Cybersecurity Innovation Forum

National Institute of Standards and Technology
Information Technology Laboratory
Computer Security Division
Security Testing, Validation, and Measurement

Michael Cooper – Manager STVM

September 11, 2015

ITL Organization Overview

Charles H. Romine, Director

Deputy Director
Jim St. Pierre

Executive Officer
Alex Folk

Senior Management Advisor
Susan Loar

Chief Cybersecurity Advisor
Donna Dodson

Chief of Staff and Associate Dir for Federal and Industrial Relations
Kamie Roberts

Associate Director for Program Implementation
Ron Boisvert, Actg.

Senior Internet Policy Advisor
Adam Sedgewick

Assistant Director for Boulder
Jack Wang, Actg.

Applied & Computational Mathematics
Ron Boisvert

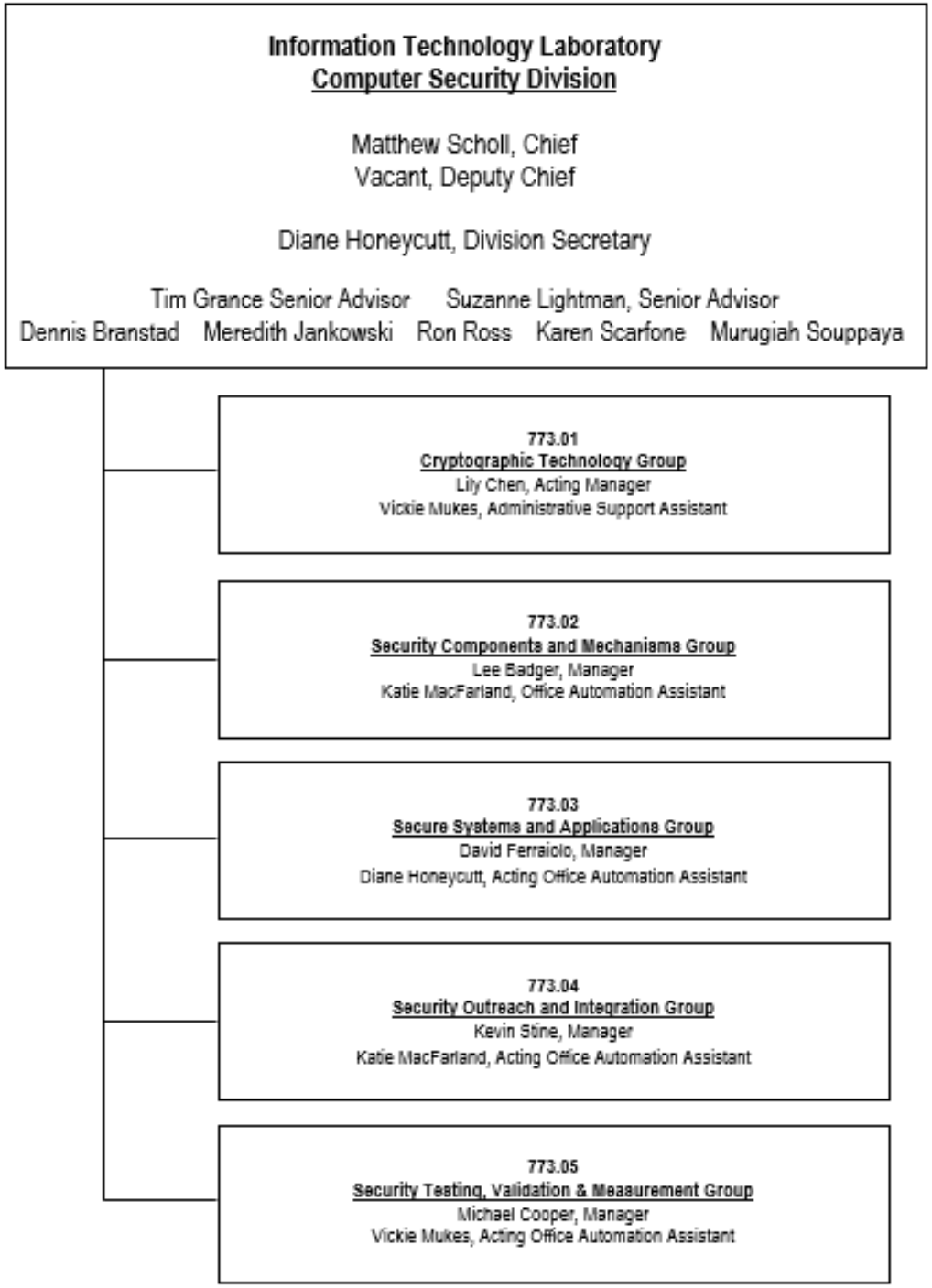
Advanced Network Technologies
Abdella Battou

Computer Security
Matthew Scholl

Information Access
Shahram Orandi

Software and Systems
Ram Sriram

Statistical Engineering
Will Guthrie


Information Technology Laboratory
Computer Security Division
Matthew Scholl, Chief
Vacant, Deputy Chief
Diane Honeycutt, Division Secretary
Tim Grance Senior Advisor
Suzanne Lightman, Senior Advisor
Dennis Branstad
Meredith Jankowski
Ron Ross
Karen Scarfone
Murugiah Souppaya
773.01
Cryptographic Technology Group
Lily Chen, Acting Manager
Vickie Mukes, Administrative Support Assistant
773.02
Security Components and Mechanisms Group
Lee Badger, Manager
Katie MacFarland, Office Automation Assistant
773.03
Secure Systems and Applications Group
David Ferraiolo, Manager
Diane Honeycutt, Acting Office Automation Assistant
773.04
Security Outreach and Integration Group
Kevin Stine, Manager
Katie MacFarland, Acting Office Automation Assistant
773.05
Security Testing, Validation & Meaasurement Group
Michael Cooper, Manager
Vickie Mukes, Acting Office Automation Assistant

Testing Group Mission

Advance information security testing, measurement science, and conformance.

STVM's testing-focused activities include validating cryptographic algorithm implementations, cryptographic modules, and Security Content Automation Protocol (SCAP)-compliant products; developing test suites and test methods; providing implementation guidance and technical support to industry forums; and conducting education, training, and outreach programs.

Programs in STVM

- CAVP – Cryptographic Algorithm Validation Program
- CMVP – Cryptographic Module Validation Program
- SCAP – Security Content Automation Protocol Validation Program
- PIV – Personal Identity Verification Validation Program

- NVD – National Vulnerability Database
- NCP – National Checklist Program
- USGCB – US Government Configuration Baseline
- Metrics Research – shared with the math division

Testing Programs: CAVP

- Tests each individual algorithm implementation against the associated standard.
- Test tool – Crypto Algorithm Validation System (CAVS)

Testing Programs: CMVP

- Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules.
- CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against FIPS 140-2.
- NIST's Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

Testing Group Functional Areas

- Research - Apostol Vassilev
  - Applied research of best security testing methodologies
  - Development of US and International Security Testing standards
  - Outreach to industry and academia
- Operations – Melanie Cook
  - Program Management – Contract management, Communications, etc
  - Validation Services – test report assignment and review
  - Quality Assurance – lab audits, quality metrics, artifacts, processes
  - Education – on standards, processes, tools
- Development – Gini Khalsa
  - Test tool development
  - Automation of Testing Processes

System Security Technology Stack

- Enterprise – all IT systems within an organization
- System – a suite of applications, products, and networks grouped logically
- Network – interconnected set of set of applications or products
- Application / Product – hardware or software crypto implementation that can be procured
- Protocol – i.e. TLS
- Scheme – i.e. key agreement scheme
- Module – container for protection of crypto algorithm implementations
- Algorithm – based on NIST SP or FIPS
- Component – testable parts of an algorithm

System Security Testing Coverage

	Hardware	Software	Hybrid	Virtual	Mobile
System					
Application					
Protocol					
Scheme					
Module					
Algorithm					
Component					

Security Testing Timeline

- Need to engage developers earlier in the lifecycle
- Need to give credit for development practices that provide assurance
- Need to provide automated verification tools for later in the lifecycle

Design – Development – Testing – Integration - Release – Installation – Operation – Retirement

Commercial Product Lifecycle

Testing Programs

- Defined roughly around technology layers, from the bottom up
- Integration of testing processes between layers/programs is difficult
  - Need research into integration testing processes at each layer into next higher layer
- Need research into root-of-trust assurances at the lowest layer to provide foundation for higher layers
  - What artifacts and evidence can be produced by hardware vendors to make supply chain assurances
- Need research into best-of-class test methodologies applicable to all programs/layers and aimed at improving the depth of testing without additional overhead to the programs
- Need research into applied technologies that could benefit the testing programs by eliminating difficult to measure/test aspects
  - Use SCAP capabilities to enable automated tests that can verify the assurances

Testing Coverage

- New technologies/embodiments create new challenges to testing that have not been fully studied
- Need to create a strong assurance case at the lowest level of the technology stack
- Need to automate testing workflow to drive down costs to vendors
- Need to interface with other testing regimes to input/output testing data
  - NIAP at application and system level
  - FISMA at system and enterprise level
- Need to develop testing tools that make integration testing at each layer easy for developers and labs
- Need to develop test methodologies and corresponding tools that automate and improve the depth of testing at each layer

ISO/IEC 19790

- Federal Register Notice – published August 12, 2015 with a 45-day comment period
  - Encourage comments from labs, vendors and other interested parties
- Comment review – 4 – 6 weeks – end of November
- US Standards necessary to support the ISO
  - FIPS 140-3 wrapper to point to ISO and to SP
  - SP 800-175D Management Manual
  - NISTIR 8019 Implementation Guidance

ISO Standard Impacts and considerations

- Pay to use standard
- Give the vendor the choice as to which validating authorities receive test data
- NIST/CSE Agreement
  - Need to change language that prohibits the sharing of test data to allow if authorized by the vendor.
- We will develop our public facing web application to support interactions between multiple validating authorities

NIST / NIAP relationship

- Working on reestablishing the Inter-agency agreement
- Technology stack – Nist responsible for lower layers, NIAP the upper
- Adoption of OS Protection Profile
- FIPS points to EAL2 which no longer exists

Miscellaneous topics

- Validation time limits – 5 years to match CRADA
- Tiered validation approach (Vendor affirmed; Lab tested; CMVP validated)
- Allow interpretation of the standard to support best security practices