INL-CON--19- XXXXX
-Revision-0

5G Wireless Technology

Expediting Wireless Research, Development, Demonstration, Evaluation, Testing, and Training

Dr. Carl Kutsche,
Chief Technology Officer, CISR

www.inl.gov

Idaho National Laboratory

GUIRR 5G Forum

June 12, 2019

Potential Value of 5G Communications to DOE

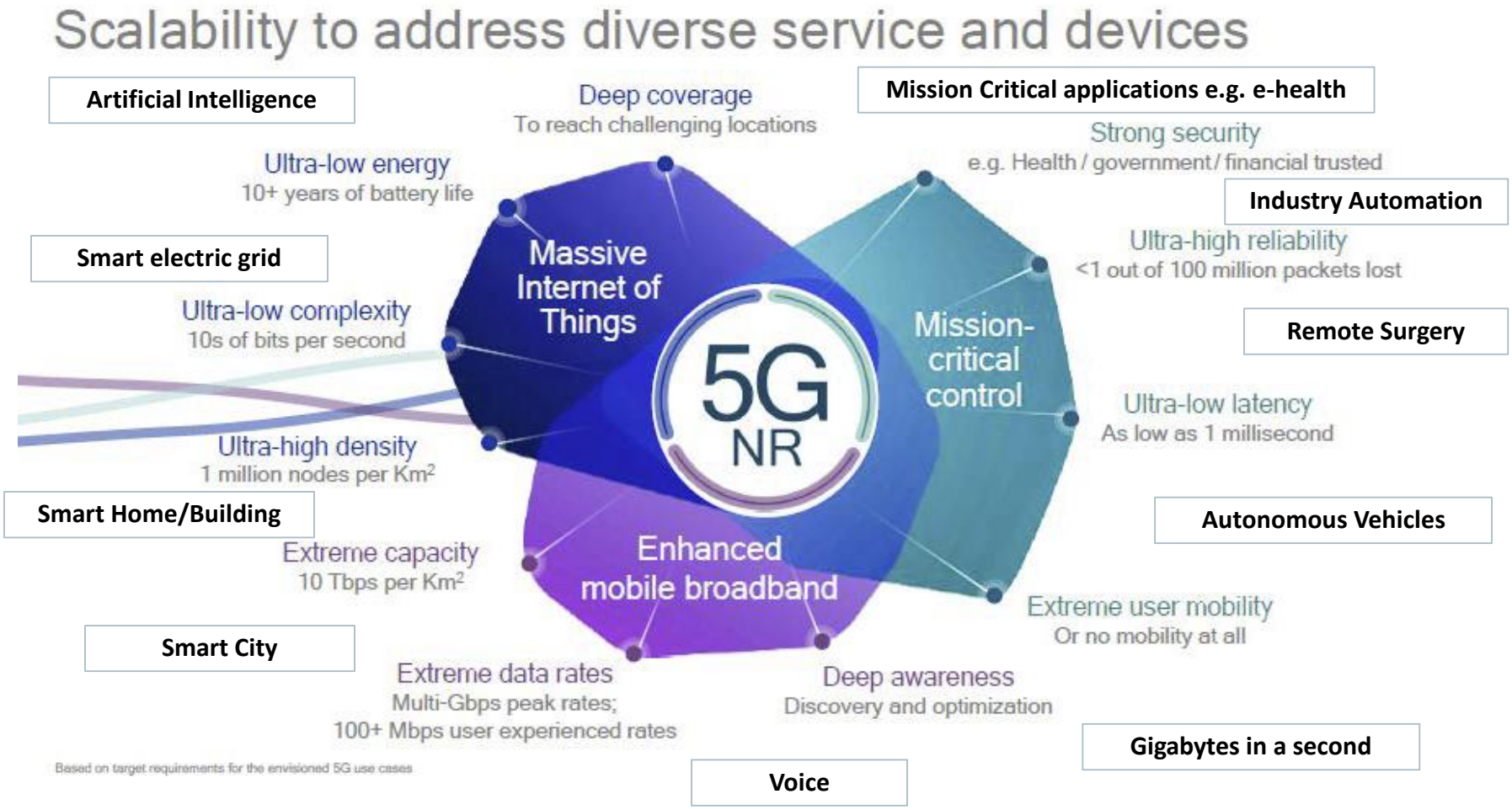
At an investment value of more than $7 billion, DOE is one of the largest users of wireless communications services with over 7,500 radio frequency assignments supporting critical mission, programmatic, and operational requirements

Sensitive Operations Supported

The loss of DOE RF Communications services would undermine the support of critical DOE mission functions, including:

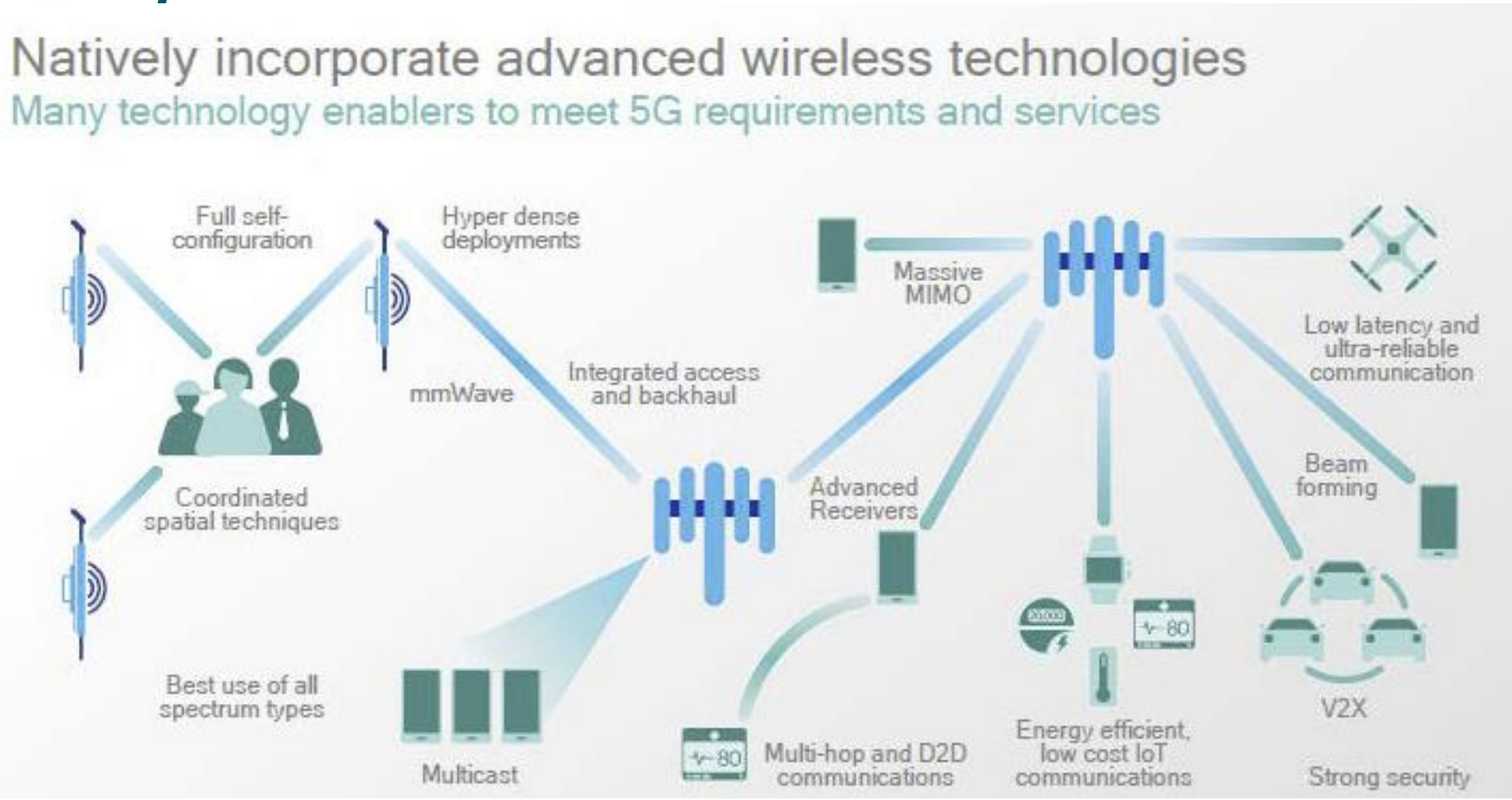
- National Power Grid Control
- Electricity Transmission and Energy Markets
- Disaster Recovery Energy Restoration
- Public and Private Energy Sector Coordination
- Electric Vehicle Adaptive Charging Networks
- Satellite Control for Nuclear Proliferation Detection
- Nuclear Protective Force Communications
- Radiological Assistance
- Nuclear Transportation Safeguards
- Perimeter Protection
- Intrusion Detection
- Environmental Remote Sensing
- Wildlife Monitoring
- Seismic Monitoring, Nuclear Energy
- Radar
- Fusion Energy Research
- Cyclotron Operation
- Remote Controlled Robotics
- Emergency First Responder Communications

A Vendor's* View of Diverse Technology Requirements to Enable 5G & Applications



* Courtesy of Qualcomm Incorporated

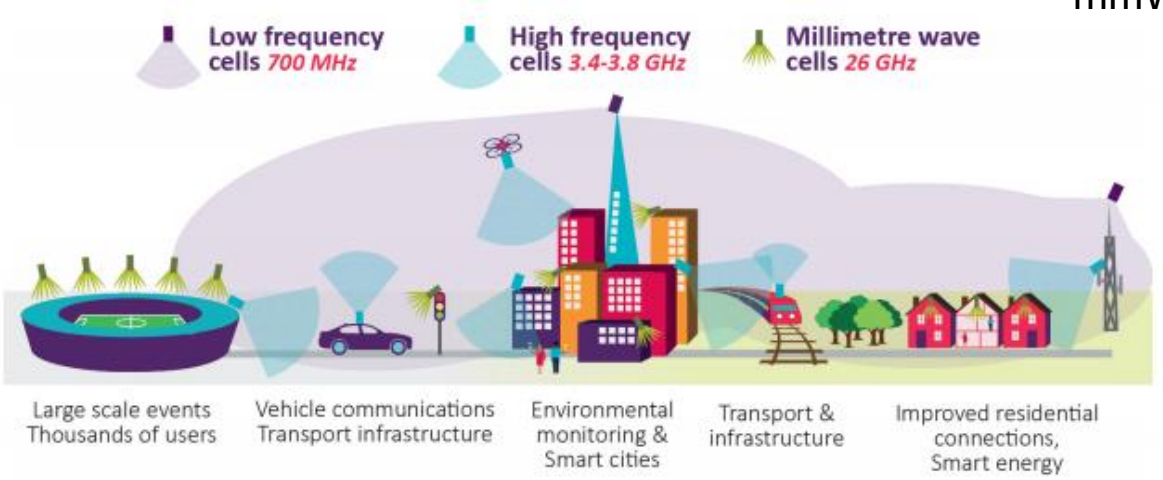
Another View of Diverse Technology Requirements to Enable 5G*



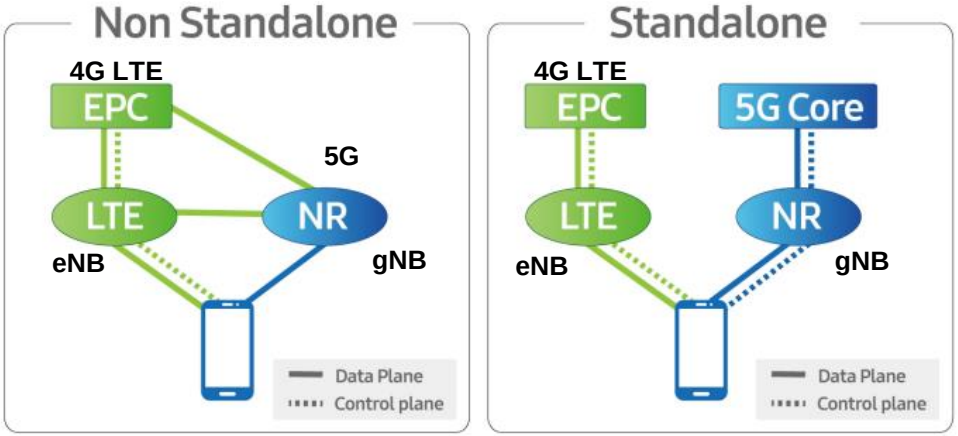
* Courtesy of Qualcomm Incorporated

Where is 5G heading - how research can accelerate it

5G Frequency Ranges and Use Cases:



5G Deployment scenarios:

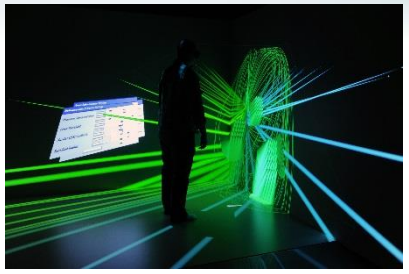


5G NSA (Non Stand Alone) **5G SA (Stand Alone)**

- US Carriers started with fixed 5G with mmWave
  - In the midst of trials with adding 5G to small cells in limited cities
  - Focus is on commercial deployment with
    - newly available licensed spectrum limited coverage
    - limited consideration for security and resiliency
- Identified national need:
  - Research, development, and testing of innovative solutions with
    - 5G NR using broader shared / unlicensed spectrum securely
- Rural and Underserved Communities
- Resilient and secure networks
- International Security Challenges

How will 5G Impact Wireless Security

“The communication sector is an integral component of the US economy and our national security, underlying the operations of all business, public safety and government.” Christopher Krebs, DHS Director of Cybersecurity and Infrastructure Security, 14 May 2019 Senate Judiciary Hearing on 5G



New key capabilities with 5G

- Beam based Air Interface for sub-6GHz and mmWave
- Use of unlicensed and shared spectrum with 5G NR (New Radio)
- 5G enabled IoT[1], connected health, vehicles, UAS etc.
- Edge computing with SDN[2] and NFV[3] for applications including industrial IoT, augmented reality (AR), connected health, and connected vehicles (V2X)

New challenges

- Adapting wireless security to beam based directional transmission
- Increase in illegal and disruptive use of spectrum sharing
- Secure operation of increasing number of connected UAS, ICS, vehicles and handsets
- Secure use of edge connectivity to enable 5G applications

[1] Internet of Things, [2] Software Defined Networking, [3] Network Function Virtualization

Securing Resilient Wireless Communications Networks

Current challenges:

- Communication disruption from both unintended and deliberate interference
- Violation of spectrum sharing rules
- Use of vulnerabilities in wireless spectrum protocols (LTE/WiFi, etc.) to disrupt or degrade services
- Illegal access of subscriber information for spectrum use, user traffic, and protected spectrum databases
- Attack on critical information such as location in a sensor network
- Use of cellular connected UAS/drone to attack critical infrastructure
- Congestion, interference, timing, latency

Approaches for starting mitigation:

- Detection and localization of interference source
- Transmission of content over a large band with very low power levels comparable to noise
- Signaling data link with higher reliability
- Real time spectrum monitoring and RF classification with machine learning
- Cryptographic methods such as authentication and encryption
- Security at the lower/physical layer exploiting uniqueness of wireless transmission
- Detection of unauthorized UAS in sensitive areas

Proposed National Acceleration on 5G Resilience and Security

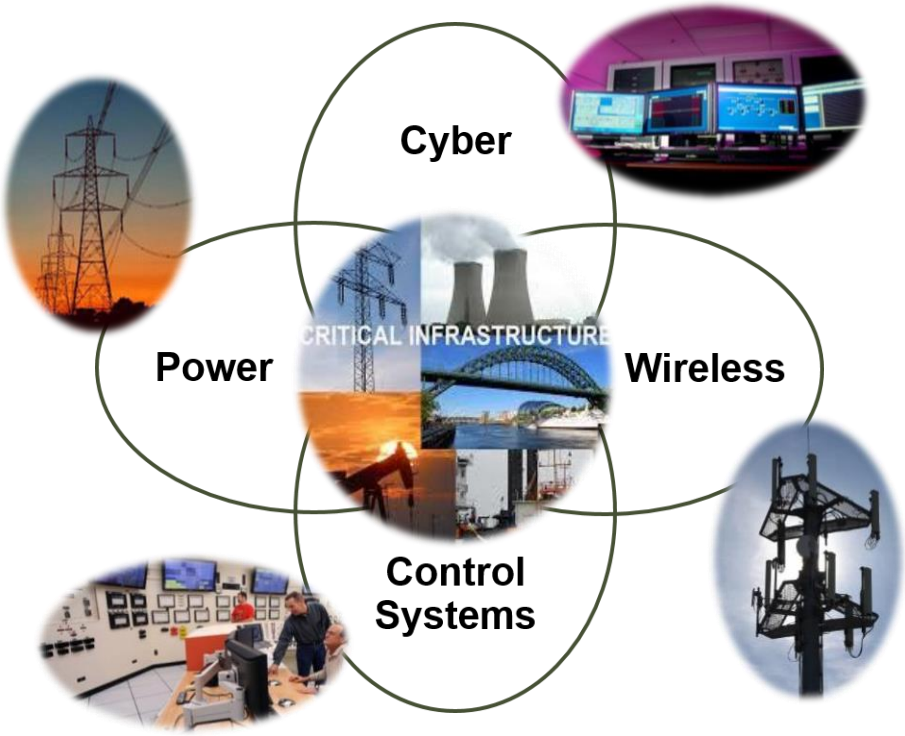
- Public-Private Partnerships
  - Provide focus on most needed capability and policy gaps facing 5G deployment
  - Add visibility to help investments in critical gap areas, spanning the “valley of death”
  - Synergize efforts at all phases from basic research to commercial adoption
  - Continue strong university collaboration on 5G security research

- 5G Evaluation Platforms
  - Identify and characterize wireless security issues that will validate effect and lead to creation of effective solutions
  - Validate in both virtual and full – scale situations
  - Provide stressed and extreme condition wireless network testing
  - Tame the “Wild West” of user and edge devices
  - Wholistic, application-specific evaluation

- Coordinate Addressing Critical Limitations
  - International challenges to system security and data protection
  - Identify the “critical assets” in 5G networks and create a set of disruptive tactics and intrusion tests (“red teaming”) to insure needed mitigations are in place.
  - Concepts helping rural and underserved areas

Idaho National Laboratory

Wireless security and resiliency are essential to protecting the nation's critical infrastructure



Capabilities for Wireless Solutions

Wireless Research:
Develop solutions to national spectrum and wireless communications security challenges

Wireless Modeling & Simulation:
Advanced software engineering, validation and testing of wireless security solution technology design

Wireless Evaluation: Test and validate full-scale deployment of wireless communications security technology solutions

INL Wireless Security Institute

- Low Latency Waveform Development
- Detection of Hostile Drones operated with Commercial Cellular
  - Identify network signatures generated Cellular controlled drones
- LTE Communications Security Assessments and Exploitation
  - Identify vulnerabilities and scenarios that can exploit them
- Wireless RF Signal Identification and Protocol Reverse Engineering
  - Detect rogue energy, classify, and demodulate wireless signals
  - Detect unauthorized use
- Cyber secure mmWave Physical Layer
  - Cybersecurity in millimeter wave communications
- Air-wave LTE and mmWave communications
  - Cellular Drone Swarm Control, Infrastructure to Vehicle Communications

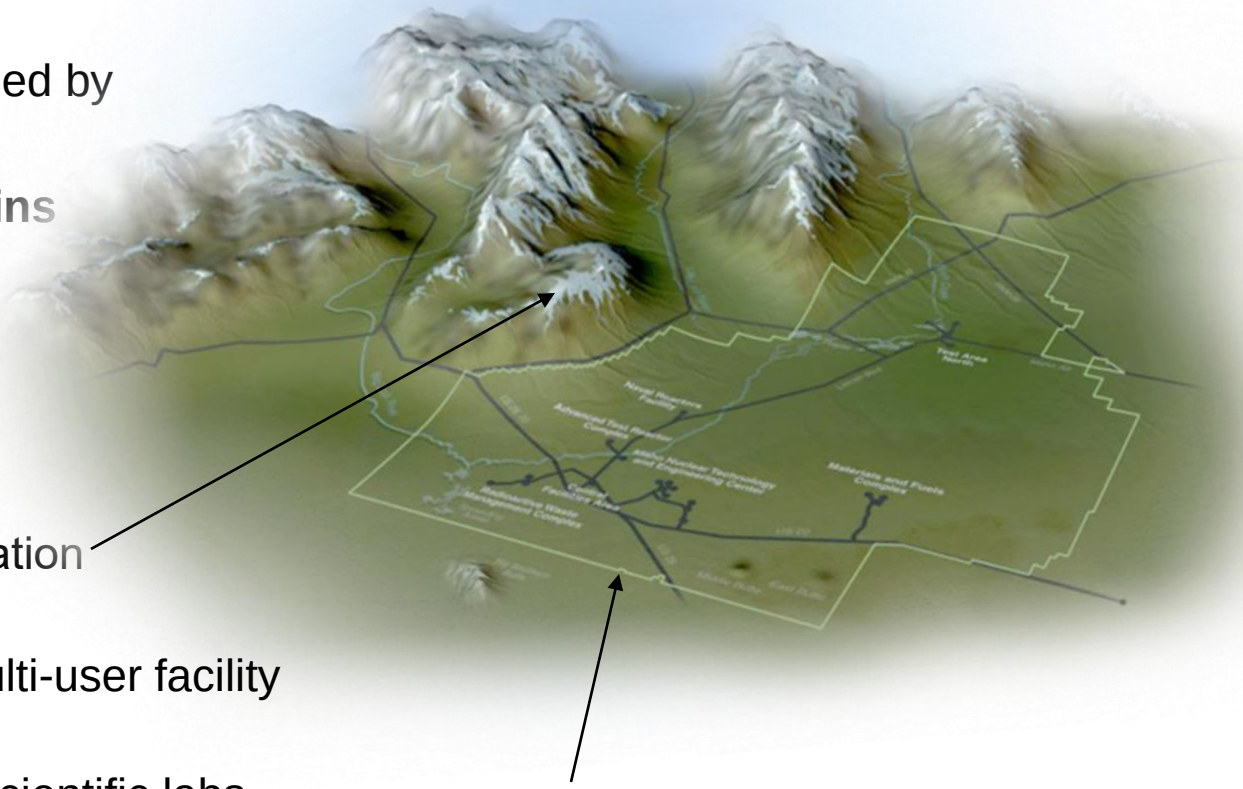
University at Buffalo
The State University of New York

THE UNIVERSITY OF UTAH®

Idaho National Laboratory

INL's 890 Sq. Miles Provides Diverse Opportunities

- **Isolated test range**
  - No nearby military bases, international airports or urban areas
  - Natural RF shield provided by caldera landscape
- **Multiple facilities and terrains**
  - 3 fixed cell sites
  - Numerous test areas
  - Rolling high desert with surrounding mountains
  - 5000' average elevation
  - Radio site at 8628' elevation
  - Controlled access
  - Secure, IP protected multi-user facility
  - Broadband data access
  - Hardware prototyping, scientific labs
- **Unrestricted airspace above 1500' AGL**



INL Test Range Boundary

Idaho National Laboratory

Carl.Kutsche@inl.gov, 208-526-5485