Building Common Understanding in Security Control Implementation and Assessment

NIST FISMA Implementation Project Phase II

5th Annual Security Automation Conference

October 28, 2009

Arnold Johnson

Computer Security Division
Information Technology Laboratory

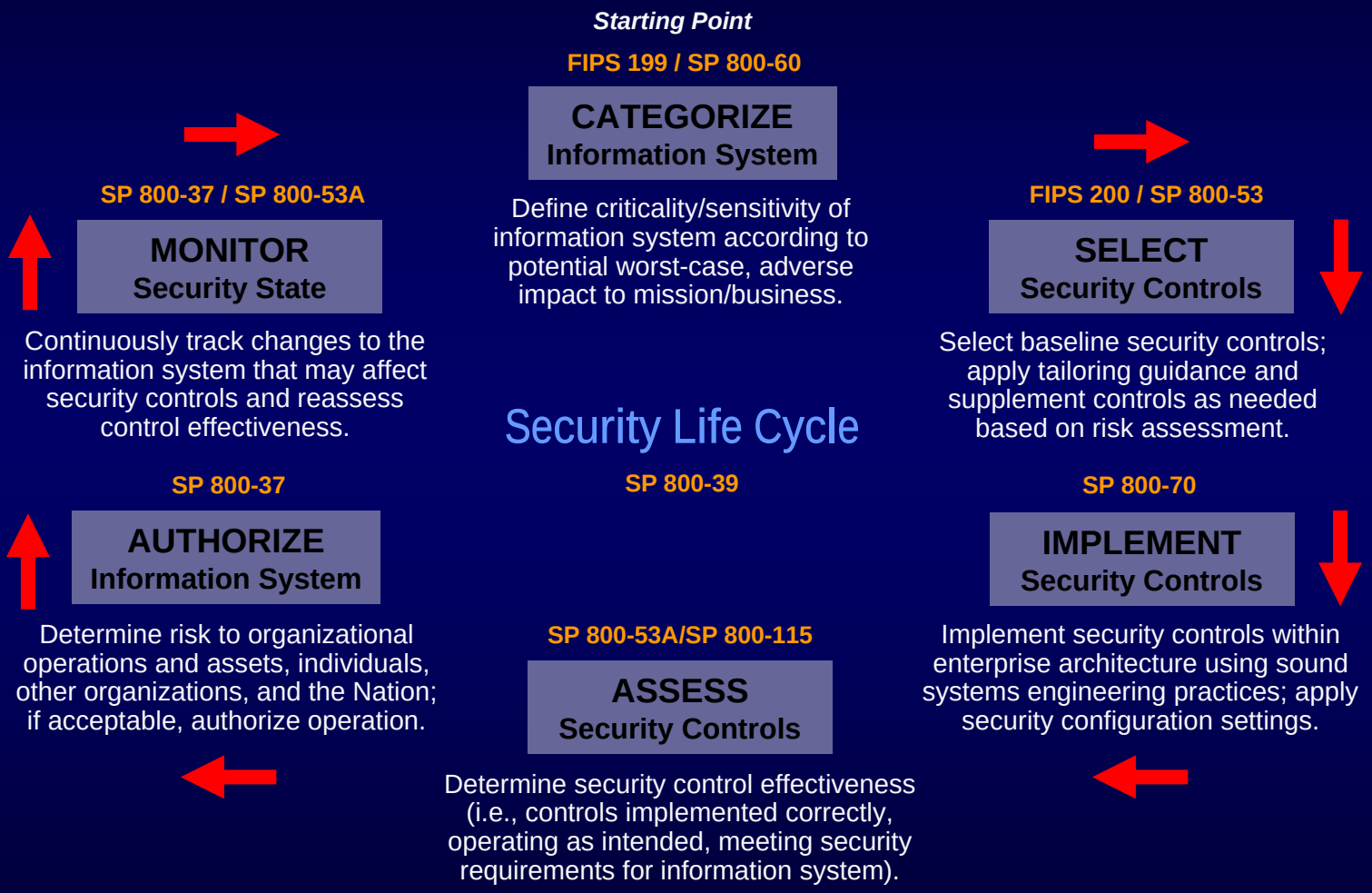
Agenda

- FISMA Project Phase I
  - *What we have accomplished to date…*
  - Publications…
- FISMA Project Phase II
  - *Where we are headed …*
  - Initiatives for common understanding…

FISMA Implementation Project

- Focus is on developing standards, guidelines and processes for supporting development, implementation and assessment of information systems consistent with FISMA 2002.
- Defined in terms of Risk Management Framework – Security Life Cycle.

Risk Management Framework



FISMA Project Phase I Publications

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment) *
- NIST Special Publication 800-39 (Risk Management) *
- NIST Special Publication 800-37 (Certification & Accreditation) *
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)*
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

* Publications currently under revision.

Common Understanding Important

- Risk Management Framework (RMF) expressed in a core set of NIST standards and guidelines.
- A large complement of supplemental NIST standards and guidelines are available for supporting implementation and assessment of security controls.
- Common protocols, programs, practices, tools, tips, techniques, etc. are either available or being identified/defined/developed.

Security Control Implementation/Assessment

- Security controls (management, operational and technical) include:
  - Policies, Plans and Procedures;
  - Processes and Activities;
  - Mechanisms (hardware, software, firmware); and
  - Products and Services.
- Adequate information system security depends on security controls functioning as planned when configured, integrated, and used in the end-user operational environment.
- Emphasis on assessing security controls in the information system operational environment.

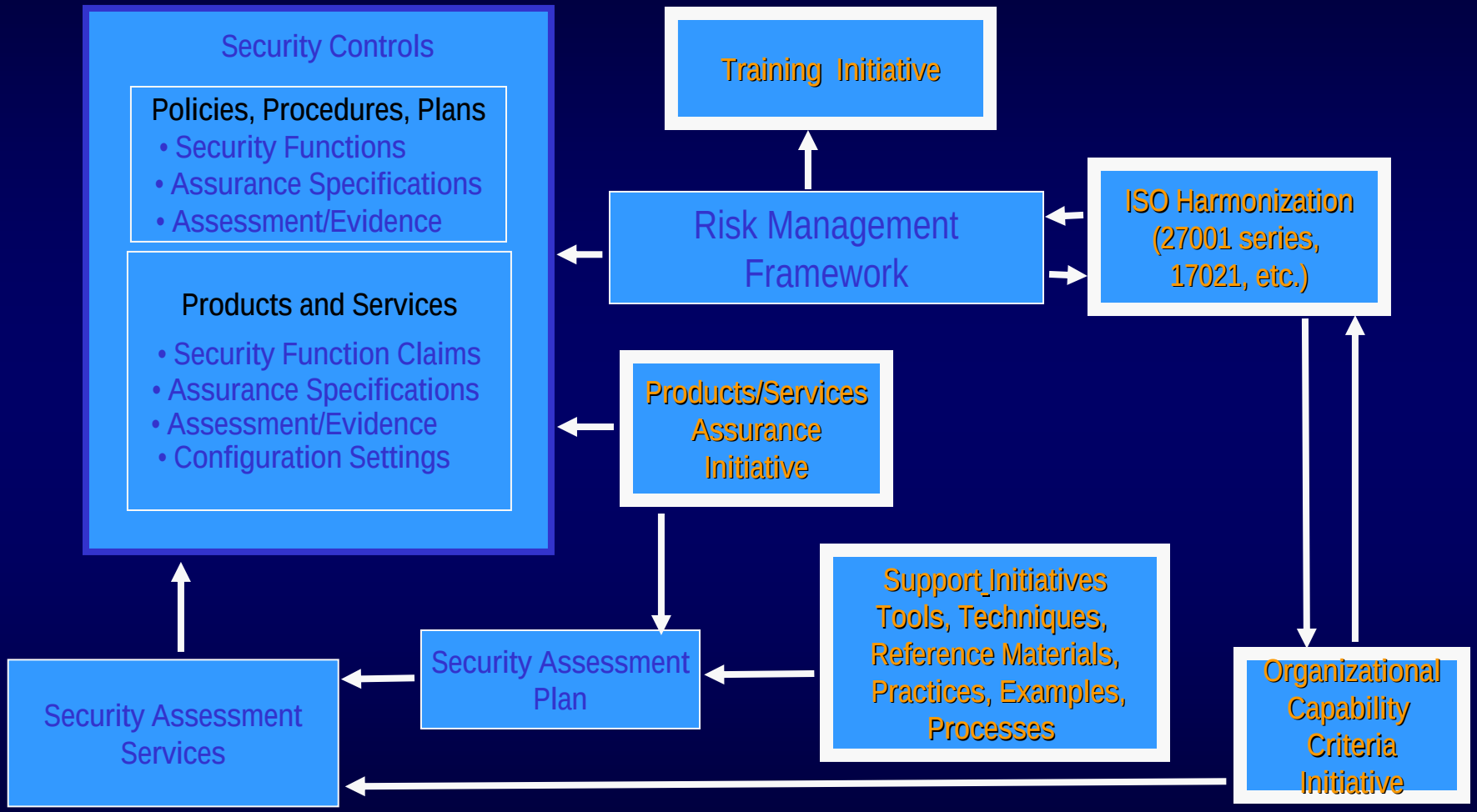
FISMA Project Phase II Objectives

- More consistent, comparable, repeatable and cost-effective security control implementation and assessment in federal information systems.
- More complete, reliable, timely, and trustworthy information for authorizing officials -- facilitating more informed security authorization decisions.
- Harmonize FISMA-related security standards and guidelines with international standards and guidelines (ISO).
- Draw upon, adapt and use available assessment-related standards, guidelines, programs, automated tools, practices and assessment sources.

Phase II Initiatives

- Training Initiative
- Products and Services Assurance Initiative
- Support Tools, Techniques, Reference Materials, Practices and Processes Initiative
- Organizational Assessment Capability Criteria Initiative
- ISO Harmonization Initiative

Phase II Initiatives



Training Initiatives

- Information security training initiative underway to provide increased support to organizations using FISMA-related security standards, guidelines, programs and services.
- Training initiative includes three components—
  - Formal Curriculum and Training Courses
  - Frequently Asked Questions
  - Quickstart Guides

Training Courses

- RMF Foundation Course
  - 1 day overview
  - Course to be held Nov 2009
  - Next course Feb/Mar 2010
- RMF Course
  - 3 day detailed
  - Course date TBD
- Web based Training Course
  - Internal review Oct/Nov 2009
  - Public release Feb 2010

Frequently Asked Questions (FAQs)

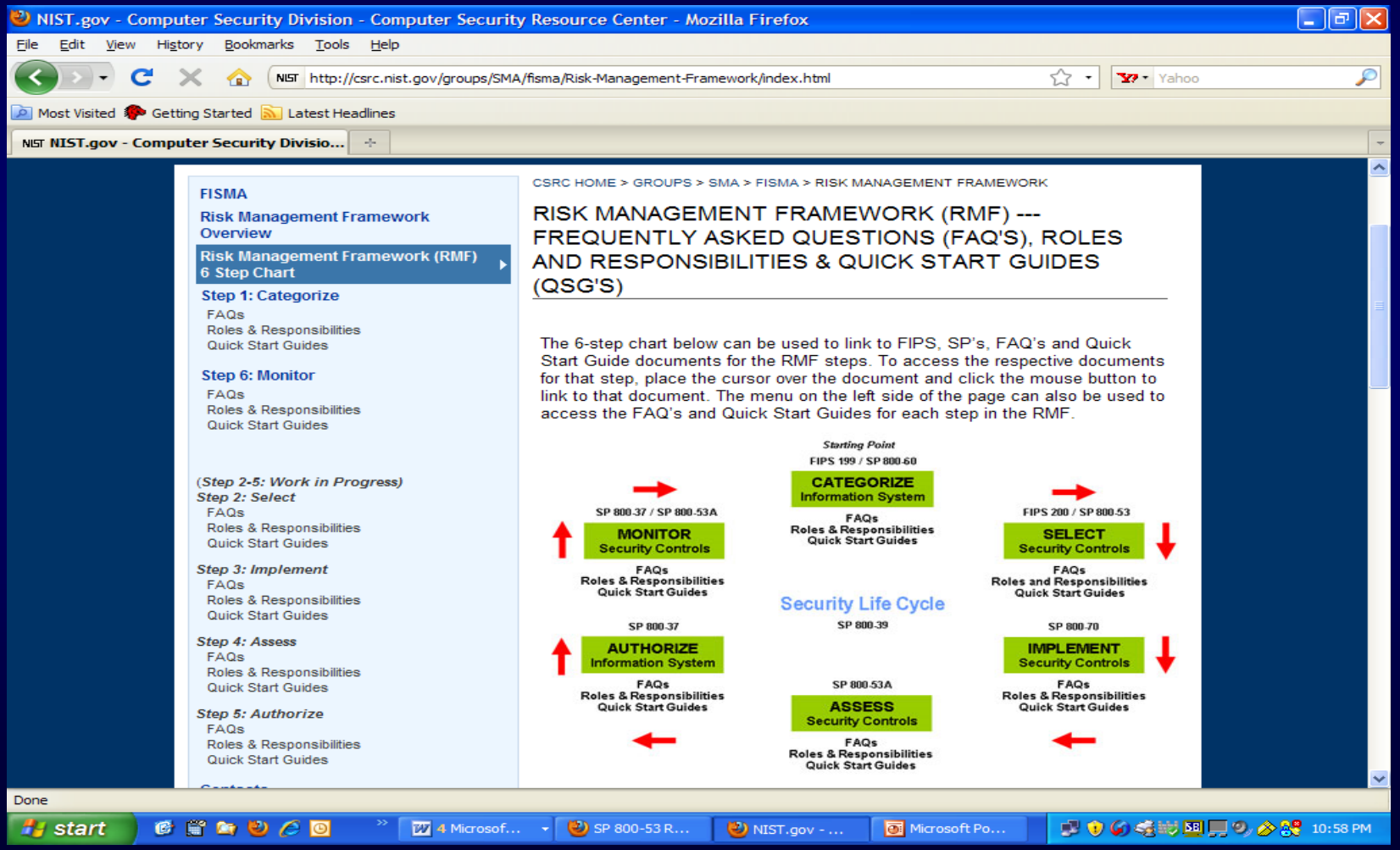
- Develop a set of FAQs for each step of the Risk Management Framework (RMF)
- Categorize step
  - Draft Posted to **csrc.nist.gov/sec-cert**
- Monitor step
  - Draft Posted to **csrc.nist.gov/sec-cert**
- Other steps under development

Quick Start Guides

- Each Step of the RMF
  - Categorize posted on **csrc.nist.gov/sec-cert**
  - Monitor posted on **csrc.nist.gov/sec-cert**
- Provide a general understanding
- Provided from management, systems and organization perspectives

Risk Management Framework

csrc.nist.gov/sec-cert



Products and Services Assurance Initiative

- Security assurance case built from:
  - Suppliers (products/services) [1st party] (i.e., developmental environment).
  - Independent Evaluation [3rd party] (i.e., laboratory environment).
  - Customers [2nd party] (i.e., operational environment).
- Products and services tested
  - Development (generically configured and functional)
  - Laboratory (independently configured and functional).
  - Operational environment (specifically configured and integrated).
- Leverage common set of techniques and tools to produce assurance evidence to support the supplier claims.
- Emphasis on providing assurance results that can be readily used, confirmed, repeated and enhanced in the end-user operational (system) environment.

Product & Service Assurance

Assessment Focus

- *Functionality*
  - Security-related functions or features of the system, for example, identification and authentication mechanisms, access control mechanisms, auditing mechanisms, and encryption mechanisms.
- *Quality*
  - In design, development, implementation, and operation
  - Degree to which the functionality is correct, always invoked, non bypassable, and resistant to tampering.
  - Achieved by employing well-defined security policy models, structured, disciplined, and rigorous hardware and secure software development techniques, and recommended system/security engineering principles and concepts when building an information system from information technology component products.
- *Evidence*
  - Grounds for confidence that the claims made about the functionality and quality of the product are being met.
  - Achieved through a variety of sources including post-development evidence brought forward regarding the design and implementation of the information system and the results of independent assessments (e.g., analyses, testing, evaluation, inspections, and audits) of the system conducted by qualified assessors using a common set of techniques and tools.

Product & Service Supplier Assurance

- Security claims specified in terms of:
  - SP 800-53 functional requirements
  - SP 800-53 assurance requirements
- Evidence provided to support claims drawing on 800-53A assessment procedures and other assessment processes.

Product/Service Supplier Claims Statement

- Minimum criteria, structure, form, guidelines, etc. for statement defined.
- Description of security features.
- Identification of 800-53 security controls product/service supported.
- Description of how product or service meets identified security control functional requirements.

Product/Service Supplier Claims Statement

- Assurances in context of SP 800-53 assurance requirements identifying targeted information system impact level – e.g., low impact:
  - How insure no obvious errors.
  - How demonstrate feature operates as intended.
  - How insure flaws discovered and addressed in a timely manner.
- Tailoring options for adapting to organization operating environments (e.g., configuration settings).

Product/Service Supplier Claims Statement

- Potential evidence to support claims.
  - Internal assessments reports.
  - External assessments reports (e.g., third party).
  - Use of SCAP validated products.
  - Results from configuration checklist testing.
- How evidence can be used or tailored to support SP 800-53A and system specific assessment procedures and processes.

Supplier Claims Statement Uses

- Form of assurances that *supplier's* can readily provide with each product release.
- Base information for including in offers to *customers*.
- Base information *customers* can use for assessing product/service acceptance or for conducting supplemental assessments if needed.

Supplier Claims Statement Uses

- Base information that can be provided to *third party evaluators* (e.g., validation laboratories) for acquiring additional assurances.
- Base information for system security *assessment providers*.
- Information for *security plans* and *security assessment plans*.

Product & Services Assurance Guide's

- Supplier claim and evidence guide

  (projected draft August 2010)
- Consumer evaluation guide

  (projected draft October 2010)

Support Tools, Reference Material, Practices and Processes Initiative

(Identify Common Available Sources or Criteria)

Examples:

- National Checklist Program (NCP)
- Security Content Automation Protocol (SCAP)
- Cryptographic Module Validation Program (CMVP)
- SCAP Validated Tools
- SP 800-115 Technical Guide to IS Testing & Assessment
- Personal Identity Verification Program (NPIVP)
- SP 800-53 Rev 3 Reference Database Application

Tools/References

SP 800-53 Rev 3 Reference Database Application

- Browse
  - Security controls, control enhancements, and supplemental guidance,
  - Summarize by control class, control family and control impact baseline.
- Search security control catalog using user-specified keywords.
- Export security control-related information to other data formats (e.g., .dbf, .xls, .htm, .xml, .csv) that can be used in various tools and applications.
- Information *read only* and can be viewed or extracted, but cannot be updated or modified using this application.
- http://csrc.nist.gov/groups/SMA/fisma/support_tools.html

Organizational Assessment Capability Criteria Initiative

Capability criteria for providing information security services —

- Assessments of Information Systems *(Operational environments)*
  - *Security controls including assurances*
  - *Configuration settings*
  - *Assessments using 800-53A, SCAP and other assessment tools*
  - *Assessment evidence*

- Assessments of Information Technology Products & Services *(Laboratory environments)*
  - *Security functionality (features)*
  - *Security assurance*
  - *Configuration settings*
  - *Assessment evidence*

ISO Harmonization Initiatives

- ISO 27000 (Information Security) Harmonization
  - Study relationship between the FISMA/NIST-based Risk Management Framework (RMF) and ISO 27001 Information Security Management System.
  - Develop mapping (Cross-walk) of NIST standards and guidelines specifications supporting the RMF to ISO 27001, Annex A [SP 800-53 Rev 3 Appendix H].
  - Develop a document that discusses commonalities and differences among the standards.
  - Develop guidance for organizations that are planning to become ISO 27001 compliant and that also wish to comply with NIST's RMF and related NIST standards and guidelines. The guidance would suggest how the organizations could meet the ISO 27001 requirements using the NIST RMF and related NIST standards and guidelines.
  - Explore options for recognition of assessment results between ISO 27001 and RMF, and for minimizing duplication of effort and cost for determining compliance.
- ISO 9000, 17020, 17021 and 17025 (Quality Systems, Inspection, Management System Audit/Certification, Testing Laboratories)

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov