NIST
Computer Security Division

Matthew Scholl

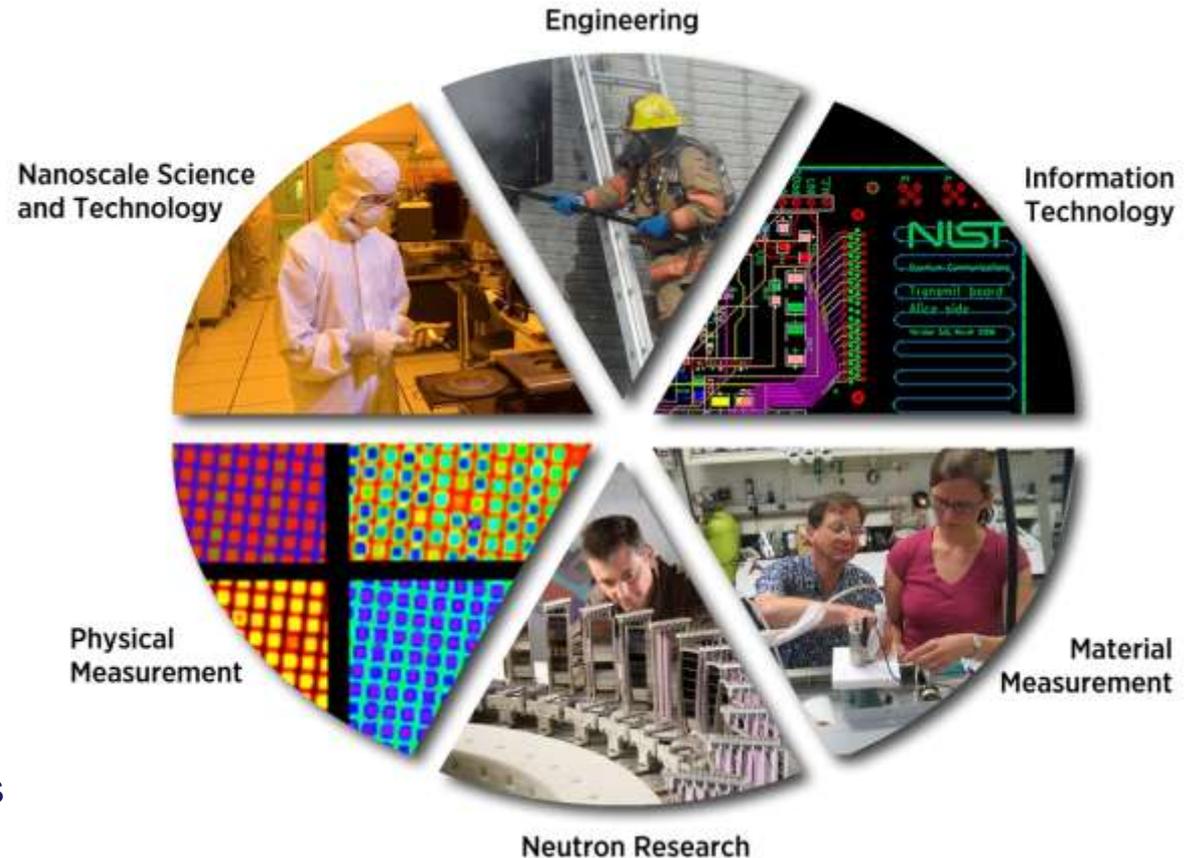June 2012

NIST Laboratories

NIST's work enables

- Science
- Technology innovation
- Trade
- Public benefit

NIST works with

- Industry
- Academia
- Government agencies
- Measurement labs
- Standards organizations

Engineering

Nanoscale Science and Technology

Information Technology

Physical Measurement

Material Measurement

Neutron Research

Computer Security Division

Group	Some Major Activities
Cryptographic Technologies	Secure Hash Competition, Authentication, Key Management, Crypto Transitions, DNSSEC, E-Voting, Quantum Computing,
Security Management and Assurance	FISMA, Health IT, Smart Grid, Supply Chain, NICE, Crypto Validation Programs, Outreach and Awareness
Secure Systems and Applications	Identity Management, Biometric Standards, Cloud and Virtualization Technologies, Security Automation, Infrastructure Services and Protocols
Security Components and Mechanisms	Virtualization, Security Automation (S CAP), Trust Roots, Continuous Monitoring, USGv6
Security Test and Metrics Group	CAVP, CMVP, S-CAP Validation, Attack Graphs, NVD

NIST's Cybersecurity Role in National Priorities

- **Legislation**
  - Federal Information Security Management Act (FISMA) of 2002
  - Cyber Security Research and Development Act (CSRDA) of 2002
  - Help America Vote Act (HAVA) of 2002
  - Energy Independence and Security Act (EISA) of 2007
  - Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

- **Presidential Directives**
  - HSPD-7
  - HSPD-12

- **Office of Management and Budget (OMB) Policy**
  - OMB Circular A-130 Appendix III

- **Administration Priorities**
  - Comprehensive National Cybersecurity Initiative (CNCI)
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)

NIST's Cybersecurity work spans …

- Security Research, Development, and Specifications
- Secure System and Component Configuration
- Test, Validation, and Measurement of Security Properties of Products and Systems
- Cryptographic Technologies
- Security Awareness and Outreach

Biometrics – Software Assurance – Domain Name Security – Identity Management – FISMA – Security Automation – National Vulnerability Database – Configuration Checklists – Digital Signatures – Security Management – Authentication – IPv6 Security Profile – Supply Chain – NICE – Health IT Security – Key Management – Secure Hash – PKI – CNCI – Smart Grid – Continuous Monitoring – Small Business Outreach – Mobile Devices – Standards – Cloud Computing – Usability – NSTIC – Passwords – Hardware Security – Electronic Voting – Wireless – Security Awareness – Vulnerability Measurement – Security Metrics

NIST's Cybersecurity work results in…

- Federal Information Processing Standards
- NIST Special Publications
- NIST Interagency Reports
- Security Models
- Open Software
- Reference & Prototype Implementations
- Journal and Conference Papers
- ANSI, ISO, ITU-T, IEEE, IETF Standards
- Patents
- Conferences and Workshops

Draft Publications
January 2012 – May 2012

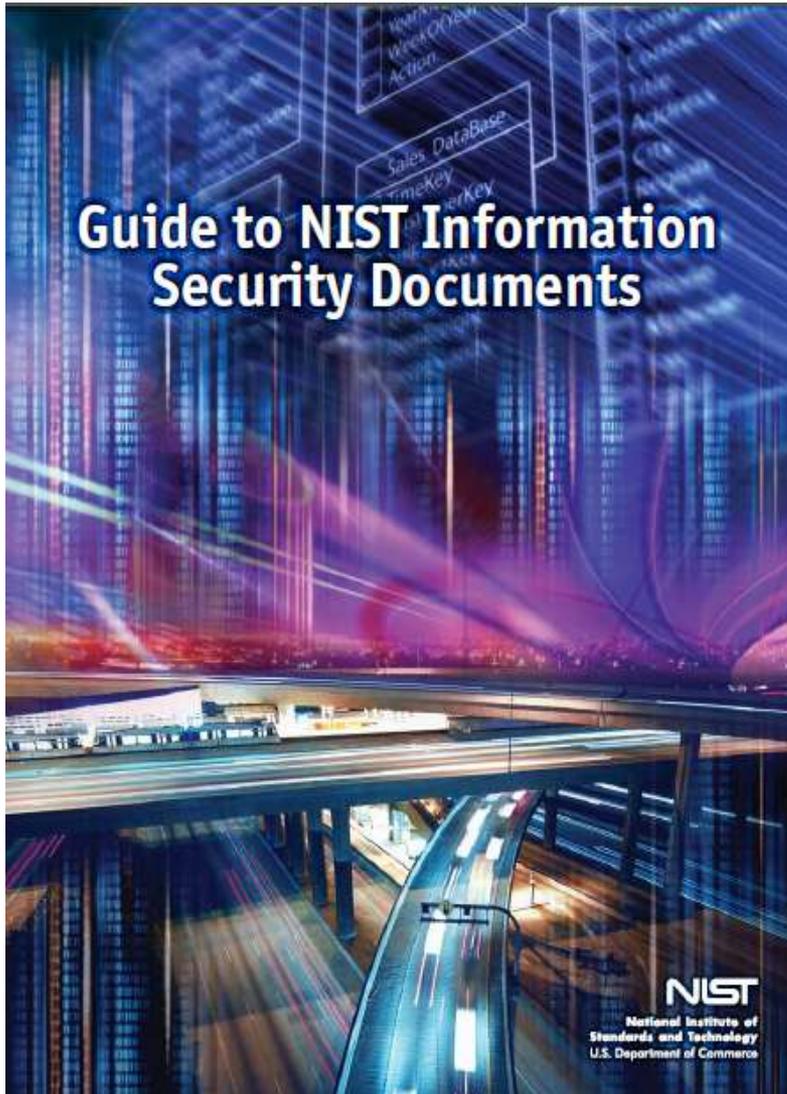| NIST IR	NIST IR-7848	DRAFT Specification for the Asset Summary Reporting Format 1.0	May
	NIST IR-7511 Rev. 3.01.165	DRAFT Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements	April
	NIST IR-7622	DRAFT Notional Supply Chain Risk Management Practices for Federal Information Systems	March
FIPS	FIPS-186 -3 Proposed Change	DRAFT Proposed Change Notice for Digital Signature Standard (DSS)	April

NIST
National Institute of
Standards and Technology

SP	SP 800-130	DRAFT A Framework for Designing Cryptographic Key Management Systems	April
	SP 800-66 Rev.2	An Introductory Resource Guide for Implementing the HIPAA Security Rule	In progress
	SP 800-53 Rev. 4	DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Initial Public Draft)	February
	SP 800-61 Rev. 2	DRAFT Computer Security Incident Handling Guide	January
	SP 800-18 Rev.2	Guide for Development Security Plans for Federal Information Systems and Organization	In progress
	SP 800-159	Guidelines for Access Control System Evaluation Metrics	In progress
	SP 800-XXX	K-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Attacks	In progress

Guide to NIST Information Security Documents

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

- NIST IR 7816, 2011 Computer Security Division Annual Report

- FIPS 180-4, Secure Hash Standard (SHS)

Upcoming/Recent Events

2012

- Technical Aspects of Botnets Workshop, NIST, *May 30*

- Fifth Annual Safeguarding Health Information, Ronald Reagan Building and International Trade Center, *June 6-7*

- National Cybersecurity Center of Excellence Workshop, *June 26*

- ICT Supply Chain Risk Management (SCRM) Workshop, NIST, *July 11-12*

- Cryptographic Key Management Workshop *(Fall 2012-TBD)*

NIST
National Institute of Standards and Technology

Upcoming Events

<u>2012</u>

- Revised Draft FIPS 201-2 Workshop, July 25

- Federal Computer Security Program Managers' Forum, August 9

- NICE "Shaping the Future of Cybersecurity Education" Workshop, NIST, October 30 – November 1

2012

- NSTIC Identity Ecosystem Governance Workshop, March 15

- 25th Annual Federal Information Systems Security Educators' Association (FISSEA) Workshop, March 27-29

- Cybersecurity for Cyber Physical Systems Workshop, April 23-24

National Cybersecurity Center of Excellence (NCCoE)

Mission

To foster an environment that aligns diverse communities to adopt and utilize comprehensive cybersecurity solutions that support immediate, operational needs.

NIST
National Institute of
Standards and Technology