US National Institute of Standards and Technology (NIST)

- Information Technology Laboratory
  
  Computer Security Division
ITL Purpose
Cultivate Trust in IT and Metrology

Division Purpose
Cultivating ITs Roots of Trust
The Importance of Standards

Article I, Section 8: The Congress shall have the power to fix the standard of weights and measures

- National Bureau of Standards established by Congress in 1901
- Eight different “authoritative” values for the gallon
- Electrical industry needed standards
- American instruments sent abroad for calibration
- Consumer products and construction materials uneven in quality and unreliable

Estimated that 80% of global merchandise trade is influenced by testing and other measurement-related requirements of regulations and standards
NIST has two main campuses

Gaithersburg, MD

Boulder, CO

Courtesy HDR Architecture, Inc./Steve Hall © Hedrich Blessing

© Geoffrey Wheeler
NIST Products and Services

Measurement Research
• ~ 2,200 publications per year

Standard Reference Data
• ~ 100 different types
• ~ 6,000 units sold per year
• ~ 226 million data downloads per year

Standard Reference Materials
• ~ 1,300 products available
• ~ 30,000 units sold per year

Calibration Tests
• ~ 18,000 tests per year

Laboratory Accreditation
• ~ 800 accreditations of testing and calibration labs
Cybersecurity Technical Portfolio

- Cryptography
- Risk Management
- Identity and Access Management
- Testing and Validation
- Software Security, Vulnerability Metrics and Configurations
- Emerging Technologies

Persistence – Excellence - Impact
Cryptography

- Use the crypto you will need at end of life, not start of project. Be agile if you can.

- Transitions are coming

- Buy, don’t build; if you can. Buy the good stuff

- Push for interoperability that “up-plays” with your partners
Risk Management

- Speak each other's language through common (standard) mechanisms
  - Cybersecurity Framework/SP 800-53/SP 800-39
  - Express your cybersecurity requirements, understand abilities of shared infrastructures, promote your capabilities – Understand
  - Prioritize to protect mission/business essentials
  - IT Controls != Safety?
  - Leverage Safety, Resilience, Redundancy into cybersecurity capabilities
  - This is a threat model
Identity and Access Management

- Who can access your systems/vehicles/bus/satellites?
  - How do you know?
- What is running on your systems?
  - How do you know?
- What resources are being accessed/used?
  - How do you know?

Good questions to to Protect/Response/Recover/Improve
Vulnerabilities, Configs

- Use of legacy software, hardware, firmware
- Understanding technical vulnerabilities
  - How bad is bad?
- Using secure configurations of software
- Ensuring secure configurations of software
Tools, References and Products

- Papers, Standards, Guidance
- Tools and Testing
  - Software, Cryptography, Identity
- Data References
  - Vulnerabilities, IT Products, Configurations
- Expanded use of GIT Hub, AWS for Distribution
  - Beacon, Test Vectors, SCAP, APPVett, Document Reviews
Find all these resources

https://www.csrc.nist.gov
Publications
Crypto Module Validation Program
NIST Risk Management Framework
Cyber Security Framework

https://www.nvd.nist.gov
Vulnerabilities
Configurations