Maximizing Research Impact

- **Supporting National Priorities**
  - Health IT
  - Smart Grid
  - Financial Services
  - National Defense
  - Transportation
  - Trusted Identities
  - Cybersecurity Education

- **Engaging the Cybersecurity Research Community**

NIST's Healthcare IT Activities

NIST enables **interoperability** and **adoption** by:

- Accelerating **standards** development and harmonization
- Developing a conformance **testing** infrastructure
- Expanding R&D and deployment of **security** protocols

Image: Shutterstock, ©Jenny Horne

- Leveraging testing infrastructure to assist with **certification** process

Leading to an emerging health IT network that is correct, complete, secure and testable.

http://healthcare.nist.gov/ Pubs: http://go.usa.gov/ggmB http://go.usa.gov/ggmQ

Smart Grid
Cyber Security Working Group (CSWG)

- To address the cross-cutting issue of cybersecurity, NIST established the Cyber Security Coordination Task Group (CSCTG) in March 2009.
- Moved under the NIST Smart Grid Interoperability Panel (SGIP) as a standing working group and was renamed the Cyber Security Working Group (SGIP–CSWG).
- The CSWG now has more than 800 participants from the private sector (including vendors and service providers), academia, regulatory organizations, national research laboratories, and federal agencies.
- Smart Grid Interoperability Panel CSWG Wiki http://go.usa.gov/ggmY
- http://www.nist.gov/smartgrid

Financial Services

- December 6, 2010 Memorandum of Understanding signed between DHS Science & Technology (S&T), National Institute of Standards and Technology (NIST), and the Financial Services Sector Coordinating Council (FSSCC) on Cybersecurity Innovation
  - http://go.usa.gov/ggEJ
- The first effort resulting from the MOU is FI-VICS, which is focused on developing and testing an identity proofing gateway concept

National Strategy for Trusted Identities in Cyberspace (NSTIC) Pilots
http://www.nist.gov/nstic/

AAMVA

- Focus: Develop and pilot an identity ecosystem with encompassing governing trust framework around public-private partnership to strengthen private-sector credentials with attributes from a state DMV
- AT&T, Biometric Signature ID, CA Technologies, Microsoft, and Virginia DMV are key partners

Daon

- Focus: deploy smartphone based, multi-factor authentication to consumers
- eBay/Paypal, AARP, Purdue are key relying parties
- A major bank (not yet publicly named) will also be an RP

Criterion

- Focus: develop a viable business model for Identity Ecosystem and attribute exchange
- Broadridge Financial, eBay/PayPal, AOL, Verizon, GE, Experian, Lexis Nexis, Ping, CA, PacificEast are key partners
- A major online retailer (not yet publicly named) will also be an RP

UCAID

- Focus: develop and integrate a privacy-protecting infrastructure that can serve a variety of Identity ecosystem needs; deploy comprehensive, multi-factor authentication across 3 major universities.
- Key partners are Brown and Carnegie Mellon University. MIT, University of Texas, University of Utah are deployment sites

Resilient

- Focus: test "privacy enhancing encryption" infrastructure in health care and K-12 environments.
- AMA, American College of Cardiology, LexisNexis, Knowledgefactor are key partners
- A major entertainment company (not yet named) is also an RP

National Initiative for Cybersecurity Education (NICE)

- Raise national awareness about risks in cyberspace
- Broaden the pool of individuals prepared to enter the cybersecurity workforce
- Cultivate a globally competitive cybersecurity workforce

http://csrc.nist.gov/nice/

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

NCCoE Vision

Provide a world class, collaborative environment for integrating cybersecurity solutions that stimulate e-commerce and national economic growth.

NCCoE Mission

Foster the rapid adoption and broad deployment of integrated cybersecurity tools and techniques that enhance consumer confidence in U.S. information systems.

Key NCCoE Goals:

- Disseminate new principles and mechanics underlying security standards, metrics, and best practices for secure and privacy-preserving information technologies
- Develop and test methods for composing, monitoring, and measuring the security posture of computer and enterprise systems
- Achieve broad adoption of practical, affordable, and useful cybersecurity capabilities across the full range of commercial and government sectors

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

NIST Information Technology Lab
http://www.nist.gov/itl/
Computer Security Division
http://csrc.nist.gov/

Bill Newhouse
william.newhouse@nist.gov