Security Testing, Validation, and Measurement
Computer Security Division
Information Technology Laboratory

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

- **NIST's Mission Statement:**
  To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

- **Information Technology Laboratory Mission Statement:**
  To promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics.

- **CSD 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.

Information Technology Laboratory

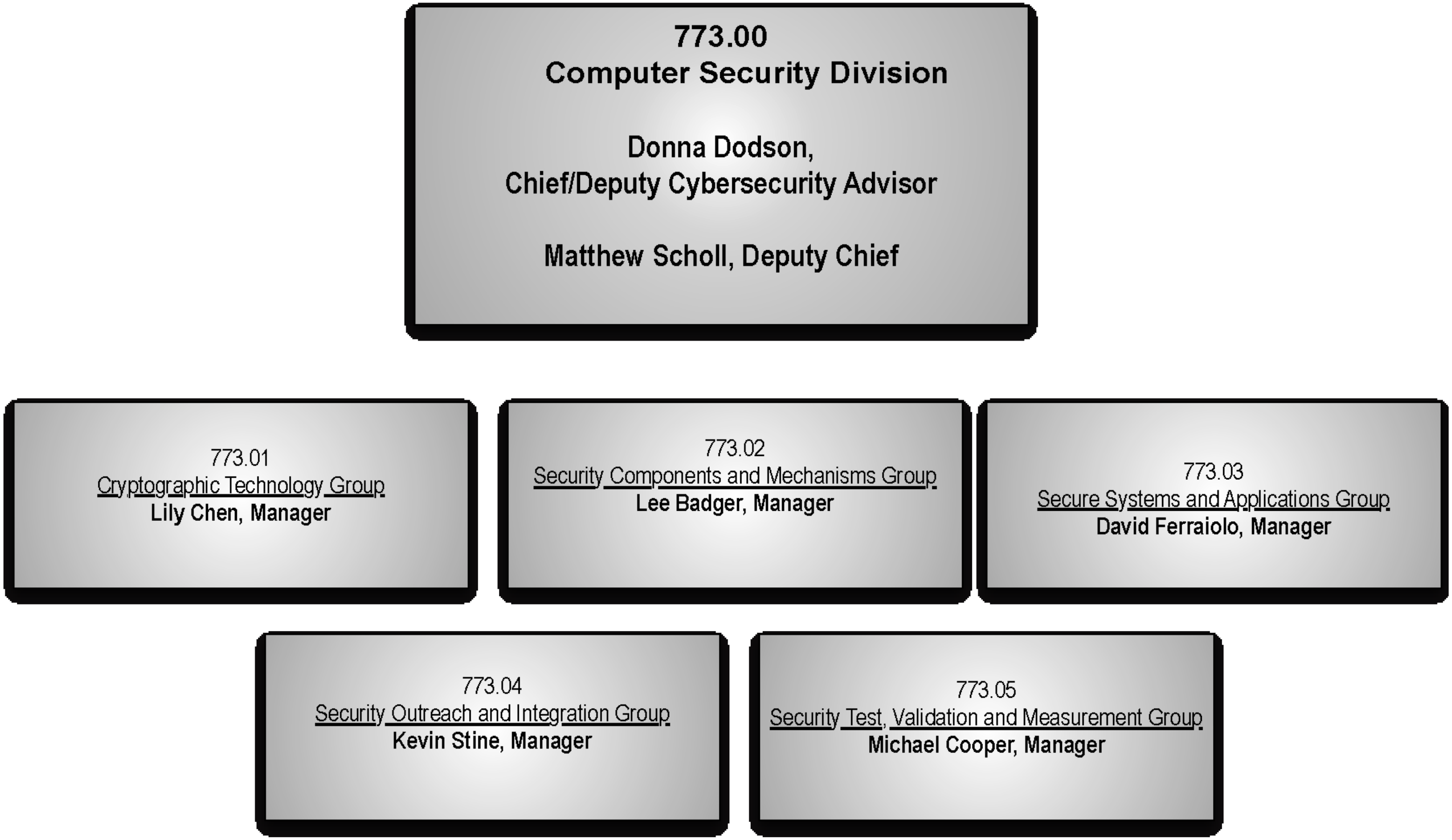
To advance the development and productive use of information technology

- tests
- test methods
- reference data
- proof of concept implementations
- technical analyses

COMPUTER SECURITY DIVISION

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



773.00
Computer Security Division

Donna Dodson,
Chief/Deputy Cybersecurity Advisor

Matthew Scholl, Deputy Chief

773.01
Cryptographic Technology Group
Lily Chen, Manager

773.02
Security Components and Mechanisms Group
Lee Badger, Manager

773.03
Secure Systems and Applications Group
David Ferraiolo, Manager

773.04
Security Outreach and Integration Group
Kevin Stine, Manager

773.05
Security Test, Validation and Measurement Group
Michael Cooper, Manager

COMPUTER SECURITY DIVISION (773)

- **CRYPTOGRAPHIC TECHNOLOGY GROUP (773.01)**: Research, develop, engineer, and standardize cryptographic algorithms, methods, and protocols.
- **SECURITY COMPONENTS AND MECHANISMS GROUP (773.02):** Research, develop and standardize foundational security mechanisms, protocols and services.
- **SECURE SYSTEMS AND APPLICATIONS GROUP (773.03):** Integrate and apply security technologies, standards and guidelines for computing platforms and information systems.
- **SECURITY OUTREACH AND INTEGRATION GROUP (773.04):** Develop, integrate and promote the mission-specific application of information security standards, guidelines, best practices and technologies.
- **SECURITY TESTING, VALIDATION AND MEASUREMENT GROUP (773.05):** Advance information security testing, measurement science, and conformance.

SECURITY TESTING, VALIDATION AND MEASUREMENT GROUP (773.05)
VALIDATION PROGRAMS

- CAVP – Cryptographic Algorithm Validation Program – Sharon Keller
- CMVP – Cryptographic Module Validation Program – Randy Easter
- SCAP – Security Content Automation Protocol Validation Program – Melanie Cook
- PIV – Personal Identity Verification Validation Program – Hildy Ferraiolo

Cryptographic Standards

- Block Ciphers
- Random Number Generation
- Digital Signatures
- Key Agreement & Transport
- Key Management
- Advanced Hash Algorithm Competition
- Hash Algorithms

Cryptographic Algorithms

Algorithms authorized for use by the US Civilian Agencies are specified in

- FIPS 186-3 Secure Hash Standards
- FIPS 197 Advanced Encryption Standard
- FIPS 198-1 Keyed Hash Message Authentication Code

FIPS-Validated Cryptographic Modules

- Cryptographic modules *may* be embedded in other products
  - Applicable to hardware, software, and firmware cryptographic modules
  - Must use the validated version and configuration
  - e.g. software applications, cryptographic toolkits, postage metering devices, radio encryption modules

- Does <u>not</u> require the validation of the larger product
  - Larger product is <u>deemed compliant to requirements </u>of FIPS 140-2

Division Projects

- Cyber Physical Systems (CPS)
- FISMA Implementation
- Health IT Security
- Supply Chain Risk Management (SCRM)
- Voting
- FIPS 201
- Biometrics
- Continuous Monitoring
- Privacy
- Authentication
- SCAP
- Hardware Roots of Trust
- Automated Combinatorial Testing

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