NIST
Computer Security Division

Donna F. Dodson

July 2011

Proposed Re-organization

Computer Security Division

Donna Dodson, Chief/Deputy Cybersecurity Advisor
Matthew Scholl, Deputy Chief

Group 1
<u>Cryptographic Technology Group</u>
William Polk, Manager

Research, develop, engineer, and standardize cryptographic algorithms, methods, and protocols

Group 2
<u>Security Components and Mechanisms Group</u>
Lee Badger, Actg. Manager

Research, develop and standardize foundational security mechanisms, protocols and services

Group 3
<u>Secure Systems and Application Group</u>
David Ferraiolo, Manager

Integrate and apply security technologies, standards and guidelines for computing platforms and information systems

Group 4
<u>Security Outreach and Integration Group</u>
Kevin Stine, Actg. Manager

Develop, integrate and promote the mission-specific application of information security standards, guidelines, best practices and technologies

Group 5
<u>Security Test, Validation and Measurement Group</u>
Matt Scholl, Actg. Manager

Advance information security testing, measurement science, and conformance

Draft Publications
January 2011 – July 2011 (1)

JUNE	SP 800-63 Rev.1 – DRAFT Electronic Authentication Guideline
	NIST IR 7698 – DRAFT Common Platform Enumeration: Applicability Language Specification Version 2.3
	NIST IR 7697 – DRAFT Common Platform Enumeration: Dictionary Specification Version 2.3
MAY	SP 800-146 – DRAFT Cloud Computing Synopsis and Recommendations
	SP 800-90A – DRAFT Recommendation for Random Number Generation Using Deterministic Random Bit Generators
	SP 800-57 Part 1 – DRAFT Recommendation for Key Management: Part 1: General
APRIL	NIST IR 7696 – DRAFT Common Platform Enumeration: Name Matching Specification Version 2.3
	NIST IR 7695 – DRAFT Platform Enumeration: Naming Specification Version 2.3
	SP 800-76-2 – DRAFT Biometric Data Specification for Personal Identity Verification

Draft Publications January 2011 – July 2011 (2)

MARCH	FIPS 201-2 – DRAFT Personal Identity Verification (PIV) of Federal Employees and Contractors
FEBRUARY	FIPS 180-4 – DRAFT Secure Hash Standard (SHS)
	SP 800-131 C – DRAFT Transitions: Validating the Transition from FIPS 186-2 to FIPS 186-3
	SP 800-131 B – DRAFT Transitions: Validation of Transitioning Cryptographic Algorithm and Key Lengths
	NIST IR 7670 – DRAFT Proposed Open Specifications for an Enterprise Remediation Automation Framework
	NIST IR 7511 Rev.2 – DRAFT Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements
	NIST IR 7756 – DRAFT CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture
JANUARY	SP 800-145 – DRAFT A NIST Definition of Cloud Computing
	SP 800-144 – DRAFT Guidelines on Security and Privacy in Public Cloud Computing

Final Special Publications

SP 800-147	Apr. 2011	Basic Input/Output System (BIOS) Protection Guidelines
SP 800-142	Oct. 2010	Practical Combinatorial Testing Monitoring for Federal Information Systems and Organizations
SP 800-135	Dec. 2010	Recommendation for Existing Application-Specific Key Derivation Functions
SP 800-132	Dec. 2010	Recommendation for Password-Based Key Derivation Part 1: Storage Applications
SP 800-131A	Jan. 2011	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
SP 800-127	Sept. 2010	Guide to Securing WiMAX Wireless Communications
SP 800-126 v1	Feb. 2011	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1
SP 800-125	Jan. 2011	Guide to Security for Full Virtualization Technologies
SP 800-119	Dec. 2010	Guidelines for the Secure Deployment of IPv6
SP 800-117	July 2010	Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0

Final Special Publications

SP 800-85 A-2	July 2010	PIV Card Application and Middleware Interface Test Guidelines (SP800-73-3 Compliance)
SP 800-82	Jun. 2011	Guide to Industrial Control Systems (ICS) Security
SP 800-78 -3	Dec. 2010	Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)
SP 800-70 v2	Feb. 2011	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
SP 800-57 Pt 1	May 6, 2011	DRAFT Recommendation for Key Management: Part 1: General
SP 800-53 A v1	Jun. 2010	Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans
SP 800-51 v1	Feb. 2011	Guide to Using Vulnerability Naming Schemes
SP 800-39	Mar. 2011	Managing Information Security Risk: Organization, Mission, and Information System View
SP 800-38 A	Oct. 2010	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode

Final NIST Interagency Reports June 2010-Present

NIST IR 7773	Nov 2010	An Application of Combinatorial Methods to Conformance Testing for Document Object Model Events
NIST IR 7771	Feb 2011	Conformance Test Architecture for Biometric Data Interchange Formats - Version Beta 2.0
NIST IR 7764	Feb 2011	Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition
NIST IR 7751	May 2011	2010 Computer Security Division Annual Report
NIST IR 7692	April 2011	Specification for the Open Checklist Interactive Language (OCIL) Ver 2.0
NIST IR 7676	June 2010	Maintaining and Using Key History on Personal Identity Verification (PIV) Cards
NIST IR 7628	Aug 2010	Guidelines for Smart Grid Cyber Security
NIST IR 7601	Aug 2010	Framework for Emergency Response Officials (ERO)
NIST IR 7559	Jun 2010	Forensics Web Services (FWS)
NIST IR 7502	Dec 2010	The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities
NIST IR 7497	Sept 2010	Security Architecture Design Process for Health Information Exchanges (HIEs)
NIST IR 7298 v1	Feb 2011	Glossary of Key Information Security Terms

Status of Key Programs and Initiatives

- FISMA Implementation Project
  - Objective:
    - Develop and update security standards and guidelines to help agencies create and maintain robust information security programs and to effectively manage risk.
  - Upcoming Activities:
    - SP 800-30 Revision 1 (Risk Assessment) – Public draft anticipated Summer 2011
    - SP 800-53 Revision 4 (Security Controls) – Public draft anticipated Summer 2011
    - SP 800-18 Revision 2 (Security Plan) – Public draft anticipated Fall 2011

Status of Key Programs and Initiatives

- SHA-3 Competition
  - Objective:
    - Develop a new cryptographic hash algorithm via a public competition to augment FIPS 180-4, Secure Hash Standard
  - Upcoming Activities:
    - Continue security and performance evaluations of the finalists with the cryptographic community
    - Hold the Final SHA-3 Candidate Conference in DC (3/12)
    - Select the winner and publish the third-round report (est. 8/12)
    - Send the revised standard (with the SHA-3 algorithm included) to the Secretary of Commerce for signature (est. 2/13)

Status of Key Programs and Initiatives

- Security Automation
  - Objective:
    - Security automation harmonizes the vast amount of IT product data into coherent, comparable information streams that inform timely and active management of diverse IT systems. Through the creation of flexible, open standards and international recognition, security automation will result in IT infrastructure interoperability, broad acceptance and adoption, and create opportunities for innovation.
  - Upcoming Activities:
    - 7th Annual Security Automation conference
      - October 31 – November 2, 2011
      - Hyatt Regency Crystal City
      - Tracks include Continuous Monitoring, Software Assurance, IT Security Threats, Network Security Automation, Management and Compliance, and more…

Status of Key Programs and Initiatives

- Cloud Computing
  - Objective:
    - Accelerate federal government adoption of cloud computing.
      - Build a USG Cloud Computing Technology Roadmap which focuses on the highest priority USG cloud computing security, interoperability and portability requirements.
      - Lead efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.
  - Upcoming Activities:
    - Nov. 2011. Fourth NIST Cloud Computing Forum.
    - Target FY 2011. 1st draft NIST USG Cloud Computing Technology Roadmap.
    - Ongoing. Interim work and products in architecture, security, standards, and use cases. See: http://www.nist.gov/itl/cloud/

Status of Key Programs and Initiatives

- NICE
  - The National Initiative for Cybersecurity Education (NICE) will be represented by four Components:
    - Component 1: National Cybersecurity Awareness Lead: Department of Homeland Security (DHS)
    - Component 2: Formal Cybersecurity Education Co-Lead Department of Education (DoED) and National Science Foundation (NSF)
    - Component 3: Cybersecurity Workforce Structure Lead: DHS
    - Component 4: Cybersecurity Workforce Training and Professional Development Tri-Leads: Department of Defense (DoD), Office of the Director of National Intelligence (ODNI), Department of Homeland Security (DHS).

- Upcoming Activities:
  - Shaping the Future of Cybersecurity Education Workshop – Engaging Americans in Securing Cyberspace
  - September 20-22, 2011, NIST Campus, Gaithersburg, Maryland
  - See: http://csrc.nist.gov/nice/

Status of Key Programs and Initiatives

- NSTIC
  - Governance Workshop:
    - June 9-10, 2011, Grand Hyatt Washington, Washington DC.
    - See http://www.nist.gov/nstic/workshops-home.html
    - 262 registered attendees
    - To discuss the Notice of Inquiry http://www.nist.gov/nstic/nstic-frn-noi.pdf
    - Webcasting of the workshop (except for breakout sessions)
  - Privacy Workshop:
    - June 27-28, 2011, MIT, Boston, MA
    - See http://www.nist.gov/itl/nstic-privacy-workshop.cfm
    - Over 130 registered attendees
  - Upcoming Activities:
    - September 2011 (possibly week of September 29) – Technology Workshop (3rd workshop)
    - Location: TBD, possibly in the Bay area

Upcoming Events

July 19-21, 2011	– ITL and Computer Security Division will host a Booth at the 2011 FOSE Conference & Exposition, Walter E. Washington Convention Center, Washington, DC.
August 11, 2011	– Federal Computer Security Program Managers' Forum NIST Meeting
Sept. 20-22, 2011	– Biometric Consortium Conference 2011, Tampa Convention Center, Tampa, FL
Sept. 26-27, 2011	– Non-Invasive Attack Testing Workshop, Todai-ji Cultural Center, Nara, Japan
Oct. 31-Nov.2, 2011	– 7th Annual IT Security Automation Conference, Hyatt Regency Arlington, VA

Past Events - 2011

March 15-17, 2011	– Federal Computer Security Program Managers' Forum NIST Meeting
March 21, 2011	– Continuous Monitoring Workshop
March 22-25, 2011	– Security Automation Developer Days – Spring 2011
April 6-7, 2011	– IDTrust 2011
April 12, 2011	– Federal Computer Security Program Managers‘ Forum NIST Meeting
April 18-19, 2011	– Draft FIPS 201-2 Workshop
May 10-11, 2011	– Safeguarding Health Information: Building Assurance through HIPAA Security
June 14-15, 2011	– Annual Offsite for Federal Computer Security Program Managers’ Forum

QUESTIONS or COMMENTS?