SAND2019-3664C

Protection of Intersecting Information, Communications, Operational, and Virtual Critical Infrastructure

SAND2019-xxxx

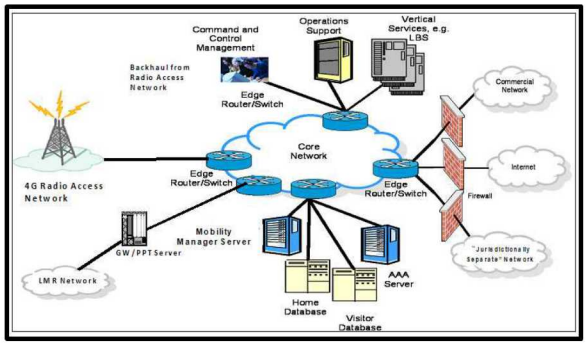
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

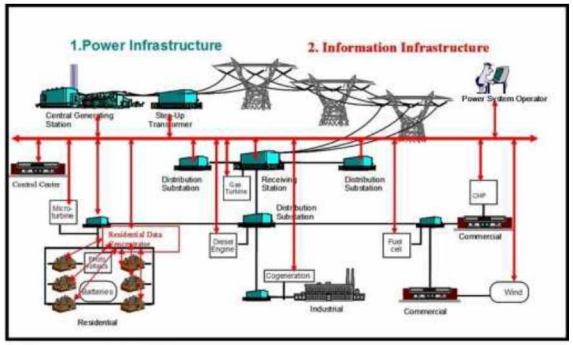
Tribal Cyber/Energy Team

Source:https://www.census.gov/geo/maps-data/maps/aian_wall_maps.html

Expert Partnership with Tribes that have Single-Point of Authority over their critical infrastructures:

- Modernization
- Physical Security
- Cyber Security
- Resilience





- Sandia National Laboratories
  - Objective Advisory – Separate From Industry
  - Breadth of Diverse National Security Missions
  - Depth In Energy, Science, Engineering, Cybersecurity
- Tribal and National Security Challenges
  - Cybersecurity (C)
  - Physical Security (P)
  - Resilience (R)
  - Secure Hardware, Software, and Virtual Technologies
  - Integrated Information (IT) & Operational Technologies (OT)
- Leap Ahead Cyber Ecosystem Challenges
  - Facilities Innovation – Smart Buildings
  - Emergent Information and Communication Technologies (ICT)
  - Energy Critical Infrastructure – Smart Grid, Micro Grid, Smart Metering
  - Community Safety & Resiliency – Smart Tribal Communities
  - Science, Technology, Engineering, Math (STEM) Workforce Development

U.S. DEPARTMENT OF ENERGY NNSA

High Performance Computing

Funding profiles for Scientific Computing at Sandia

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

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

- Continuous Access to Large Compute Systems
- ~60PF, ~10B Processor Hours/Year

Operations

- Scientific Computing Platforms – 14 clusters in 4 environments
- 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

Center for Computing Research

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 Collaboration with Industry and Academia

U.S. DEPARTMENT OF ENERGY NNSA

National Critical Infrastructure and Broadband Impacts

√ Cyber Innovation

√ Cross Sector Impact

Dept. of Homeland Security Defined Critical Infrastructure Sectors

Source: Sandia National Laboratories: Resilient Infrastructure Systems

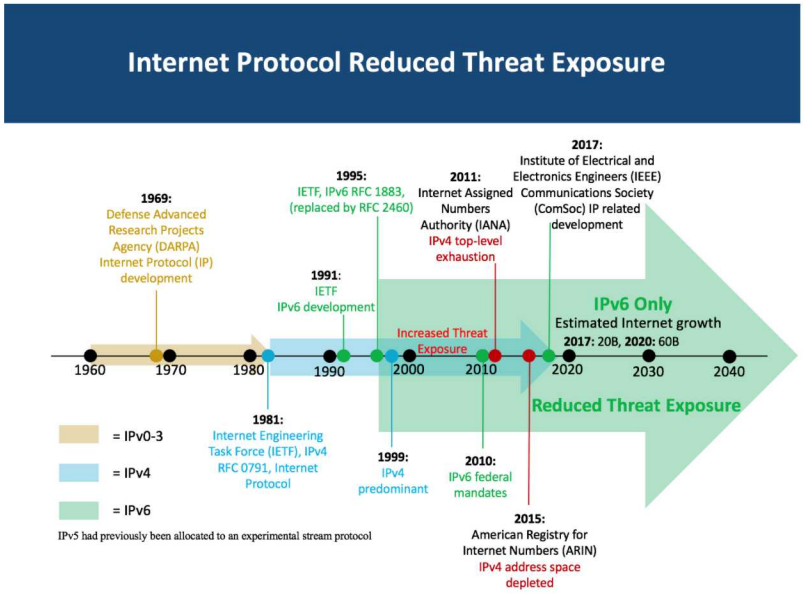
Source: Networking and Information Technology Research and Development Program, https://www.nitrd.gov/apps/broadband/

Broadband = Vast Expansion and Device Connectivity

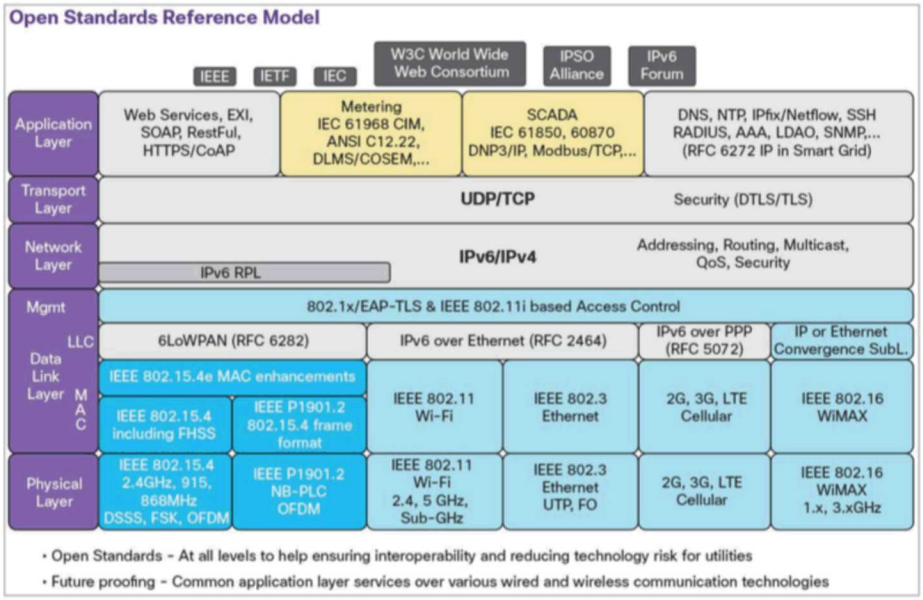
Impact for all Critical Infrastructure and Broadband Stakeholders!

U.S. DEPARTMENT OF ENERGY | NNSA

Standards-Based Innovation Enablers



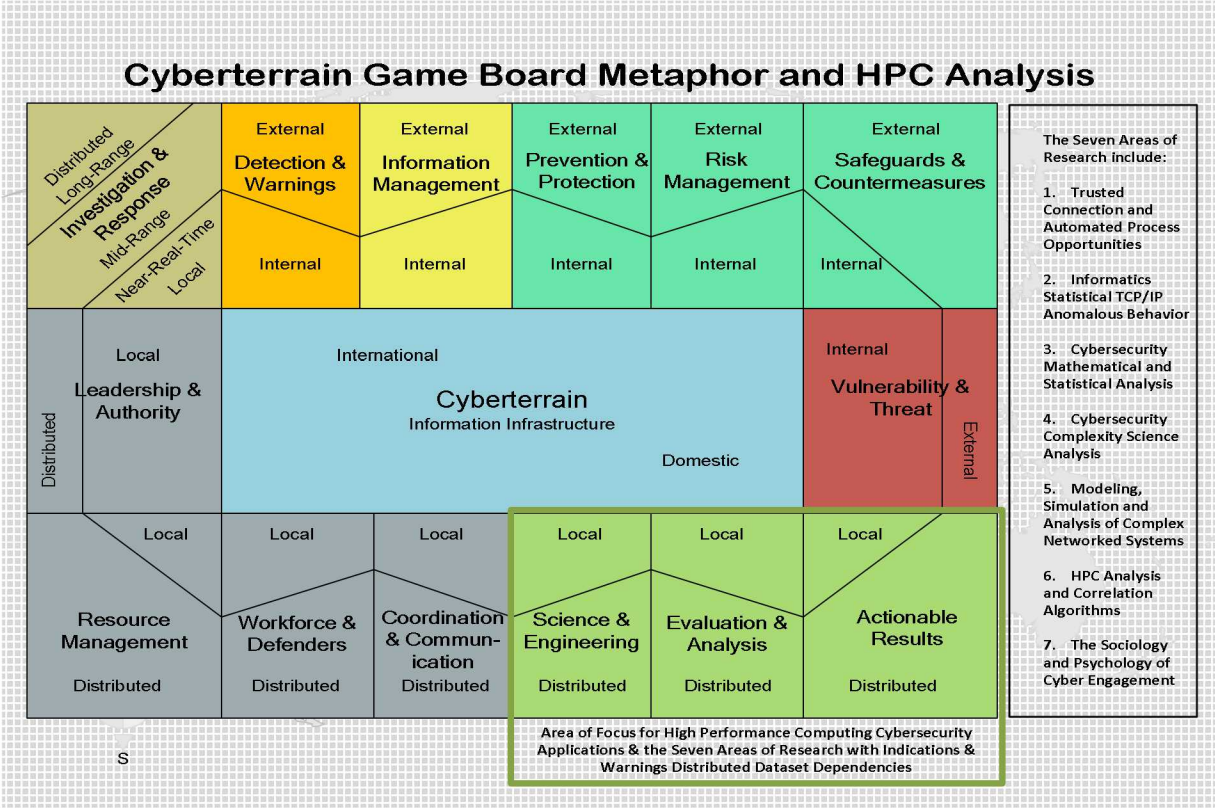
Source: Sandia National Laboratories Tribal Cyber Energy



Source: Cisco Systems, Inc. ™
https://www.cisco.com/c/en/us/solutions/industries/energy/external-utilities-smart-grid/field-area-network.html

Cyber-Peanut Game Board

A Stakeholder Game of Protection for Intersecting Information, Communication, Operational, and Virtual Infrastructure



Source: SAND2010-4766 National Cyber Defense and High Performance Computing Analysis-Concepts Planning Roadmap

Cyber Analytic Innovation

Cyber Resilient Energy Delivery Systems R&D Methodologies Concept

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

Cross Sector Change/Impact

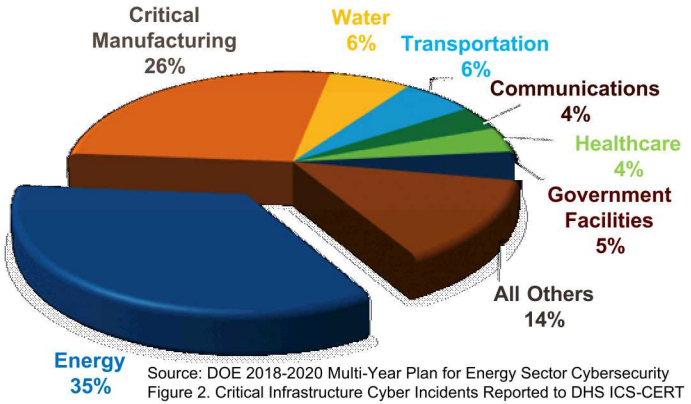
- Information – Big Data
- Communications – Mobile
- Operational – Safety & Security
- Virtual – Cloud

Brainstorm Session #1
High level considerations for protection of information in evolving infrastructure services

Information Value and Residence – Virtual Perspective

- Authorization – FEDRamp, Designated Approving Authority, Other
- Public – Non-Sensitive Information
- Private – Sensitive Information
- Owner – Agency, Organization, Community, Individual
- Steward – 3rd Party, Provider
- Elastic – Ephemeral
- Records – Long Lived
- Information Assurance – Authentication, Inheritance, Multitenant
- Cyber Security Framework – Identify, Protect, Detect, Respond, Rec

Cyber Threat



Source: DOE 2018-2020 Multi-Year Plan for Energy Sector Cybersecurity Figure 2. Critical Infrastructure Cyber Incidents Reported to DHS ICS-CERT (2013-2015)
https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

Infrastructure Maturity and Modernization

- Organization – Government, Agency, Department, Enterprise, Corporate, Business
- Provider – Commercial Cloud Service Provider (CSP) / Internet Service Provider (ISP)
- Information Systems – Computing, Platform, Vendor
- Operational Systems – Life Safety, Physical Security, Facilities
- Operational Support Systems – Domain Name Service (DNS) Address Records (A/AAAA), Internet Protocol (IP) Address Management (IPAM), Help Desk / Ticketing, Incident Response
- Services – Legacy, Cloud, Email as a Service (EaaS), Software (SaaS), Platform (PaaS), Infrastructure (IaaS)
- Network – IPv4, IPv6, Dual Stack, Wireline, Wireless, Trusted Internet Connection (TIC), Broadband

Brainstorm Session #2
High level considerations for protection of information in evolving infrastructure services

Data and Service Location
- Internal – On Prem, Private Cloud, Local
- External – Off Prem CSP, External Facing Services (DNS, Email, Web), Distributed
- Internal/External – Dependencies, Caveats, Differences, Separation, CONUS, OCONUS

Service Delivery
- Physical – Hardware, Device, Client/Server, Wireline
- Virtual – Cloud, Software Defined Network (SDN), Artificial Intelligence (AI), Augmented Reality (AR)
- Mobile – Wireless, Mobile Networks, Near Field Communications, Intranet, Internet

Information Asset Security
- Confidentiality – Encryption at Rest, In Transit, In Process
- Integrity – Validation, Authorization, Authentication, Audit, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Compliance (DMARC)
- Availability – Virtual, Multisource, Multipath, Mobility, Portability, Staffing, Skills Development
- Vulnerability and Exposure – Risks, Change, Configuration, Partners, Processes, Operations, Tech, Admin
- Attack Surfaces – Services, Neighborhood, Organization, Mobile, Device, Supply Chain, User, Insider
- Resilience – Critical Infrastructure, Cyber Relevant Time, Continuity, Operations, Diversity, AppSec

Brainstorm Session #3

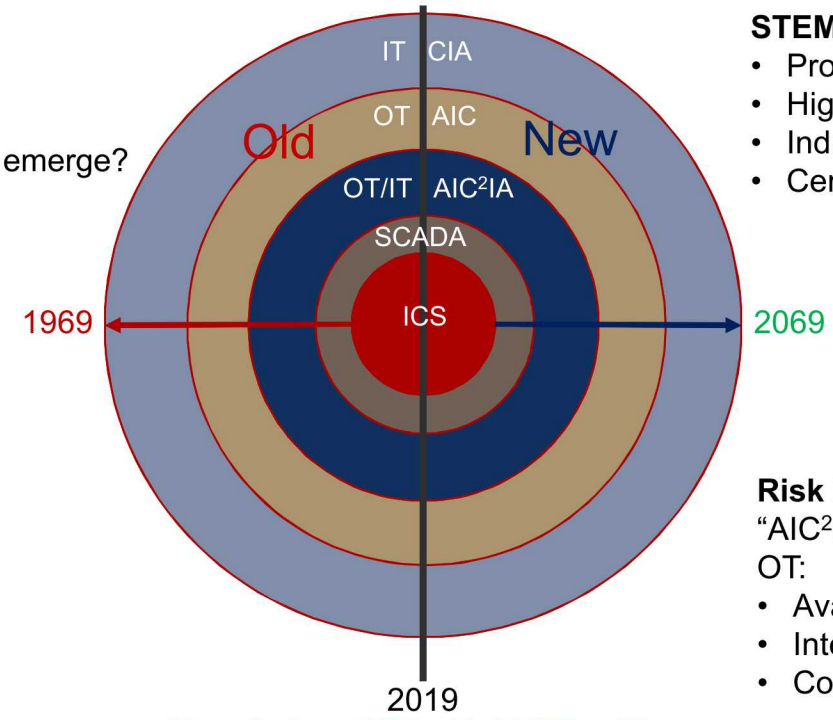
High level considerations for protection of information in evolving infrastructure services

Brainstorm Session Questions

- What use cases can be elicited?
- Who is responsible for what?
- What are the risks and payoffs?
- What security architecture insights emerge?
- What mitigation insights emerge?
- What priorities can be identified?
- What analytics can be inferred?
- How long will it take to finish?
- How much will it cost to complete?

Parking Lot Issues:

Technology (T) Workforce Call to Action



Knowledge, Skills, & Abilities Gap

STEM Workforce

- Professional Organizations
- Higher Education
- Industry Training
- Certifications

(T)

Risk Management

"AIC²IA" Security Model

OT:

- Availability
- Integrity
- Confidentiality

IT:

- Confidentiality
- Integrity
- Availability

Key Points:

Tribal Single Point of Authority

- Governance
- Departments
- Communities
- Enterprises
- Infrastructure
- Workforce

Leap Ahead of Legacy

Long-Term Gain with New Standards

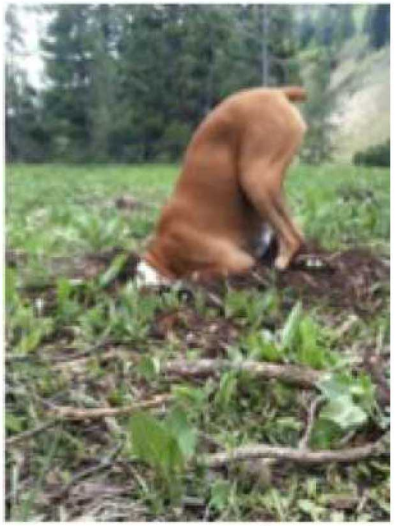
CPR Design

- Cyber Security
- Physical Security
- Resilience

Mahalo!

Curtis Keliiaa
cmkelii@sandia.gov
Sandia National Laboratories

Digging for Clues?



Questions Please!