NIST Information Technology Laboratory
Computer Security Division

Mission

– 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.
Major FY07 Activities

- Key Initiatives
  - Secure Hash
  - Security Metrics
  - Security Content and Other C&A Automation Initiatives
  - Federal Desk Top Security Configuration Activities
  - Security Product Assessment Requirements and Methods
- Security support to ITL and other NIST programs
  - Voting
  - Health Care IT
  - ITL Program Initiatives
    - Support Identity Management Program
    - Help establish other programs (e.g., Cyber Security, Trustworthy Networking, Trustworthy Software)
- Maintenance of existing body of standards and guidelines in response to evolution of threat technologies and institutional environments
- Integrate support to national and international standards bodies (e.g., ANSI, ISO, IEEE, IAB/IETF, ICAO)
- General technical support to requests from OMB and other EOP organizations, GAO and Congressional staff, individual Departments and Agencies, other DoC organizations, and other NIST organizations (e.g., CNSS, TWIC, WHTI, E-Passport, REAL ID).
Current Challenges

- Cryptographic Algorithms (Long Range)
  - Public Key Cryptography in Quantum Computing Environment
  - Symmetric Key Management for Large and Complex Communications Environments
  - Light Footprint Algorithms
- Access Control
  - Login Passwords, Tokens, and Biometrics
  - Single Sign-on
  - Electronic Physical Access Control
  - Policy Machine
  - Vendor Support
  - Product Assessment vs Module Validation
- Harmonization of Federal standards and guidelines with IC/NSS requirements
- Defense against electronic identity fraud
- Balancing standards mission against implementation support requirements
Division Structure

- Division Office
  - Overall division management
  - Coordination of support to ITL programs
  - 4 Federal employees

- Security Technology
  - Security mechanisms’ development, standards, and guidelines
  - 18 Federal employees, 5 Guest Researchers

- Security Research and Emerging Technologies
  - Security applications research, security guidelines, security checklists
  - 19 Federal employees, 6 Guest Researchers

- Security Management and Assistance
  - Security Management standards, guidelines, and outreach
  - 17 Federal employees

- Security Testing and Metrics
  - Cryptographic algorithm module validation program management
  - 11 Federal employees
Security Technology Group

IT Security Mechanisms

**Goal**: Develop and improve mechanisms to protect the integrity, confidentiality, and authenticity of Federal agency information by developing security mechanisms, standards, testing methods, and support infrastructure requirements and methods.

**Programs**:
- Security Mechanism Standards Toolkits
  - Cryptographic Standards
  - Password Mechanisms
- Cryptographic Key Infrastructures
- Develop measures of effectiveness
- Applications Support
  - E-Authentication
  - Voting Systems (with SDCT)

**FY07 Staff**: 18 Employees, 5 Guest Researchers

**Basis for Program Priority**:
- Help America Vote Act (10/02)
- PITAC Cyber Security Report lists authentication technologies at top of R&D priority list (2/05).
- NIST FY 2007 Budget Request cites encryption standards technical expertise and response to statutory assignments as having saved industry $1 billion (2/06).
- CSIA Federal Plan for Cyber Security and Information Assurance R&D lists authentication and cryptography among its top funding priorities (4/06).

**FY07 Priorities**: Secure Hash Algorithm replacement research, Password Guideline Revision, E-Authentication and Key Management Guidelines.

Security Research and Emerging Technologies Group

IT Security Research and Applications

**Goal:**
Devise advanced security methods, tools, and guidelines through conducting near and midterm security research.

**Programs:**
- Security Research
  - Access Control and Policy Management
  - Automation Assistance to FISMA Reporting (Security Content Automation)
  - Ad hoc Networks and Wireless Security
  - Combinatorial Testing (Pseudo exhaustive)
  - Quantum Crypto Protocols
- National Vulnerability Database
- Protection of Personally Identifiable Information (PII)
- Security Related Protocol Standards.
- Identity Management (PIV, Smart Cards and Biometrics)
- Operating Systems and Applications Security Hardening Guidelines
- Technical Guidelines for Federal Agencies

**FY07 Staff:** 19 Employees, 1 Student, 6 Guest Researchers

**Basis for Program Priority:**
- Research, modeling, and reference implementation builds vital competencies
- FISMA, Cyber Security R&D Act, and prior legislation directs NIST to conduct research in support of its national role of providing security standards and guidelines to Federal Agencies (12/02).
- PITAC Cyber Security Report (2/05)
- HSPD-7 and HSPD-12 are driving the most resource intensive FY07 activities.

**FY07 Priorities:** Security metrics program initiation, security configuration guidelines, wireless security, secure use of RFIDs, security in quantum computing environments, electronic identity standards and guidelines.

Security Management and Assistance Group

IT Security Management

Goal:
Provide computer security guidelines to ensure sensitive government information technology systems and networks are sufficiently secure to meet the needs of government agencies and the general public.

Programs:
• Standards and Guidelines
• Outreach
• Additional Initiatives

FY07 Staff: 17 Employees

Basis for Program Priority:
• The FISMA Implementation Project was established in January 2003 to produce security standards and guidelines required by FISMA.

Basis for Program Priority (continued):
• Cyber Security: Innovative Technologies for National Security are identified in the Research Initiatives for President’s Innovation Agenda.
• The Information Security and Privacy Advisory Board founded in accordance with 15 U.S.C. 278g-4, pursuant to the Federal Advisory Committee Act, 5 U.S.C.
• Appendix III to OMB Circular No. A-130 charges the Secretary of Commerce to develop and issue appropriate standards and guidelines for the security of sensitive information in Federal computer systems.

FY07 Priorities: FISMA implementation guidelines and support, product security assessment requirements development, update of guideline documents.

Cryptographic Testing & Validation

**Goal:**
Improve the security and technical quality of cryptographic products needed by Federal agencies (U.S., Canada, and UK) and industry, by developing standards, test methods & validation criteria, and the accreditation of independent third party testing laboratories.

**Programs:**
- Cryptographic Module Validation Program (CMVP)
- Cryptographic Algorithm Validation Program (CAVP)
- Test tools and algorithm & protocol test suite development
- Cryptographic Module Testing Laboratory and Personal Identification Verification laboratory accreditation
- Security Testing Research

**FY07 Staff:** 11 Employees

**Basis for Program Priority:**
- NIST FY 2007 Budget Request cites encryption standards technical expertise and response to statutory assignments as having saved industry $1 billion (2/06).
- CSIA Federal Plan for Cyber Security and Information Assurance R&D lists authentication and cryptography among its top funding priorities (4/06).
- ISO19790: Security Requirements for Cryptographic Modules accepted as an international standard (5/06).

**FY07 Priorities:**
- FIPS 140-3 publication, maintain effectiveness of cryptographic algorithm and module validation programs, incorporate NIST personal identity verification program test validation, establish basis to support future NVLAP-based product assessment validation activities.

**Products:**
FY06 Formal NIST Publications
(See [csrc.nist.gov](http://csrc.nist.gov) for latest publications)

- Special Publication 800-87: *Codes for the Identification of Federal and Federally-Assisted Organizations*, October 2005
- NISTIR 7250: Cell Phone Forensic Tools: An Overview and Analysis," October 2005
- Special Publication 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005
- Special Publication 800-83: *Guide to Malware Incident Prevention and Handling*, November 2005
- Special Publication 800-77: *Guide to IPsec VPNs*, December 2005
- NISTIR 7275: "Specification for the Extensible Configuration Checklist Description Format (XCCDF)," January 2006
- Special Publication 800-76: *Biometric Data Specification for Personal Identity Verification*, February 2006
FY06 Formal NIST Publications (Continued)

- Special Publication 800-73 Revision 1: *Interfaces for Personal Identity Verification*, March 2006
- Special Publication 800-85A: *PIV Card Application and Middleware Interface Test Guidelines* (Special Publication 800-73 compliance), April 2006
- FIPS 201-1: *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Updated June 2006
FY06 Formal NIST Publications (Continued)

- Special Publication 800-85B: *PIV Data Model Test Guidelines*, July 2006
- NISTIR 7337: “Personal Identity Verification Demonstration Summary,” August 2006
- Special Publication 800-84: *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- Published Drafts [Public Review]: 16 Special Publications (plus two FIPS revisions)
FY07 Formal NIST Publications

- Special Publication 800-89: *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006
- Special Publication 800-76-1: *Biometric Data Specification for Personal Identity Verification*, January 2007
FY07 Formal NIST Publications

- Draft Special Publication 800-82 (Second Public Comment): Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, June 2007
- Draft FIPS 140-3, Security Requirements for Cryptographic Modules, July 2007
- Draft Special Publication 800-41 Ver 2: Guidelines on Firewalls and Firewall Policy, July 2007
- Draft Special Publication 800-70 Ver 2: NIST National Checklist Program for IT Products—Guidelines for Checklist Users and Developers, July 2007
- Draft Special Publication 106, Randomized Hashing Digital Signatures, July 2007
- Draft Special Publication 800-113: Guide to SSL VPNs, August 2007
- Draft Special Publication 800-48 Ver 2: Wireless Network Security: IEEE 802.11a/b/g/n, Bluetooth, and Other Technologies, August 2007
- Draft Special Publication 800-28 Ver 2: Guidelines on Active Content and Mobile Code, August 2007
- Draft Special Publication 800-xx: The Information Security Automation Program (ISAP), August 2007
Thank You!

William C. Barker
Chief, Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

wbarker@nist.gov
http://csrc.nist.gov