SAND2013-0955C

Sandia National Laboratories

# Digital Security: Protecting Your IT and Communications Networks

## The Role of Broadband in Emergency Preparedness

SAND Number: 2013-0955C
Unclassified Unlimited Release
Curtis M. Keliiaa
February 12, 2013

Operated by
LOCKHEED MARTIN

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.

# FCC National Broadband Plan

**Goal No. 1**: At least 100 million U.S. homes should have affordable access to actual download speeds of at least 100 megabits per second and actual upload speeds of at least 50 megabits per second.

**Goal No. 2**: The United States should lead the world in mobile innovation, with the fastest and most extensive wireless networks of any nation.

**Goal No. 3**: Every American should have affordable access to robust broadband service, and the means and skills to subscribe if they so choose.

**Goal No. 4**: Every American community should have affordable access to at least 1 gigabit per second broadband service to anchor institutions such as schools, hospitals and government buildings.

**Goal No. 5: To ensure the safety of the American people, every first responder should have access to a nationwide, wireless, interoperable broadband public safety network.**

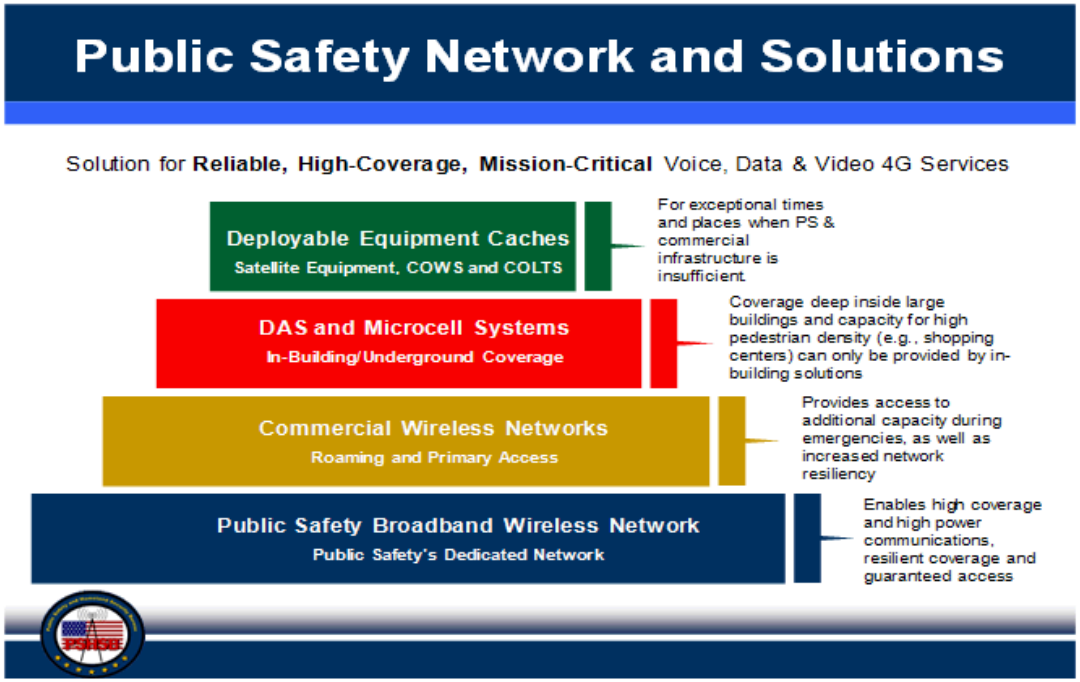
**Goal No. 6**: To ensure that America leads in the clean energy economy, every American should be able to use broadband to track and manage their real-time energy consumption.

http://www.broadband.gov/

# Nationwide Public Safety Network

**ELECTRONIC CODE OF FEDERAL REGULATIONS**
**PART 90—PRIVATE LAND MOBILE RADIO SERVICES**
**§ 90.19 Nationwide Public Safety Broadband Network.**

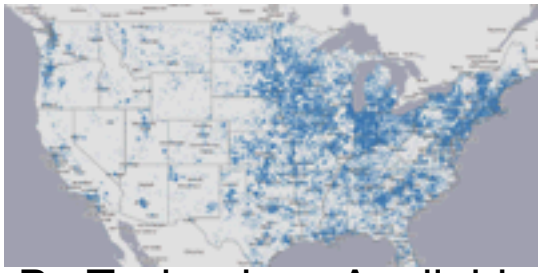
Pursuant to the Middle Class Tax Relief and Job Creation Act of 2012, Public Law 112-96, 126 Stat. 156 (2012), the 758-769 MHz and 788-799 MHz bands are allocated for use by the First Responder Network Authority to deploy a **Nationwide Public Safety Broadband Network as prescribed by statute**. [77 FR 62462, Oct. 15, 2012]




http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=&rgn=div5&view=text&idno=47&node=47:5.0.1.1.3

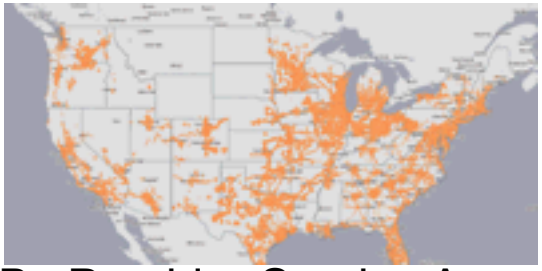
# National Broadband Maps

By Speed Available



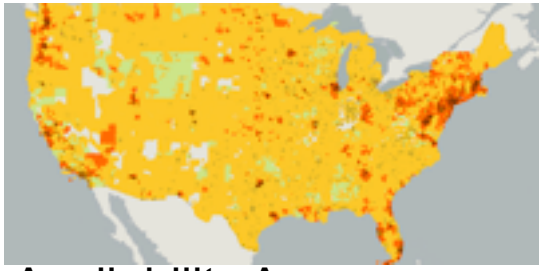
By Technology Available

By Number of Providers



By Provider Service Area

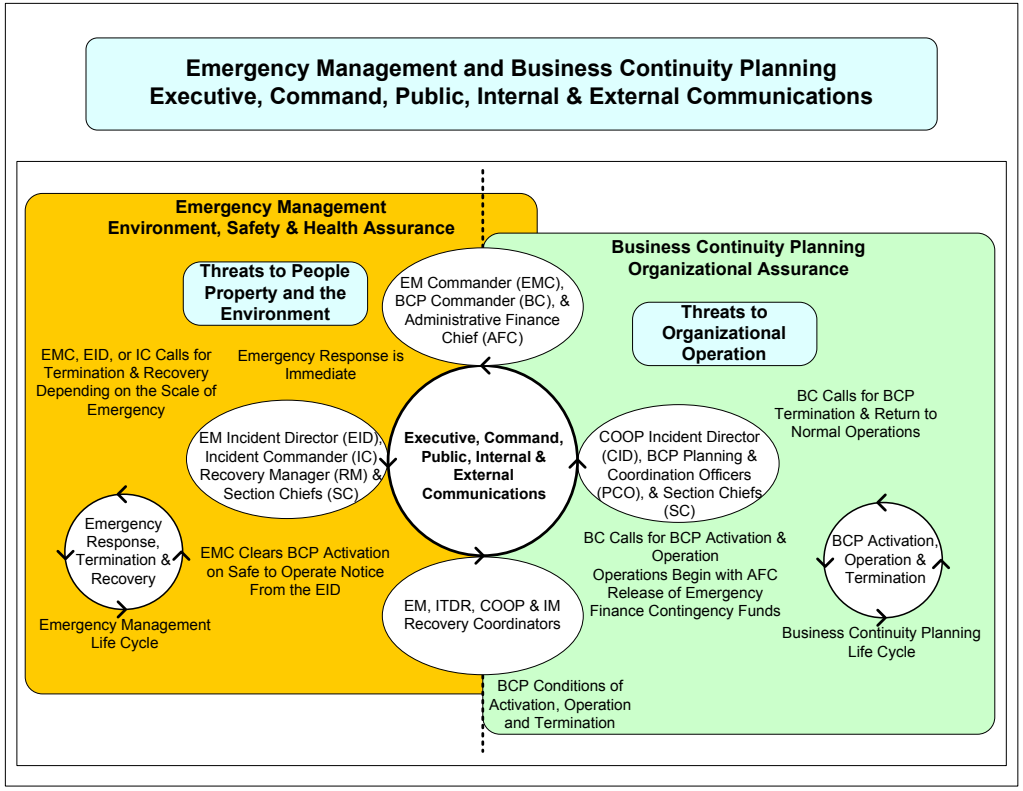
http://www.broadbandmap.gov/



Availability Across Demographic Characteristics

# Emergency Response and Recovery

1. Emergency Management – The Safety of People, Property, and the Environment
2. Business Continuity Planning – Continuity of Operations and IT Disaster Recovery



# National Incident Management System

*National Incident Management System 7* (NIMS) HSPD–5 2008

"to reduce the loss of life and property and harm to the environment. "

a. Preparedness

**b. Communications and Information Management**

**"rely on communications and information systems that provide a common operating picture to all command and coordination sites"**

c. Resource Management

d. Command and Management

e. Ongoing Management and Maintenance

http://www.fema.gov/national-incident-management-system

# A New Era of Opportunity

Sandia National Laboratories

- The Second Internet - 3.4 x 10 to the 38th address space
- Broadband
- Wireless Broadband
- Mobility and Smartphones
- Network Mobility
- Virtualization, Cloud and Clustering Technologies

Tribal Authorization - 2012 FEMA Reauthorization Act, Section 210

# and Challenges!

- **Regulatory Change (ITU, WCIT, and FCC)**
- **Unserved and underserved Advanced Internet Service Areas**
- **Cybersecurity Amid Sophisticated Threats**
- **Changing Technology Landscape For Emergency Preparedness**
- **Interoperability**
- **Complexity**

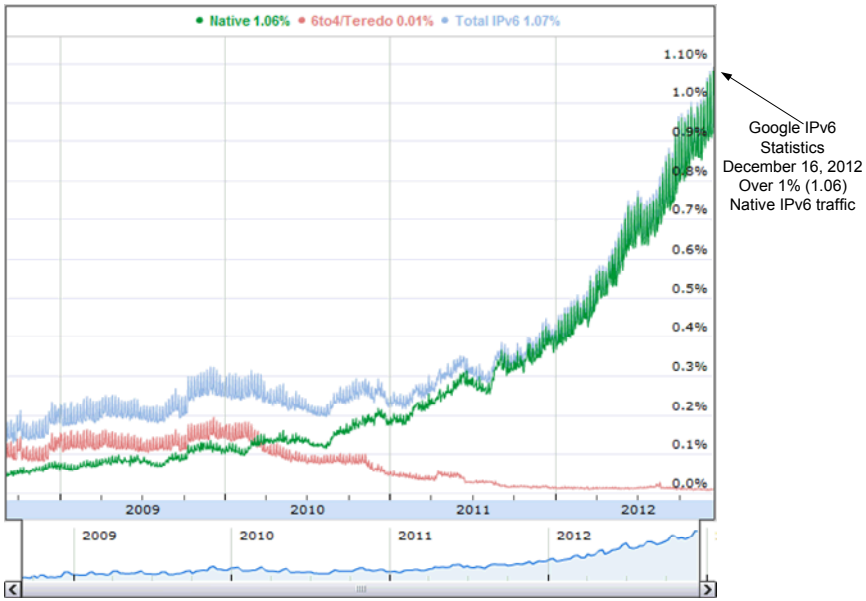
# Technology Landscape

Sandia National Laboratories

Recommendation 16.15: The FCC should address IP-based communications

- P25 – Conventional Digital Fixed Station Interfaces (Statement of Requirements 2.7.2)
- Mobility
- NG E911 may affect location accuracy and Automatic Location Identification (ALI) for VoIP
- Non-voice methods of communicating with 911 like text and multimedia messages
- Access to PSAPs via various IP-based communications modes.
- NG E911 beyond traditional voice-centric devices

**Changing IP Technology**




Larry Page, Google's Chief: company was in "uncharted territory" because of rapid changes in mobile technology.

# Interoperability

**Interoperability:** Ability of systems, personnel, and equipment to provide and receive functionality, data, information and/or services to and from other systems, personnel, and equipment, between both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively together. Allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on- demand, in real time, when needed, and when authorized.

http://emilms.fema.gov/IS700aNEW/glossary.htm

# More Interoperability Guidance

Sandia National Laboratories

## DIGITAL GOVERNMENT: BUILDING A 21ST CENTURY PLATFORM TO BETTER SERVE THE AMERICAN PEOPLE, MAY 23, 2012

- Government-wide open data, content, and web API policy and identify standards and best practices for **Improved Interoperability**
- Digital Services Innovation Center: Identify shared and open content management system solutions
- DHS/DOD/NIST: Develop government-wide mobile and wireless security baseline

http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

## NIMS System 7 December 2008

- **Communications Interoperability** allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video in real time, when needed, and when authorized. It is essential that these communications systems be capable of interoperability, as successful emergency management and incident response operations require the continuous flow of critical information among jurisdictions, disciplines, organizations, and agencies.
- **Interoperability Planning** requires accounting for emergency management and incident response contingencies and challenges. Interoperability plans should include considerations of governance, standard operating procedures (SOPs), technology, training and exercises, and usage within the context of the stress and chaos of a major response effort. Coordinated decision-making between agencies and jurisdictions is necessary to establish proper and coherent governance and is critical to achieving interoperability. Agreements and SOPs should clearly articulate the processes, procedures, and protocols necessary to achieve interoperability.

http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

# Complexity!

HSToday.US Article 10/16/2012
**Plans & Challenges Emerge For Nationwide Public Safety Broadband**
By: Dan Verton
"The First Responder Network Authority (FirstNet), an independent board established to oversee the creation of a nationwide public safety broadband network (NPSBN) for first responders, recently started the difficult work of designing a blueprint of what such a massive network might look like."
"But as public comments on the proposed conceptual architecture of the network began flowing in this week, the **sheer size and scope of the effort** -- combined with the multitude of existing systems currently in use across the country -- suggest that planning, policy and integration activities will be more difficult and time consuming than actually building the network"
http://www.hstoday.us/industry-news/general/single-article/plans-challenges-emerge-for-nationwide-public-safety-broadband/88d3ce2a0fe3a0272750c78870133f9d.html

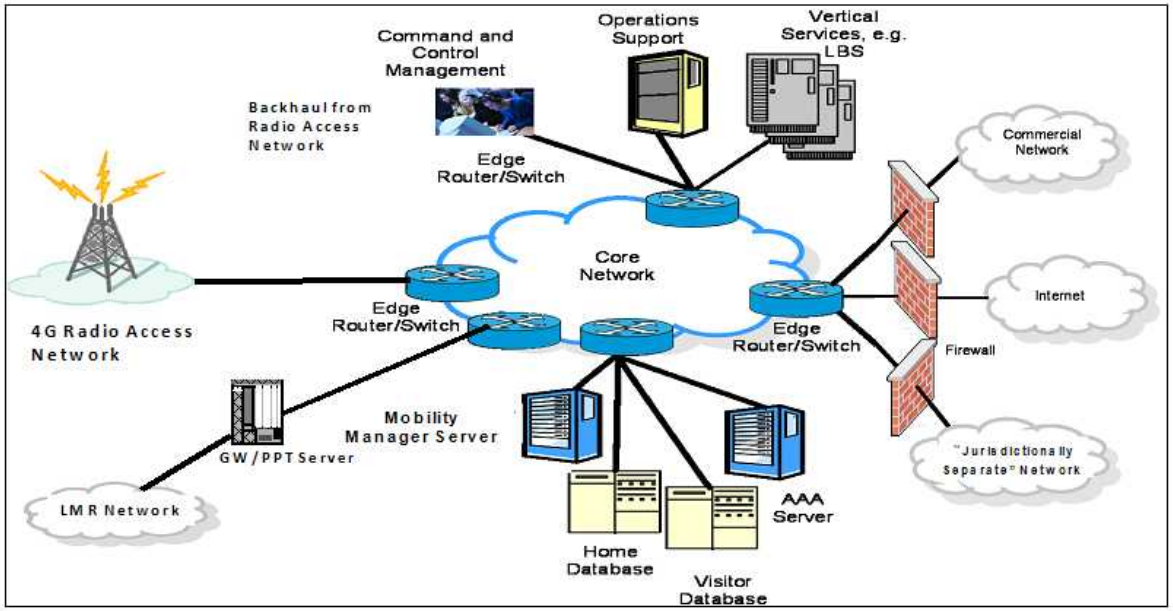
MIT Review Article 11/26/2012
**The Spectrum Crunch That Wasn't**
By: David Talbot
"Those armies of smartphone owners—and their tablet-toting brethren—are contributing to a striking increase in wireless data usage: Cisco Systems estimates that **mobile data traffic will grow by a factor of 18 by 2016, and Bell Labs predicts it will increase by a factor of 25.**"
"spectrum "crunches - mobile phone usage that overwhelms the available wireless frequencies—would occur at highly specific locations and times. Sometimes, **alternative strategies can completely solve these localized problems**."
http://www.technologyreview.com/review/507486/the-spectrum-crunch-that-wasnt/

Xconomy Article 1/7/2013
**Mobility and Big Data: Why They Need Each Other to Thrive**
By: Scott Snyder:
"Mobile devices and apps will generate **seven exabytes of data by 2015, a number that will continue to double and perhaps triple each year**. Not only are huge volumes of data/content being communicated through mobile networks, but there has been unexpected growth in related communications and transactions, such as:
"Salesforce.com getting 60 percent of its "transaction volume" from mobile devices"
"Pandora delivering 60 percent of its music minutes to mobile devices"
"Facebook getting 30 percent of its traffic from mobile"
"Twitter getting 55 percent of tweets from mobile"
http://www.xconomy.com/boston/2013/01/07/mobility-and-big-data-why-they-need-each-other-to-thrive/

# Cybersecurity

Recommendation 16.5: The FCC should issue a cybersecurity roadmap

- Identify the five most critical cybersecurity threats
- Establish a two-year plan, including milestones, to address threats




Sality botnet horizontal scan of the entire IPv4 address space conducted in February 2011 used to try to discover and compromise VoIP-related (SIP server) infrastructure.
(Cooperative Association for Internet Data Analysis (CAIDA))
http://www.caida.org/publications/presentations/2012/analysis_stealth_scan_lisa/

# Protection of Information

Sandia National Laboratories

**Internet Connected Systems Are At Risk!**

## Cybersecurity

1. Confidentiality – Encryption
2. Integrity – Digital Certificates / Signatures
3. Availability – Redundancy and Backups
4. Incident Response

## Personnel

1. Background Checks
2. Clearances/Access Controls
3. Knowledge, Skills and Abilities

## Protect Against

- Inappropriate Access and Use
- Cyber Attack and Compromise
- Data Loss
- Service Disruption

**Information Ownership and Stewardship**

# The Value of Information

Sandia National Laboratories

## Know the Value of your Information… Categorize

1. What is it?
   - Situational Awareness
   - Trade Marks and Copy Rights
   - Intellectual Property
   - Personally Identifiable Information (LE, Med)
   - Proprietary Information
2. Is it Accurate?

## To you and to others… Protect with need-to-know

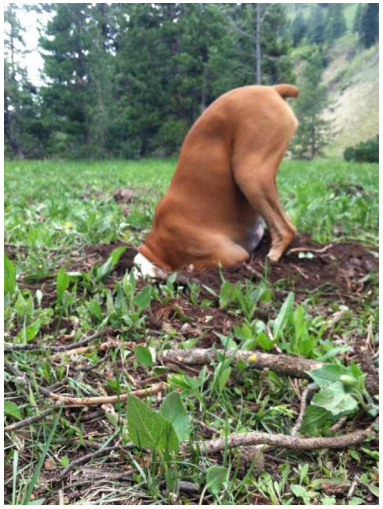
1. System certification and accreditation
2. Access controls
3. Encryption at rest and in transit

# Incident Response and Investigation

Sandia National Laboratories

## Incident Response

1. Is it an Issue, Problem, or Threat?
2. Issue Resolution - Help Desk
3. Problem Fix – Repair or Design Team
4. Threat Mitigation – Cyber Security Team
5. System / Network Compromise - Investigation Team



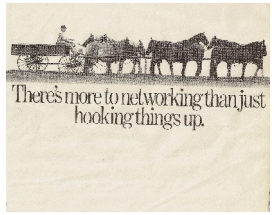
## Investigation, Forensics and Chain of Custody

1. Power
2. Disk Imaging
3. Memory
4. Hashing – preserving the integrity of evidence

## Professional Qualifications

1. Education
2. Certifications
3. Ethics
4. Experience
5. Clearances
6. Jurisdiction – some things must be handed off to law enforcement

# ISC2 CISSP Domains - CBK's




**Access Control** - security architecture
**Telecommunications and Network Security** - network structures, transmission methods, transport formats and security measures for availability, integrity and confidentiality
**Information Security Governance and Risk Management** - development, documentation and implementation of policies, standards, procedures and guidelines
**Software Development Security** – controls in systems, development, and applications software
**Cryptography** - principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity.
**Security Architecture and Design** - concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and controls used to enforce levels of confidentiality, integrity and availability
**Operations Security** - controls over hardware, media and operators with access privileges
**Business Continuity and Disaster Recovery Planning** - preservation of the business in the face of major disruptions to normal business operations
**Legal, Regulations, Investigations and Compliance** - computer crime laws and regulations; investigative measures and techniques used to determine if a crime has been committed and methods to gather evidence
**Physical (Environmental) Security** - threats, vulnerabilities and countermeasures utilized to physically protect an enterprise's resources and sensitive information.

https://www.isc2.org/

# SANS 20 Critical Security Controls

Sandia National Laboratories

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Device Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Loss Prevention
18: Incident Response Capability
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

SysAdmin, Audit, Network, Security (SANS) Institute, 20 Critical Security Controls
http://www.sans.org/critical-security-controls/

# Educate Your Community

Sandia National Laboratories

**Users and Workforce**

1. Appropriate Use and Protection of Information
2. Science, Technology, Engineering and Math (STEM)
3. Information and Communications Technology (ICT)
4. Education Curriculum Opportunities

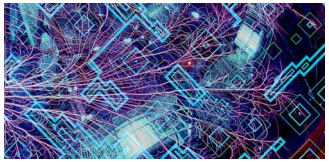
**Additional Resources**

1. DHS National Coordinating Center for Telecommunications (NCC)
2. FCC Emergency Response Interoperability Center (ERIC)…
3. Cyber Emergency Response Center (CERC)
4. National Institute of Standards and Technology (NIST)
5. SysAdmin Audit Network Security (SANS) Institute
6. International Information System Security Certification Consortium (ISC2)

# Tribal Government Relations


http://www.sandia.gov/

# Sandia Advanced Information & Network Systems Engineering


Network R&D


Analysis


Cryptography


Assessments


HPC


Mod & SIM


Cyber Security


Wireless

http://www.sandia.gov/

# Sandia Cyber Engineering Research Laboratory

Sandia National Laboratories


**Tracer FIRE (Forensic Incident Response Exercise) is a hands-on computer security workshop for cyber security professionals. Tracer FIRE aims to empower cyber security responders with critical thinking skills and leadership experience that today's analysts need to combat the adversary.**

# Tribal Government Program Development

Tribal Energy Program

Advanced Information and Network Systems Engineering

Objective Advisory / Advocate Role

Operated by LOCKHEED MARTIN

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.