



NIST Computer Security Activities

William C. Barker
April 2009

Presentation Overview

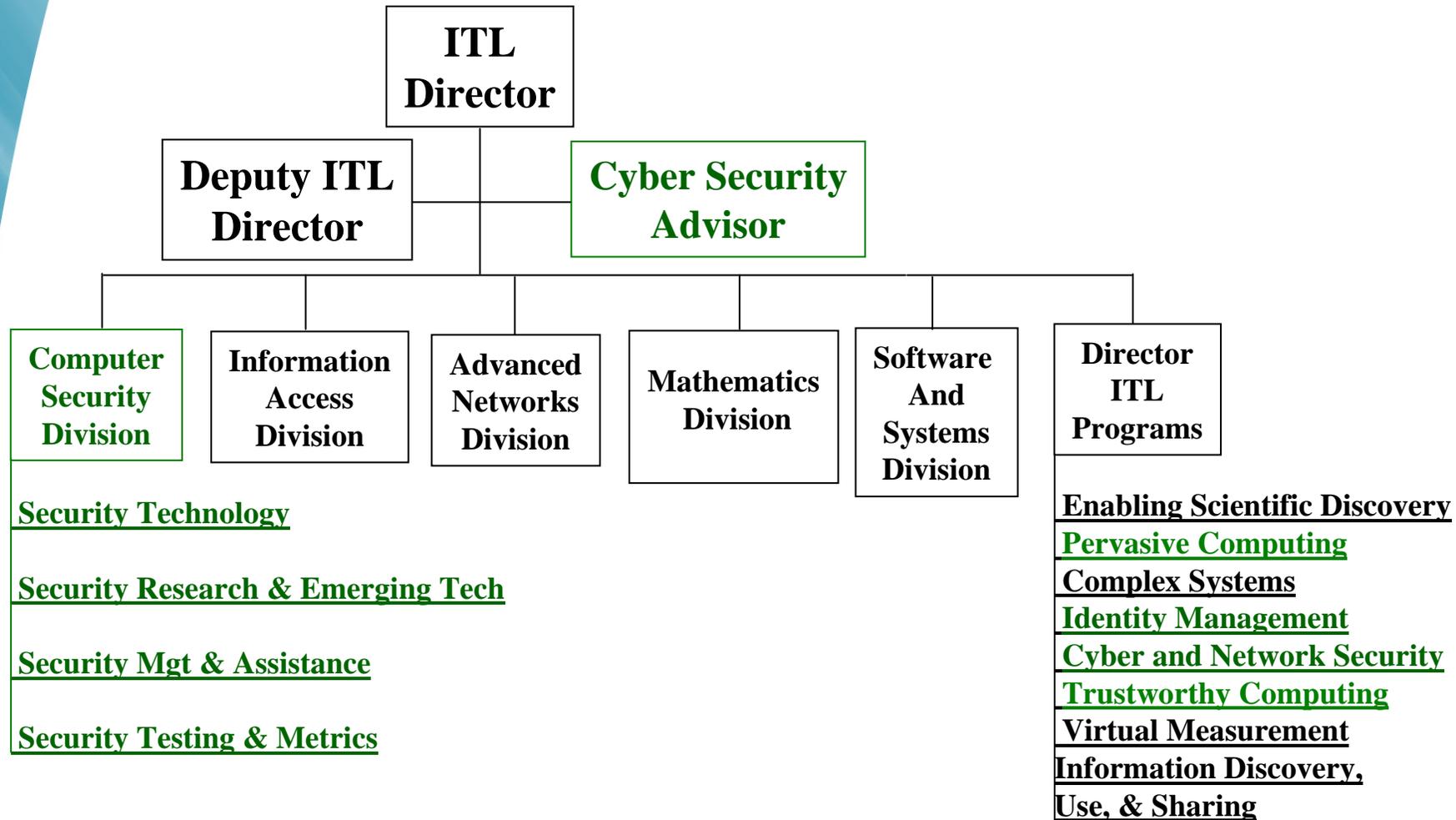
- Information Technology Laboratory
- NIST Basis for Information Security Activities
- Federal Information Processing Standards and Guidelines
- Projects and Initiatives



Information Technology Laboratory (ITL)



ITL Cybersecurity Organization





Computer Security Division (CSD)



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.

Core Focus Area

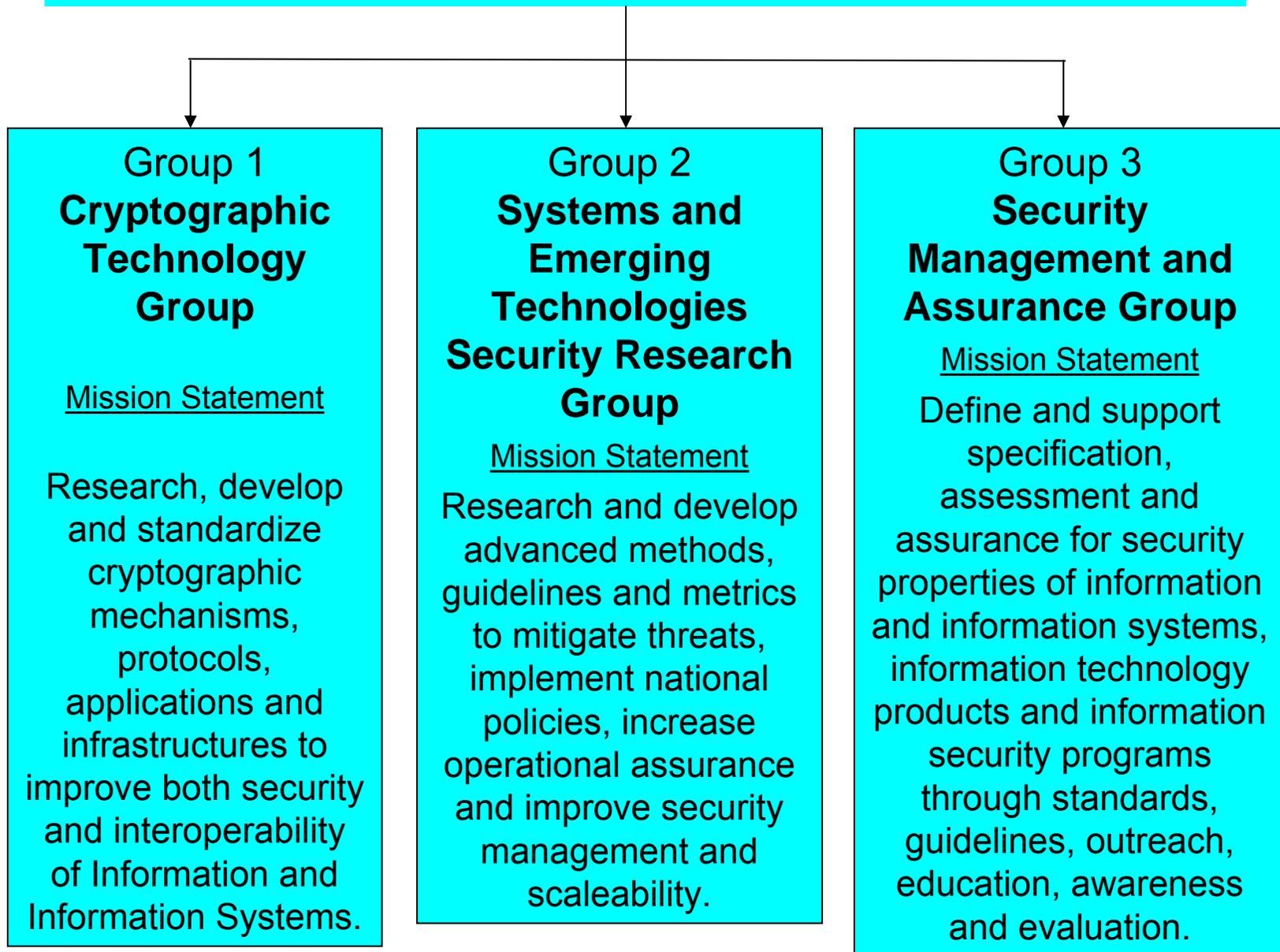
- Research, Development, and Specification
 - Security Mechanisms (e.g. protocols, cryptographic, access control, auditing/logging)
 - Security Mechanism Applications
 - Confidentiality
 - Integrity
 - Availability
 - Authentication
 - Non-Repudiation
- Secure System and Component configuration
- Assessment and assurance of security properties of products and systems

Delivery Mechanism

1. Standards – FIPS, International Consensus, National Consensus
2. Guidelines – SPs, NISTIRs
3. Journal & Conference papers
4. Training
5. Workshops & Conferences – Sponsorship by hosting, and participation in external conferences and workshops
6. Consortia & For a
7. Reference Implementations & Demonstrations
8. Conformance Verification Activities
9. Test, Tools and other conformance determination tools
10. Committee Participation
11. Implementation support



Computer Security Division 893



Community Engagement

Representative Customers and Collaborators



Community Engagement

- Industry
 - Accessing Expertise and Leveraging Resources
 - Coordinating Standards and Initiatives
- Academia
 - Accessing Expertise and Leveraging Resources
 - Representative Institutions and Consortia
- International
 - Formal Standards Groups
 - Accessing Expertise and Leveraging Resources
- Federal, State, and Local Government
 - Interdepartmental
 - Department of Commerce
 - State and Local Governments

Community Engagement Examples

- Chief Information Officers (CIO) Council
- Federal Systems Security Governance Board Member
- National Cyber Study Group (NCSG) Member
- Cyber Security and Information Assurance Interagency Working Group
- Information Security Research Council
- Common Terrorism Information Security Standards Working Group
- Committee for National Security Systems (Observer)
- Information Sharing Environment Enterprise Architecture Security Working Group
- Supply Chain Risk Management Working Group
- Federal Information Systems Security Educators' Association
- Software Assurance Forum
- IT Entrepreneurs' Forum
- Governance Coordinating Council
- Federal Enterprise Architecture Security and Privacy Profile Working Group
- Interagency C&A Transformation Working Group
- Internet Engineering Task Force (IETF) Security Chair
- International Organization for Standardization (Chair/Convener several Committees, Work Groups, and Task Forces)
- American National Standards Institute
- International Committee for Information Technology Standards (Biometrics Chair)
- Biometrics Consortium Co-Chair
- National Science & Technology Council Committee on Biometrics and Identity Management (Co-Chair)



NIST Basis for Information Security Activities

NIST Responsibilities for Cyber Security

- NIST is responsible for *developing standards and guidelines*, including minimum requirements, that provide adequate information security for all agency operations and assets in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, but such standards and guidelines shall not apply to national security systems.
- Under FISMA NIST shall "*conduct research*, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security."
- NIST develops *guidelines consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems*, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.
- In accordance with the Cyber Security Research and Development Act, The National Institute of Standards and Technology *develops, and revises as necessary, checklists setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system* that is, or is likely to become, widely used within the Federal Government.
- Homeland Security Presidential Directive 7; "The Department of Commerce will *work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts*, including using its authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements."
- Homeland Security Presidential Directive 12: "The Secretary of Commerce shall promulgate in accordance with applicable law a Federal *standard for secure and reliable forms of identification* (the "Standard")"



Federal Information Processing Standards and Guidelines

NIST Information Technology Standards

- Information Technology (IT) Standards and Guidelines for the Federal Government
 - Public Information
 - Coordinated in a Public Forum
 - IT Security Standards Mandatory for Non-National Security Agencies
 - Harmonized With National Security Community to Support Information Sharing
 - Voluntary for States, Localities, Industry, and Consensus Standards Organizations
- Public and Industry “Buy-in” to Foster Widespread Implementation
- Technical Source of IT Security Expertise for Federal Agencies
- Collaborative Access to International IT Security Expertise in Industry, Academia, and Standards Organizations
- Government-wide vs Community-specific Focus

Examples of Standards Applicability

- NIST Federal Information Processing Standards and Guidelines
 - Mandatory for Non-NSS Federal Agencies
 - Harmonization with NSS Standards
 - Voluntary for Industry and State and Local Governments
- Federal Agency Standards and Regulations
 - Domain-specific
 - Regulatory Agency Mandates for Industry and Public
- National and International Consensus Standards Bodies (E.g., ISO, ITU, INCITS, ANSI)
 - Usually voluntary
 - Some nations mandate (e.g., ISO by Japan)
- Internet Engineering Task Force (IETF) (Voluntary)
- Industry-specific Standards Bodies - E.g., IEEE (Generally Voluntary)
- Industry Associations - E.g., Smart Card Alliance, Security Industry Assn, International Biometrics Industry Association (Usually Binding for Members)



Some Recent NIST Standards (See csrc.nist.gov for latest publications)

- Federal Information Processing Standards
 - FIPS 201-1: *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Updated June 2006
 - FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
 - FIPS-198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, July 2008
 - FIPS-180-3, *Secure Hash Standard (SHS)*, October 2008
 - Draft FIPS 186-3 *Digital Signature Standard (DSS)*, November 2008
 - Draft FIPS 140-3, *Security Requirements for Cryptographic Modules*, July 2007



Current Priorities

Key Security Initiatives

- Executive Initiatives
 - Comprehensive National Cybersecurity Initiative and 60 Day NSC Study
 - SmartGrid
 - Healthcare IT
- Other Executive Priorities
 - Cloud Computing
 - Citizen Facing Authentication
 - Automated Security Configuration Compliance Determination
- Industry/Security Community Initiatives
 - Product Assurance Reform
 - Government-wide Security Controls and Processes



Some Other Key Security Projects and Initiatives

- Research
 - Technical Cyber Security Mechanisms
 - Secure Network Protocols
 - Biometrics Technologies and Metrics
- Standards
 - Technical Cyber Security Guidelines
 - Secure Network Protocol Standards and Guidelines
 - FISMA and Executive Policy Conformance Standards and Guidelines
 - Biometrics and Identity Management Standards and Guidelines
- Implementation Support
 - FISMA Implementation Support
 - Executive Policy Implementation Support
 - Technical Support to Homeland Security Programs and Initiatives
- Test and Evaluation
 - Biometrics Performance and Interoperability Testing
 - Cryptographic Conformance Testing
 - IT System Security Configuration & Conformance Tool Test & Validation
 - Identity Management Interoperability Conformance Determination

Future and Ongoing Challenges

- Long Term Research
 - Advanced Cryptography (e.g., hash, public key, quantum, light footprint)
 - Inherently Secure, High Assurance, and Provably Secure Systems and Architectures
 - Composable and Scalable Secure Systems
 - Autonomic Systems
 - Ad-hoc Networks and Wireless Security
 - Network Measurement and Visualization Tools
 - Secure Distributed Systems
 - Infrastructure for Information Security R&D

Identity Management Activities

- Personal Identity Verification Program
- Support to Other Federally Sponsored Activities
 - TWIC
 - E-Passport
 - WHTI
- ISO/IEC 24727
- ISO SC 27 Biometric Standards Activities
- OECD Support
- Laboratory Research Program

Product Assurance

- Criteria/Requirements/Controls
 - Standards
 - Profiles
 - Claims
 - Derived Test Requirements
 - Documentation Requirements
- Conformance Demonstration Process
 - Assertion with Procurement Enforcement
 - Independent Testing (Qualification or Acceptance)
 - Third Party Validation
- Reciprocity
 - Interagency
 - NSS/Non-NSS Federal
 - National Cross-Jurisdictional (E.g., States, Localities)
 - International
- Life Cycle Considerations
 - Development Environment
 - Installation and Configuration
 - Life Cycle Configuration Management



Some Additional Cyber Security Projects

- Information Systems Security Lines of Business
 - FISMA Reporting
 - Certification & Accreditation
 - Tier I Awareness
 - Tier II Training
 - Situational Awareness and Incident Response (SAIR)
 - Enterprise Architecture Security
- Protective Programs and R&D Group
- DHS Essential Body of Knowledge Review
- DHS Sector Specific Plan (SSP) Reviews
- Supply Chain Risk Management (SCRM) Working Group
- Governance Coordinating Council Working Group
- IPv6 Standards/Guidelines/Support
- National Infrastructure Protection Plan Information Technology Sectors Review
- SP 800-30 Rev. 1 Guideline for Information System Risk Assessments
- Policy Machine Development
- National Vulnerability Database (NVD)
- Security Content Automation Protocols (SCAP)
- Open Vulnerability Assessment Language (OVAL) Development {SCAP funding}
- The Common Vulnerabilities and Exposures (CVE) Project* {SCAP funding}
- Personal Identity Verification (PIV) Program (HSPD-12)
- First Responder Identification activities (First Responder Authentication Cards (FRAC))
- Transportation Workers Identification Credentials (TWIC) Data Model and Card Interface Conformance Test Development*
- ANSI-Homeland Security Standards Panel Work Group on Credentialing and Access Control for Disaster Management
- National Infrastructure Protection Plan, Sector Specific Plan areas for IT
- SP 800-16 (NIST Role-based Training Guideline) Assistance to Immigration & Customs Enforcement, Transportation Security Administration, Customs & Border Protection and DHS "headquarters"



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)*

For Additional Information

- NIST
 - <http://www.nist.gov/>
- NIST's Information Technology Lab
 - <http://www.itl.nist.gov/>
- Computer Security Resource Center
 - <http://csrc@nist.gov>
- National Vulnerability Database
 - <http://nvd.nist.gov>
- Biometrics Resource Center
 - <http://www.itl.nist.gov/div893/biometrics>
- Biometrics Research
 - Finger: <http://fingerprint.nist.gov>
 - Face: <http://face.nist.gov>
 - Iris: <http://iris.nist.gov>

Thank You!

William C. Barker
Chief Cyber Security Advisor
100 Bureau Drive
Gaithersburg, MD 20899-8930

Telephone: 301-975-8443

E-Mail: wbarker@nist.gov