Secure and Sustainable Energy Future
Integrated Cyber Physical Impact Analysis
Douglas M. Osborn

Governor's Summit on Energy Security & Infrastructure
## Sandia Addresses National Security Challenges

<table>
<thead>
<tr>
<th>Decade</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1950s</td>
<td>Nuclear weapons, Development engineering, Production and manufacturing engineering</td>
</tr>
<tr>
<td>1960s</td>
<td>Nuclear weapons, Development engineering, Multiprogram laboratory</td>
</tr>
<tr>
<td>1970s</td>
<td>Nuclear weapons, Multiprogram laboratory, Missile defense work</td>
</tr>
<tr>
<td>1980s</td>
<td>Nuclear weapons, Missile defense work, Post-Cold War transition</td>
</tr>
<tr>
<td>1990s</td>
<td>Nuclear weapons, Post-Cold War transition, Stockpile stewardship</td>
</tr>
<tr>
<td>2000s</td>
<td>Nuclear weapons, Post-Cold War transition, National security, START Post 9/11</td>
</tr>
<tr>
<td>2010s</td>
<td>Nuclear weapons, LEPs Cyber, biosecurity proliferation, Evolving national security challenges</td>
</tr>
</tbody>
</table>
Sandia addresses energy challenges

1970s
- Multi-program laboratory
- Energy crisis

1980s
- Missile defense work
- Cold War

1990s
- Post-Cold War transition
- Stockpile stewardship

2000s
- START
- Post 9/11
- National security

2010s
- LEPIs
- Cyber, biosecurity proliferation
- Evolving national security challenges

- Solar
- Nuclear
- Fossil
- Wind
- Geothermal
- Combustion
- Nuclear Waste

- Atmospheric Monitoring
  - Water & Energy
    - Grid/Energy Storage
      - Biomass
        - Energy Cyber
Examples of Sandia’s impact

Core, dynamic, and rapid response

Core: Long term research that solves the nation’s immense problems

- Drilling technologies, nuclear reactor safety, nuclear waste disposal, and Strategic Petroleum Reserve

Dynamic: Addressing current national needs on a 5-10 year timeframe

- Efficient engines, renewable energy technologies, and grid modernization

Rapid Response: Quick mobilization of expertise for urgent national needs

- Aliso Canyon, Fukushima, and Deepwater Horizon
Current US Energy Objectives

Secure and Resilient
• Energy systems should be secure from and resilient to natural disruptions as well as man-made attacks. Security must be addressed along the entire energy service value chain from supply (energy resources, materials, and technologies) to operations (distribution, storage, and end-use of fuels/electricity).

Economically Competitive
• Energy systems should provide energy services that are abundant, sustainable, and affordable—taking into account the full market impacts and life-cycle costs of the energy-service value chain.

Environmentally Responsible
• Clean energy systems should minimize air, water, and land pollutant emissions; GHG emissions; biota impacts; and disruption of water and land resources.

Source: QTR, page 19
Secure & Sustainable Energy Future
High Level Objective

Drawing upon our differentiating capabilities and as a principal element of the national lab system, Sandia makes major contributions to the nation’s energy security and resilience, economic viability, and environmental sustainability.
SSEF Strategy Elements

**STATIONARY POWER**
- Safety, security, & resilience of the energy infrastructure
- Higher efficiency & environmentally sound energy sources
- Back end of the nuclear fuel cycle

**CLIMATE & EARTH SYSTEMS**
- Arctic climate measurements & modeling
- Water/energy nexus
- Sustainable subsurface energy development

**TRANSPORTATION ENERGY**
- Co-evolution of engines & fuels
- Alternative fuels: hydrogen & natural gas
- Biomass conversion to reduce GHG emissions

ENERGY & CLIMATE RESEARCH
LABS FOUNDATION
Stationary Power

Safety, Security & Resilience of the Energy Infrastructure

Protect energy systems through R&D advances in cyber and physical security and resiliency

Higher Efficiency & Environmentally Sound Energy Sources

Advance the next generation of energy technologies

Back End of the Nuclear Fuel Cycle

Develop effective radioactive waste solutions across transportation, storage, and disposal
Sandia integrates an array of modeling and simulation capabilities to manage this risk and secure systems:

- Threat modeling
- Adversary-based vulnerability assessment
- Network and control system emulation, simulation, and analysis
- Physical system modeling and simulation
- Critical infrastructure modeling
ICPIA Modeling and Activities

Not linear: Can start anywhere into the framework based on the question asked, or problem to be solved
ICPIA Example Use Cases

- **Support New Threat Analysis** - Explore the impact of previously unidentified threats and vulnerabilities

- **Provide test bed for integrating systems** – upgrading a system and analyze for an improved security posture

- **Help design secure architectures** – evaluating protective measures (detection, deter, respond) such as encryption

- **Act as a training tool** - for Red Team attackers or for Plant Operators to develop event response procedures

- **Identify R&D gaps** – to reduce system risk

- **Supports integrated risk management** - attack difficulty metrics, impact and consequence analysis, moving to “all hazards” analysis
Questions?