Remarks on Quantum Communications

Richard Hughes
Physics Division, LANL

Los Alamos
NATIONAL LABORATORY

- **Quantum Communications (micro-scale … macro-scale) is an important sub-field of QIS**

- **a National Quantum Information Science Initiative should include a strong Quantum Communications component**

- **"science" ↔ "technology" interplay is essential: <u>both</u> aspects should be included in a National Initiative**

Los Alamos
NATIONAL LABORATORY

The US has vigorous quantum communications research activities in universities, government and corporate labs

BOSTON UNIVERSITY

rle AT MIT RESEARCH LABORATORY OF ELECTRONICS AT MIT

Los Alamos NATIONAL LABORATORY

UNM

UNIVERSITY OF OREGON

Telcordia®

NuCrypt

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

IBM

CALTECH

Berkeley
University of California

MagiQ

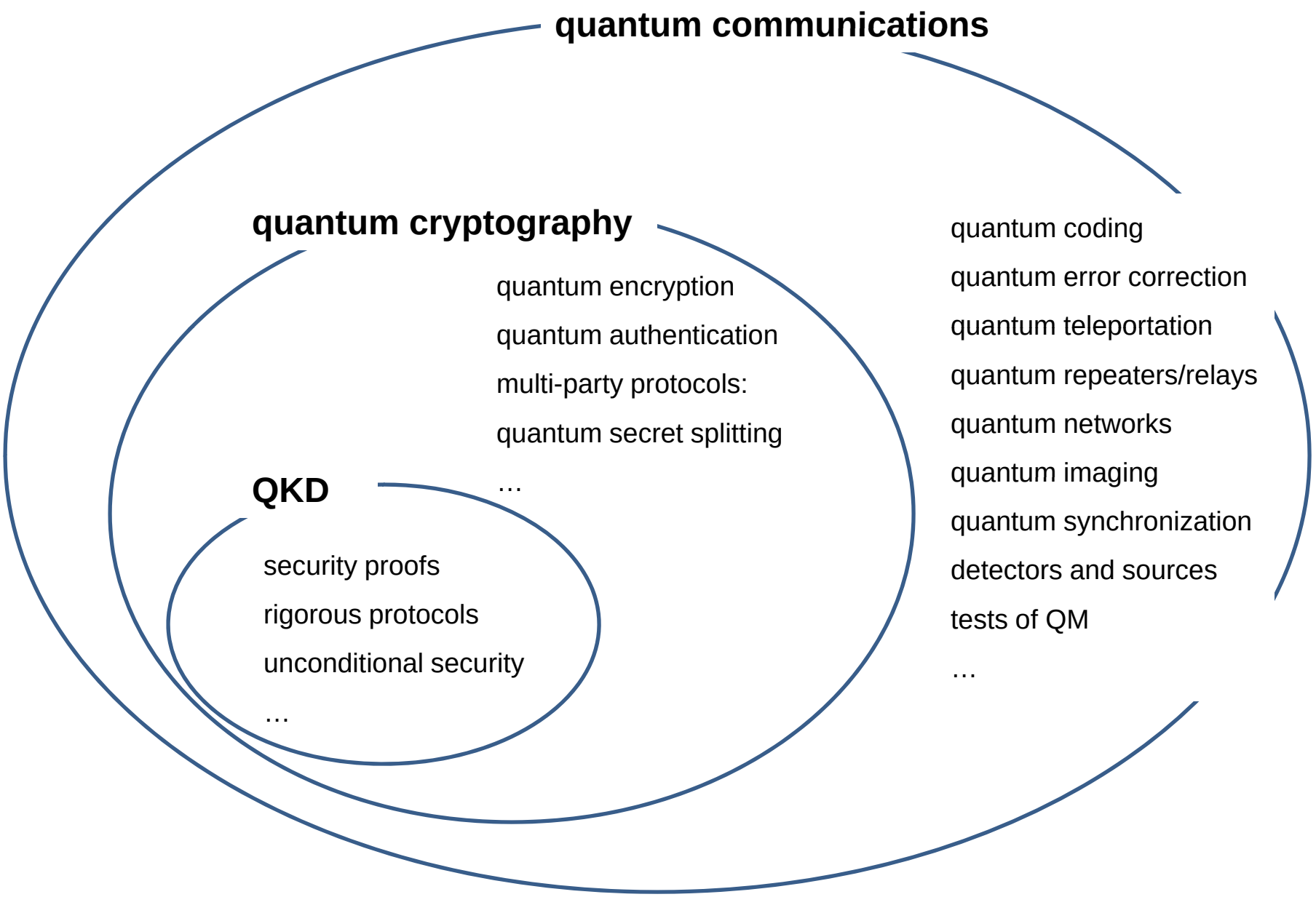
BBN TECHNOLOGIES
A Verizon Company

Princeton Lightwave

OAK RIDGE NATIONAL LABORATORY
Managed by UT-Battelle for the Department of Energy

disclaimer: partial list of institutions only

Fundamental science with great technological potential



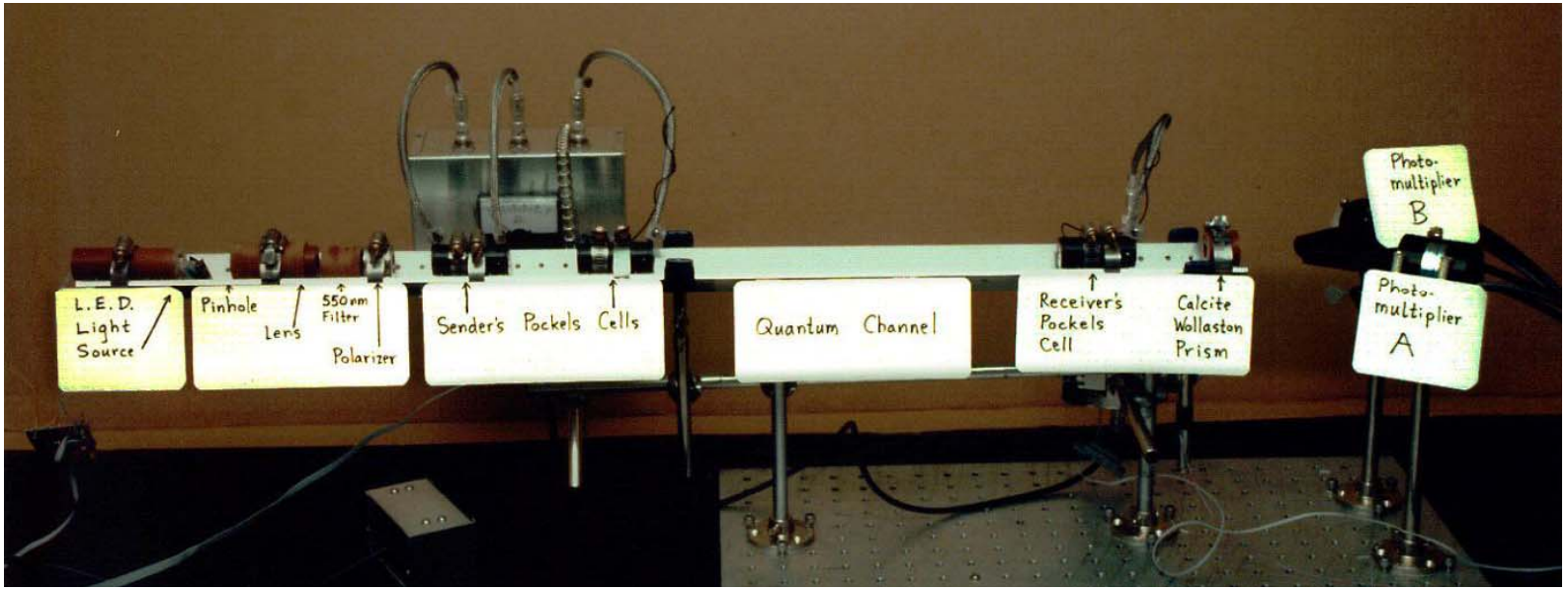
Quantum Key Distribution was invented 25 years ago:

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984

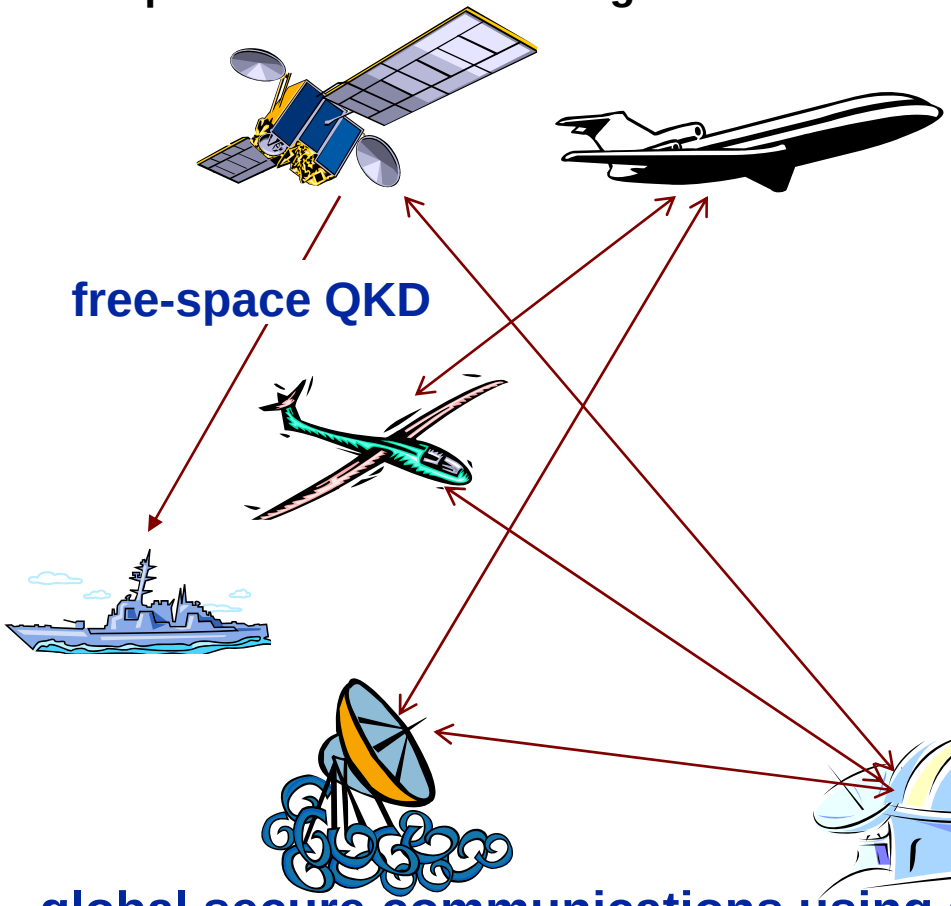
… and first demonstrated 18 years ago: the BBBSS91 experiment

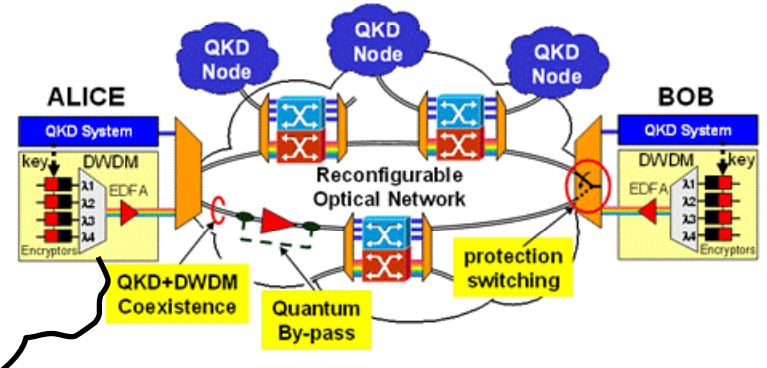


Quantum Key Distribution:
tremendous improvements in security, "domains of use"

Free-space QKD at LANL > 1994

- a methodology that makes free-space & satellite quantum communications possible
- demonstrated in daylight over outdoor ranges optically equivalent to satellite-to-ground





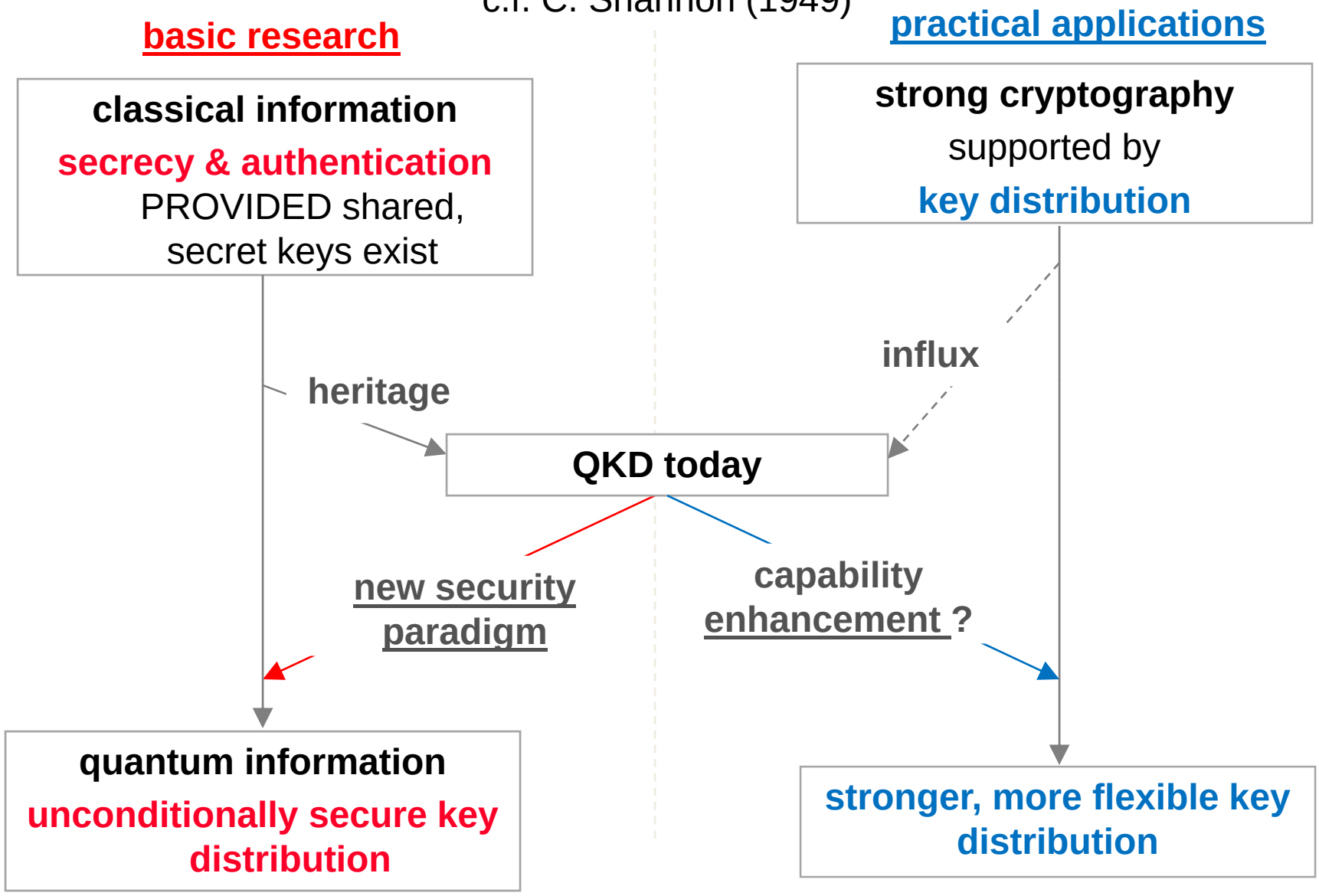
Optical fiber QKD at LANL > 1993

- QKD demonstrated in active transparent enterprise & metro-area networks
- > 140km range demonstrated with ultra-strong security

global secure communications using satellite QKD

QKD is evolving along “science” and “technology” tracks

c.f. C. Shannon (1949)



QKD is not “just engineering”

QKD experiments stimulate fundamental quantum communications research

- **there is no such thing as a "qubit": photons have color, direction, <u>polarization</u>**

- **evolution of QKD security proofs:**

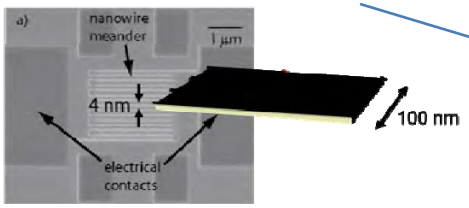
- **QKD continues to be a rich area of fundamental QIS research**

"qubit" ↔ "photon" insights provide deeper understanding of abstract quantum communications concepts, in general

QKD “technology” enables experimental implementation of new quantum communications concepts

“photon” → “qubit” understanding

new sources + detectors



“domains of use”

new quantum communications concepts

satellite-to-ground entanglement distribution

loophole-free tests of Bell inequalities

multi-party quantum cryptography

…

interplay of “science” and “technology” is essential

Quantum Cryptography Research Roadmap: http//qist.lanl.gov

LA-UR-04-4085

ver 1.0 quantum cryptography roadmap released June 2004: QKD focus

- funded by ARDA 2002 – 2005

developed by a Technology Experts Panel

a Research Roadmap:

apply some gentle direction

describe state-of-play and likely progress

identify opportunities and gaps

an aid to the research community and a descriptive tool for program management

A Quantum Information Science and Technology Roadmap

Part 2: Quantum Cryptography

Report of the
Quantum Cryptography Technology Experts Panel

"When elementary quantum systems…are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media."
Charles H. Bennett and Gilles Brassard (1984)

Disclaimer:
The opinions expressed in this document are those of the Technology Experts Panel members and are subject to change. They should not to be taken to indicate in any way an official position of U.S. Government sponsors of this research.

July 19, 2004
Version 1.0

ARDA

SCIENCE ⇔ TECHNOLOGY

Quantum Communications will lead to new technologies aligned with OSTP objectives

Top-level Technology Issues from http://ostp.gov

"The Obama administration and OSTP will develop policies that will:

…

- Protect America's Cyber Networks: Initiation of new and powerful protection strategies to ensure that America's cyber network remains safe from espionage and disruption

…

… the United States must maintain and take full advantage of its technical and strategic superiority in space, which can simultaneously enhance our national security and provide crucial information about environmental and climatologic trends."

Quantum Communications Science and Technology, including QKD, should be parts of a National QIS Initiative

What constitutes a National QIS Initiative ?

- **a more coordinated approach to funding research, across multiple agencies ?**
  - ~ stable funding
- **or something more ?**
  - what will be the scope, objectives, and who will set them ?
- **US QIS researchers should have opportunities to provide input**
- **the process for formulating a National Initiative needs to be transparent**
- **what will be the product of this workshop, who will formulate it, and how will it be used ?**