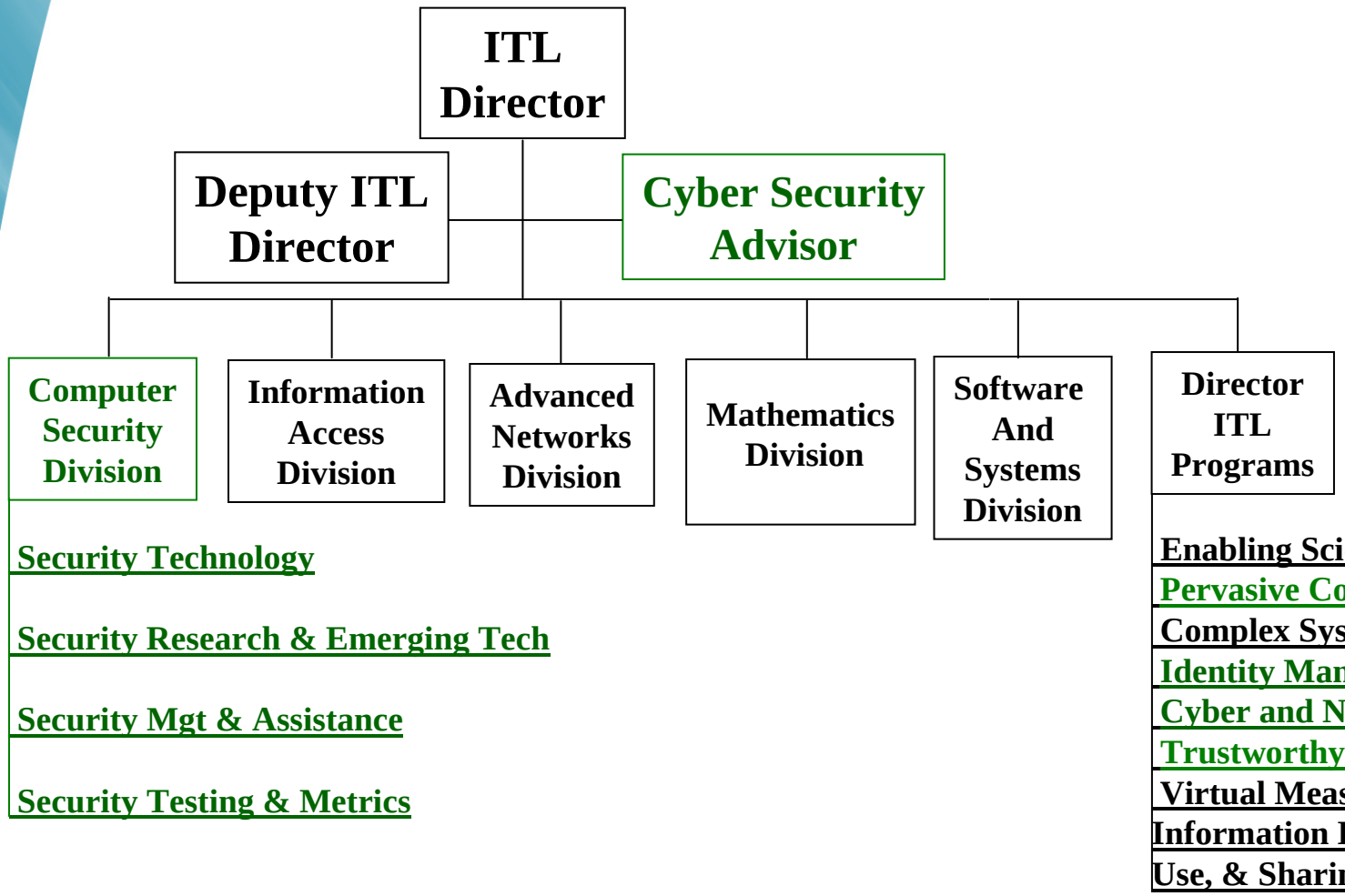
NIST Computer Security Division

Donna F. Dodson
donna.dodson@nist.gov
April 2009

Current Events and NIST CSD

- American Recovery and Reinvestment Act of 2009
- Ominbus Bill
  - STRS
  - Initiatives
- Executive and Congressional Activities
- ITL Programs
- CSD Reorganization

ITL Organization



Computer Security Division Reorganization

Previous

Computer Security Division

- Security Technology Group
- Security Research & Emerging Tech Group
- Security Mgt & Assistance Group
- Security Testing & Metrics Group

New

Computer Security Division

- Cryptographic Technology Group
- Systems and Emerging Technologies Security Research Group
- Security Management and Assurance Group

Computer Security Division 893

Old Mission Statement:

Provide standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems.

New Mission Statement:

Conduct research, development and outreach necessary to provide standards and guidelines, mechanisms, tools, metrics and practices to protect our nation's information and information systems.

Computer Security Division 893

Group 1
Cryptographic Technology Group

Mission Statement

Research, develop and standardize cryptographic mechanisms, protocols, applications and infrastructures to improve both security and interoperability of Information and Information Systems.

Group 2
Systems and Emerging Technologies Security Research Group

Mission Statement

Research and develop advanced methods, guidelines and metrics to mitigate threats, implement national policies, increase operational assurance and improve security management and scaleability.

Group 3
Security Management and Assurance Group

Mission Statement

Define and support specification, assessment and assurance for security properties of information and information systems, information technology products and information security programs through standards, guidelines, outreach, education, awareness and evaluation.

Cryptographic Technology Group Major Projects

- Cryptographic Functions and Protocol Standards
- Voting System Security
- FIPS 140-3
- Wireless Cryptographic Standards
- Key Management Standards & Guidelines
- Authentication

Systems and Emerging Technologies Security Research Group Major Projects

- Policy Machine
- National and International Biometric Standards
- Identity Management System Standards and Research
- IDMS Credential Interoperability
- Combinatorial Testing
- Security Metrics
- Security Automation Content Protocol
- Cloud Computing
- Technical Security Guidance

Security Management and Assurance Group Major Projects

- Extra CSD Activities
- Federal Information Security Management Act (FISMA) Implementation Project
- Healthcare Information Technology Security
- Cryptographic Validation Program
- Information Technology Product Assurance Program

Some 2008 Publications

Final Publications in 2008

- SP 800-124, Oct 2008 *Guidelines on Cell Phone and PDA Security*
- SP 800-123, Jul 2008, *Guide to General Server Security*
- SP 800-121, Sep 2008, *Guide to Bluetooth Security*
- SP 800-116, Nov 2008, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*
- SP 800-115, Sep 2008, *Technical Guide to Information Security Testing and Assessment*
- SP 800-113, Jul 2008, *Guide to SSL VPNs*
- SP 800-108, Nov 2008, *Recommendation for Key Derivation Using Pseudorandom Functions*
- SP 800-87 Rev 1, Apr 2008, *Codes for Identification of Federal and Federally-Assisted Organizations*
- SP 800-79-1, Jun 2008, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)*
- SP 800-73 -2, Mar. 7, 2008, *Interfaces for Personal Identity Verification (4 parts):*
  1- End-Point PIV Card Application Namespace, Data Model and Representation
  2- End-Point PIV Card Application Interface
  3- End-Point PIV Client Application Programming Interface
  4- The PIV Transitional Data Model and Interfaces
- SP 800-68 Rev 1, Oct 2008, *Guide to Securing Microsoft Windows XP Systems for IT Professionals*
- SP 800-67 Ver. 1.1, Jun 2008, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
- SP 800-66 Rev 1, Oct 2008, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*
- *SP 800-64 Rev 2, Oct 2008, Security Considerations in the System Development Life Cycle*
- SP 800-61 Rev 1, Mar 2008, *Computer Security Incident Handling Guide*
- SP 800-60 Rev 1, Aug 2008, *Guide for Mapping Types of Information and Information Systems to Security Categories*: (2 Volumes)
- SP 800-55 Rev 1, Jul 2008, *Performance Measurement Guide for Information Security*
- SP 800-53A, Jun 2008, *Guide for Assessing the Security Controls in Federal Information Systems*
- SP 800-48 Rev 1, Jul 2008, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*
- SP 800-28 Version 2, Mar 2008, *Guidelines on Active Content and Mobile Code*
- NIST IR 7516, Aug 2008, *Forensic Filtering of Cell Phone Protocols*
- NIST IR 7442, Apr 2008, *Computer Security Division 2007 Annual Report*
- NIST IR 7275 Rev. 3, Jan 2008, *Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4*

Other 2008 Publications

Published Drafts in 2008 (Public Comment Drafts)

- SP 800-107, July 9, 2008, *Recommendation for Applications Using Approved Hash Algorithms*
- SP 800-106, July 31, 2008, *Randomized Hashing Digital Signatures* (2d Draft)
- SP 800-102, November 12, 2008, *Recommendation for Digital Signature Timeliness*
- SP 800-82, September 29, 2008, *Guide to Industrial Control Systems (ICS) Security*
- SP 800-70 Rev. 1, September 19, 2008, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*
- SP 800-63 -1, Feb 26, 2008, *Electronic Authentication Guidelines*
- SP 800-57 Part 3, October 24, 2008, *Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance*
- SP 800-41 Rev 1, July 9, 2008, *Guidelines on Firewalls and Firewall Policy*
- SP 800-39, Apr 3, 2007, *Managing Risk from Information Systems: An Organizational Perspective*
- SP 800-37 Rev 1, August 19, 2008, *Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach*
- NIST IR 7511, August 13, 2008, Security Content Automation Protocol (SCAP) Validation Program Test Requirements
- NIST IR 7502, May 30, 2008, *The Common Configuration Scoring System (CCSS)*