Information Technology Laboratory Computer Security Division (CSD)
Computer Security Resource Center (CSRC)
NIST National Institute of Standards and Technology

Please take a moment to fill out our survey. This survey is in regards to the CSRC website. Your input on how to improve the CSRC website is beneficial for us and also to improve our services to you. Please **click here** to go to the survey form which is located on CSRC. In advance, we appreciate your time for filling out this survey.

About CSD:

- Mission Statement
- Projects / Focus Areas
- CSD staff
- Location
- **Publications**
  - Special Publications
  - FIPS
  - NIST IRs
  - ITL Security Bulletins
- Advisories / Alerts

CSRC Website:

- **New!** Infosec in the SDLC
- **New!** Program Review for Information Security Management Assistance (PRISMA)
- **New!** Mobile Ad Hoc Network Security (MANET)
- Knowledge Based Authentication Symposium
- Spam Technology Workshop
- FISMA Implementation Project
- Security Certification and Accreditation
- Practices & Checklists Implementation Guide
- Wireless Security
- ASSET
- Awareness, Training and Education
- Cryptographic Standards Toolkit
- Federal Agencies

Program Areas
CSD's work is grouped into five major categories, described below. A more complete listing of research areas is given here.

- NIST Computer Security - **PUBLICATIONS**

- **Cryptographic Standards and Applications:**
  Focus is on developing cryptographic methods for protecting the integrity, confidentiality, and authenticity of information resources.....
  - Advanced Encryption Standard (AES)
  - Cryptographic Standards Toolkit
  - Encryption Key Recovery and S/MIME
  - Public Key Infrastructure (PKI)

- **Security Testing:**
  Focus is on working with government and industry to establish more secure systems and networks by developing, managing and promoting security assessment tools, techniques, services, and supporting programs for testing, evaluation and validation.....
  - Automated Security Self-Evaluation Tool (ASSET)
  - Cryptographic Module Validation Program (CMVP)
  - IPSec
  - National Information Assurance Partnership (NIAP)

- **Security Research / Emerging Technologies:**
  Focus is on research necessary to understand and enhance the security utility of new technologies while also working to identify and mitigate vulnerabilities.....

CSRC Website Highlights

- Would you like to receive e-mail notification(s) when NIST releases new security publications? Click here to learn more about it and how to subscribe to this list.

CSD News:
(dates in bold reflects when announcement was posted)

- **August 25, 2004** --
  Researchers have recently announced they have discovered a new way to break a number of cryptographic hash algorithms. Click here to read NIST's brief comments on recent cryptanalytic attacks on secure hashing functions and the continued security provided by SHA-1. SHA-1 is one of the hash functions specified in the Secure Hash Standard, Federal Information Processing Standard 180-2.

- **August 25, 2004** --
  NIST invites and requests nominations of individuals for appointment to the Information Security and Privacy Advisory Board (ISPAB). The call for nominations can be found here. The Board advises the Director of NIST, the Secretary of Commerce and the Director of OMB on information security matters.

- **August 19, 2004** --
  On October 6 and 7, 2004: NIST, with co-sponsorship from Department of Homeland Security (DHS) and the National Cyber Security Partnership's Coordinating Committee, will hold a Common Criteria Users' Forum (CCUF) at L'Enfant Plaza in