Where Cybersecurity Meets Big Data

Potential Areas for HPC Analysis

- Trusted Connection and Automated Process Opportunities
- Informatics Statistical TCP/IP Anomalous Behavior
- Cybersecurity Mathematical and Statistical Analysis
- Cybersecurity Complexity Science Analysis
- Modeling, Simulation and Analysis of Complex Networked Systems
- HPC Analysis and Correlation Algorithms
- The Sociology and Psychology of Cyber Engagement

Advocate for a National Cyber Defense HPC Analysis Initiative

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

QUESTIONS & DISCUSSION

Sandia Report SAND2010-4766, Unlimited Release, Printed September 2010
http://prod.sandia.gov/techlib/access-control.cgi/2010/104766.pdf

THANK YOU

Curtis Keliiaa
Sandia National Laboratories
Advanced Info & Network Sys Engineering
Email: cmkelii@sandia.gov
(505) 845-0185

P.O. Box 5800
Mail Stop 1324
Albuquerque, NM 87185-1324

Jason Hamlet
Sandia National Laboratories
Assurance Tech and Assessments
Email: jrhamle@sandia.gov
(505) 845-0903

P.O. Box 5800
Mail Stop 0671
Albuquerque, NM 87185-0671

Supplemental Slides

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

Factors & Personification

Risk Factors	Personification Risk Mitigation
Intrusion via loosely defined access-control	Personification schema & composite index
Changes in Need-To-Share and Need-To-Know policy	Global, local and anonymous security-domain relevance via COI identifiers
Global connectivity and increased mobility of users	Composite location, COI, and associated authorization identifiers
Service oriented architectures	Service type descriptor (web, network quality of service, virtualized, simulated/interactive)
Increased discoverability of centralized information assets	Information asset discoverability descriptors (globally discoverable, fully metadata discoverable, limited metadata discoverable, or exempt from discovery) to be matched with specific global, local, and anonymous COI entitlements
Convergence of multimedia data types (voice, video and data)	Complex-data descriptors to indicate composite data types and/or associated attachment data types
Electronic recording, transmitting and wireless enabled devices	Fixed or mobile device capability descriptors, may include mobility zones (location) and associated authorization/restriction attributes such as time of day or user/group.

Sandia National Laboratories

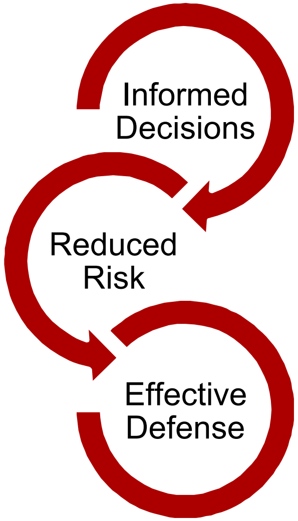
Exceptional service in the national interest

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

Threat Characteristics & Quantifiable Objectives



Threat Characteristics

Category	Funding	Goal Intensity	Stealth	Physical Access	Cyber Skills	Implementation Time	Cyber Org Size
I	H	H	H	H	H	Decades/Years	Hundreds
II	H	H	H	M	M	Years	Tens of Tens
III	M	H	M	M	M	Months	Tens
IV	L	M	H	L	H	Months	Tens
V	L	M	M	L	M	Months	Ones
VI	L	L	L	L	L	Weeks	One

National Cyber Defense Quantifiable Objectives

Inform the Decision Maker	Inform the Defender	Minimize Exposure	Reduce the Attack Surface	Effective Defense
Degree of Coordination	Degree of Unity	Degree of Investment	Degree of Resilience	Degree of Commitment

Sandia National Laboratories

Exceptional service in the national interest

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

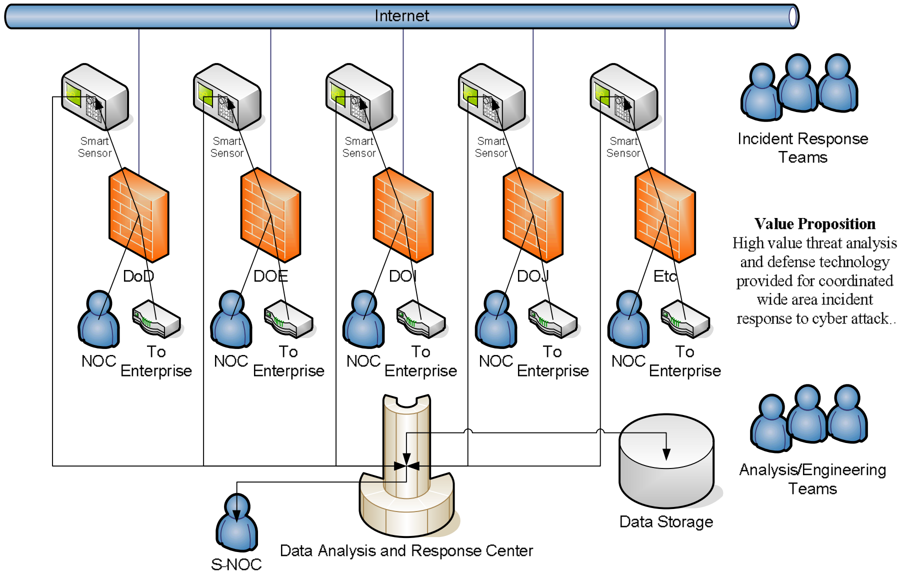
Cyber Threat Levels, Severity Indicators, & Principals

Cyber Threat Levels	Severity Indicators (binary and hex)	
Normal (all clear)	0000	0
Suspicious anomalous activity	0001	1
Suspicious low level malicious activity	0010	2
Suspected coordinated malicious activity	0011	3
Suspected sophisticated malicious activity	0100	4
Confirmed low level malicious activity	0101	5
Confirmed coordinated malicious activity	0110	6
Confirmed sophisticated malicious activity	0111	7
Suspected Cyber attack	1000	8
Suspected multi-point Cyber attack	1001	9
Suspected automated Cyber attack	1010	A
Suspected sophisticated Cyber attack	1011	B
Confirmed Cyber attack	1100	C
Confirmed multi-point Cyber attack	1101	D
Confirmed automated Cyber attack	1110	E
Confirmed sophisticated Cyber attack	1111	F

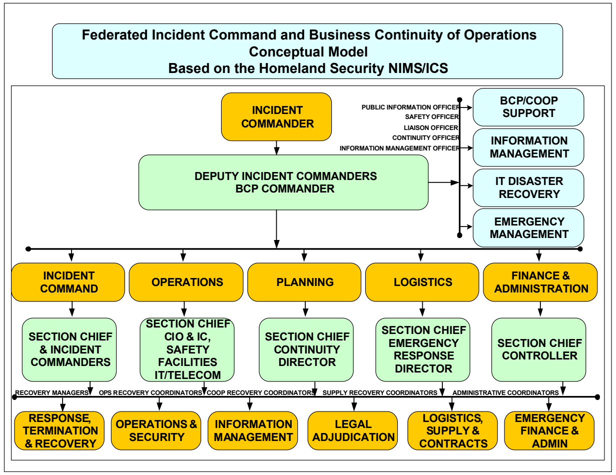
Principles of Operation:

- *Notice of Intrusion Principle* - intrusion notification data will be characterized using common terms and definitions to keep traffic nominal but high value.
- *Local Accountability Principle* – local response teams will be accountable to assess evidentiary information in support of coordinated analysis, investigation, and recovery from intrusion or attack.
- *Portability Principle* – a standardized format and glossary are used for threat levels and severity.
- *Containment Principle* - local cybersecurity policies take precedence over foreign entitlement assertions.
- *Discoverability Principle* - information assets are implicitly globally discoverable, unless explicitly identified as fully metadata discoverable, limited metadata discoverable, or exempt from discovery.
- *Portability Principle* – a standardized format with associative data dictionary and glossary are used for the personification schema, index, identifiers, and descriptors.

Federated Business Continuity



Value Proposition
High value threat analysis and defense technology provided for coordinated wide area incident response to cyber attack..



Federated Incident Command and Business Continuity of Operations
Conceptual Model
Based on the Homeland Security NIMS/ICS

INCIDENT COMMANDER

PUBLIC INFORMATION OFFICER
SAFETY OFFICER
LIAISON OFFICER
CONTINUITY OFFICER
INFORMATION MANAGEMENT OFFICER

BCP/COOP SUPPORT

INFORMATION MANAGEMENT

IT DISASTER RECOVERY

EMERGENCY MANAGEMENT

DEPUTY INCIDENT COMMANDERS
BCP COMMANDER

INCIDENT COMMAND

OPERATIONS

PLANNING

LOGISTICS

FINANCE & ADMINISTRATION

SECTION CHIEF & INCIDENT COMMANDERS

SECTION CHIEF CIO & IC, SAFETY FACILITIES IT/TELECOM

SECTION CHIEF CONTINUITY DIRECTOR

SECTION CHIEF EMERGENCY RESPONSE DIRECTOR

SECTION CHIEF CONTROLLER

RECOVERY MANAGERS
OPS RECOVERY COORDINATORS
COOP RECOVERY COORDINATORS
SUPPLY RECOVERY COORDINATORS
ADMINISTRATIVE COORDINATORS

RESPONSE, TERMINATION & RECOVERY

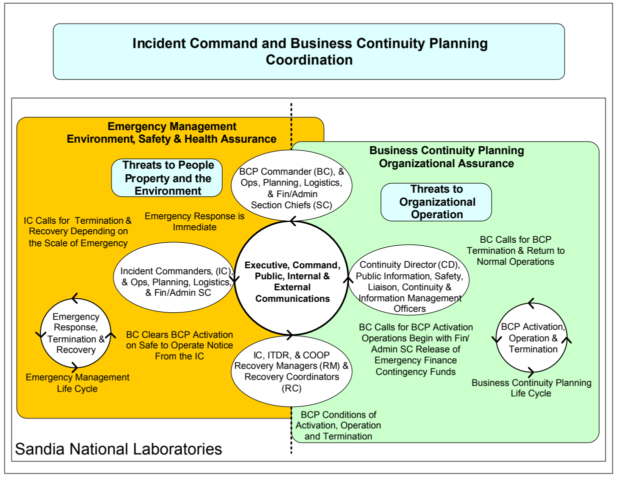
OPERATIONS & SECURITY

INFORMATION MANAGEMENT

LEGAL ADJUDICATION

LOGISTICS, SUPPLY & CONTRACTS

EMERGENCY FINANCE & ADMIN



Incident Command and Business Continuity Planning Coordination

Emergency Management
Environment, Safety & Health Assurance

Threats to People Property and the Environment

BCP Commander (BC), & Ops, Planning, Logistics, & Fin/Admin Section Chiefs (SC)

Business Continuity Planning
Organizational Assurance

Threats to Organizational Operation

IC Calls for Termination & Recovery Depending on the Scale of Emergency

Emergency Response is Immediate

Incident Commanders, (IC), & Ops, Planning, Logistics, & Fin/Admin SC

Executive, Command, Public, Internal & External Communications

Continuity Director (CD), Public Information, Safety, Liaison, Continuity & Information Management Officers

BC Calls for BCP Termination & Return to Normal Operations

Emergency Response, Termination & Recovery

BC Clears BCP Activation on Safe to Operate Notice From the IC

IC, ITDR, & COOP Recovery Managers (RM) & Recovery Coordinators (RC)

BC Calls for BCP Activation Operations Begin with Fin/ Admin SC Release of Emergency Finance Contingency Funds

BCP Activation, Operation & Termination

Emergency Management Life Cycle

Business Continuity Planning Life Cycle

BCP Conditions of Activation, Operation and Termination

Sandia National Laboratories

References

1. SAND2009-6671 P A Sensor Network Study, January 2010
2. SAND2005-5411, Generic Threat Profiles, David P. Duggan, Unlimited Release, July, 2005
3. Architectural Reasoning Explained, Gettit Muller, 2010, http://www.gaudisite.nl
4. Palacios and Kitten: New High Performance Operating Systems For Scalable Virtualized and Native Supercomputing, John Lange, Kevin Pedretti, Trammell Hudson, Peter Dinda, Zheng Cui, Lei Xia, Patrick Bridges, Andy Gocke, Steven Jaconette, Mike Levenhagen, and Ron Brightwell

   Northwestern University, Department of Electrical Engineering and Computer Science

   Sandia National Laboratories, Scalable System Software Department

   University of New Mexico, Department of Computer Science
5. SAND2010-2179 Statistical Language Analysis for Automatic Exfiltration Event Detection, April 2010
6. A Scientific Research and Development Approach to Cyber Security, Submitted to the Department of Energy On Behalf of the Research and Development Community, December 2008. Comments to Charlie Catlett, Argonne National Laboratory
7. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, April 17, 2009, https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
8. President's Council of Advisors on Science and Technology (PCAST), http://www.whitehouse.gov/administration/eop/ostp/pcast
9. President's Innovation and Technology Advisory Committee, http://www.whitehouse.gov/the-press-office/executive-order-presidents-council-advisors-science-and-technology
10. National Research Council 2005 publication, Getting Up To Speed: The Future of Supercomputing
11. The Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
12. Cybersecurity Act of 2010, http://commerce.senate.gov/public/index.cfm?p=Legislation&ContentRecord_id=f2256d47-85a9-4c64-b9e0-40ab01564735