NIST Risk Management Framework Overview

NIST, FISMA, and RMF Overview

June 9, 2014

Kelley Dempsey

NIST IT Laboratory

Computer Security Division

NIST

- National Institute of Standards and Technology
- Founded in 1901 as the National Bureau of Standards
- NIST is a NON-regulatory federal organization within the Department of Commerce
- NIST's Mission - 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. (see www.nist.gov)
- Information Technology Lab/Computer Security Division

NIST/ITL/CSD Types of Publications

- Federal Information Processing Standards (FIPS)
  - Signed/approved by the Secretary of Commerce
  - FISMA made FIPS mandatory for federal organizations
- Special Publications (SPs)
  - Providing guidance to federal organizations on information technology security since 1990
  - Are not mandatory for use (but see slide 7)
- NIST Interagency Reports (NISTIRs)
  - Describe research of a technical nature to a specialized audience

See them all at http://csrc.nist.gov

NIST/ITL/CSD Public Comment Process

- All publications produced by CSD go through the public comment process
- Your voice will be heard!!
- Receive notifications of newly posted drafts (and more) by subscribing at http://csrc.nist.gov/publications/subscribe.html
- There may be one or more drafts of a given publication
- Drafts are published at http://csrc.nist.gov/publications/PubsDrafts.html
- Lengths of public comment periods vary

FISMA and NIST

- FISMA – Federal Information Security Management Act
  - Law enacted by Congress - part of the E-Gov Act of 2002
  - Applies to federal organizations and their contractors
  - Requires implementation of “information security protections commensurate with the risk and magnitude of the harm”
- NIST – National Institute of Standards and Technology
  - FISMA requires NIST to develop standards and guidelines to help federal organizations improve the security of federal information and information systems (and implement FISMA)
  - NIST publications – http://csrc.nist.gov/publications

Directives and NIST

- OMB – Office of Management and Budget
  - Directives in the form of Memos and Circulars (usually)
  - May mandate NIST guidance for use by federal organizations
- EOs and PDs – Executive Orders and Presidential Directives
  - Directives from the Executive Office of the President
  - May direct NIST to provide guidance or develop a standard
- HSPD – Homeland Security Presidential Directive
  - An Executive Order focused on ensuring homeland security with implementation usually managed by DHS
  - Example: HSPD-12 which calls for a common ID standard for federal employees and contractors

Joint Task Force Transformation Initiative

A Broad-Based Partnership —

- National Institute of Standards and Technology
- Department of Defense
- Intelligence Community
  - Office of the Director of National Intelligence
  - 16 U.S. Intelligence Agencies
- Committee on National Security Systems

Standards/Guidelines for FISMA & RM

- FIPS - Federal Information Processing Standards
  - FIPS 199 – Standards for Security Categorization
  - FIPS 200 – Minimum Security Requirements
- SPs – Special Publications
  - SP 800-18 – Guide for System Security Plan development
  - SP 800-30 – Guide for Conducting Risk Assessments
  - SP 800-34 – Guide for Contingency Plan development
  - SP 800-37 – Guide for Applying the Risk Management Framework
  - SP 800-39 – Managing Information Security Risk
  - SP 800-53/53A – Security controls catalog/assessment procedures
  - SP 800-60 – Mapping Information Types to Security Categories
  - SP 800-128 – Security-focused Configuration Management
  - SP 800-137 – Information Security Continuous Monitoring
  - Many others for operational and technical implementations

Risk can never be eliminated and so it must be *MANAGED*!!

Managing risk doesn't mean *fixing everything,* nor does it mean *not fixing anything…*

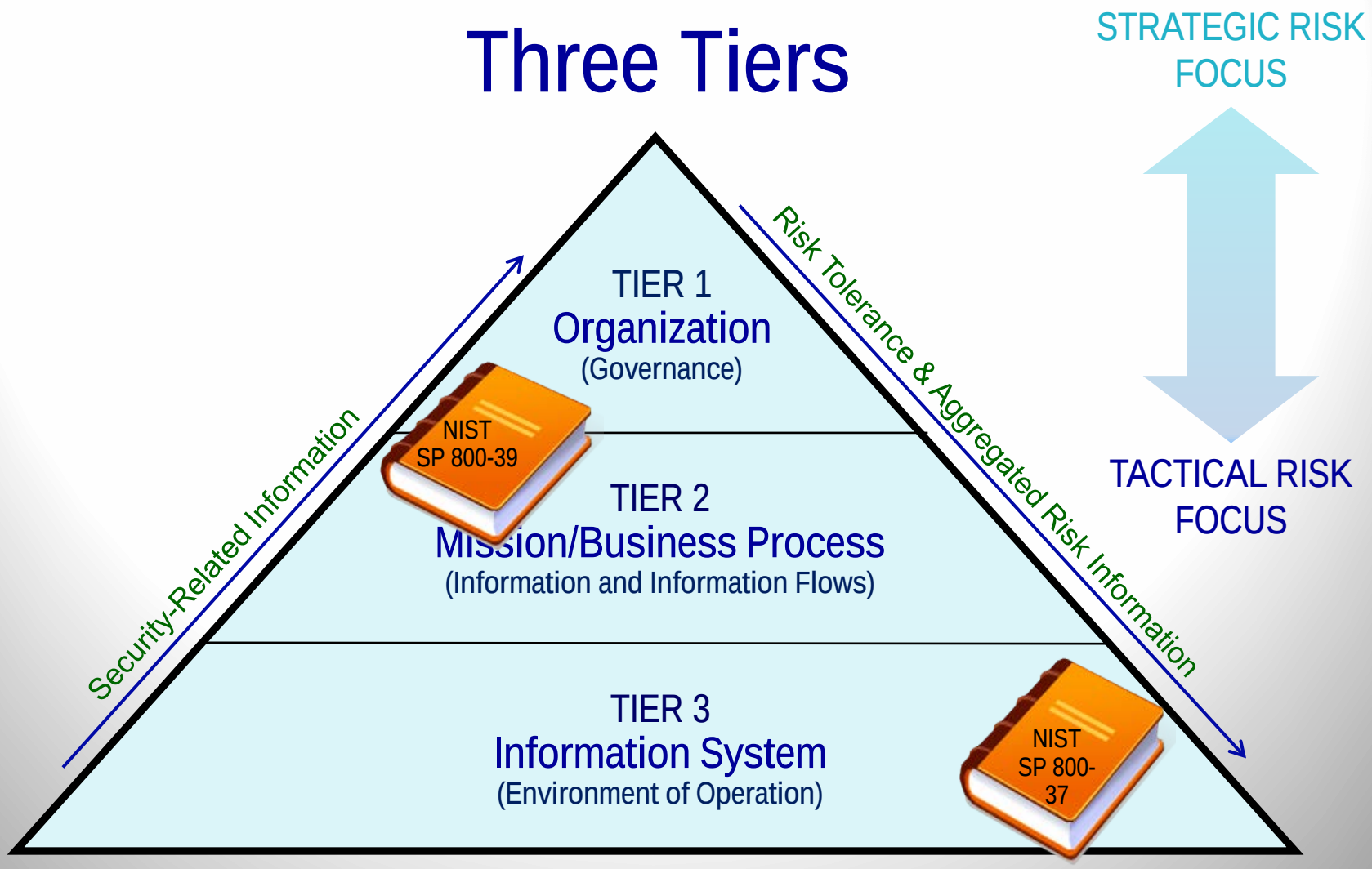
Graphic copied from: http://www.featurepics.com/online/Risk-1109124.aspx

NIST SP 800-39

Managing Information Security Risk: Organization, Mission, and Information System View

- Multi-tiered risk management approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus

Three Tiers


STRATEGIC RISK FOCUS
TACTICAL RISK FOCUS
Security-Related Information
Risk Tolerance & Aggregated Risk Information
TIER 1
Organization
(Governance)
NIST SP 800-39
TIER 2
Mission/Business Process
(Information and Information Flows)
TIER 3
Information System
(Environment of Operation)
NIST SP 800-37

Risk Management in 800-39

Seeks to broaden the narrow view that information security is only a technical matter or stovepipe independent of organizational risk by providing concepts that:

- Establish a relationship between **aggregated** risk from information systems and mission/business success
- Encourage senior leaders to recognize the **importance of managing information security risk** within the organization
- Foster a culture where risk from systems is automatically considered in the context of the EA and at all phases of the SDLC
- Help those with system level security responsibilities understand how system-level issues affect the organization/mission as a whole.

Components of Risk Management

- Framing Risk
- Assessing Risk
- Responding to Risk
- Monitoring Risk

NIST Special Publication 800-30

Revision 1

Guide for Conducting Risk Assessments

- Addresses the **Assessing Risk** component of Risk Management (from SP 800-39)
- Provides guidance on applying risk assessment concepts to:
  - All three tiers in the risk management hierarchy
  - Each step in the Risk Management Framework

Risk Assessment

- A three-step process:
  - Step 1: *Prepare for the assessment*
  - Step 2: *Conduct the assessment*
  - Step 3: *Maintain the assessment*
- In the context of four risk factors:
  - Threats (source and event)
  - Vulnerabilities
  - Likelihoods
  - Impacts

Assessment Approaches

- **Quantitative Assessments**

  Set of methods, principles, or rules for assessing risk based on the use of numbers—where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

- **Qualitative Assessments**

  Set of methods, principles, or rules for assessing risk based on non-numerical categories or levels (e.g., low, moderate, high, very high).

- **Semi-Quantitative Assessments**

  Set of methods, principles, or rules for assessing risk that uses bins (e.g., 0-15, 16-35, 35-70, 71-85, 86-100), scales (e.g., 1-10), or representative numbers whose values and meanings are not maintained in other contexts.

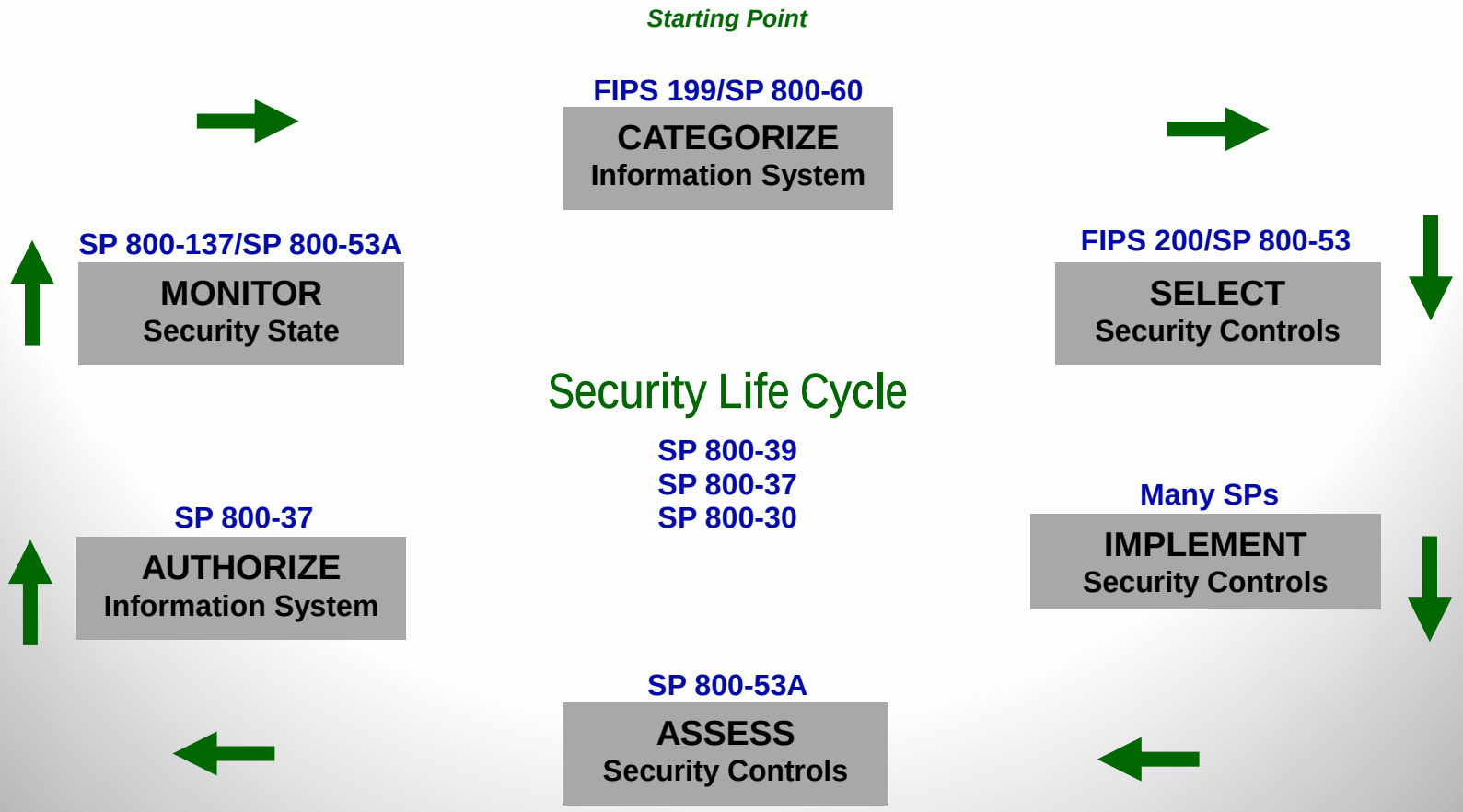
NIST SP 800-37

Revision 1

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- A holistic risk management process
- Integrates the RMF into the SDLC
- Provides processes (tasks) for each of the six steps in the Risk Management Framework at the system level

Risk Management Framework



RMF Roles and Responsibilities

- Risk Executive Function – RE(F)
- Authorizing Official - AO
- Senior Information Security Officer - SISO
- Common Control Provider
- Information System Owner
- Information Owner/Steward
- Information System Security Officer - ISSO
- Security Control Assessor

RMF Step 1
Categorize

FIPS 199

Standards for Security Categorization of Federal Information and Information Systems

- Supports Step 1 (Categorize) of the RMF
- In the context of ***security objectives*** from FISMA
  - Confidentiality – unauthorized disclosure
  - Integrity – unauthorized modification/destruction
  - Availability – disruption of access to/use of information
- Defines three ***impact levels:***
  - Low – loss would have a ***limited*** adverse impact
  - Moderate – loss would have a ***serious*** adverse impact
  - High – loss would have a ***catastrophic*** adverse impact

NIST Special Publication 800-60

Revision 1

Guide for Mapping Types of Information and Information Systems to Security Categories

- Supports Step 1 (Categorize) of the RMF
- Volume 1 provides guidance
- Volume 2 provides a catalog of information types and provisional categorizations (impact levels)
  - Low
  - Moderate
  - High
- The standard for impact levels is FIPS 199

NIST Special Publication 800-18

Revision 1

Guide for Developing Security Plans for Federal Information Systems

- Guidance for developing system security plans
  - Structure and content
  - Template
- Supports all RMF steps, but **begins during Step 1**
- Used to record information about the system
  - System boundary/diagram
  - Roles and responsibilities
  - Security control implementation details

RMF Step 2
Select

FIPS 200

Minimum Security Requirements for Federal Information and Information Systems

- Defines 17 security-related areas (families) that:
  - Represent a broad-based, balanced security program
  - Include management, operational, and technical types of controls (all are needed for defense in depth)
- Specifies implementation of minimum baseline of security controls, as defined in NIST SP 800-53
- Specifies that the baselines are to be appropriately tailored

NIST Special Publication 800-53

Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

- A catalog of security controls
- Supports Step 2 (Select) of the RMF
- Defines three security baselines (L, M, H)
- Initial version published in early 2005
- Revision 4 final was published 30 April 2013
  - Errata update published January 2014

Security Controls

- The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
- 800-53 defines three types of controls:
  - Common controls
  - System specific controls
  - Hybrid controls

800-53 Security Control Families

ID	FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PM	Program Management

SP 800-53 Baselines

- Baselines are defined in Appendix D, Table D-2
- Baselines are determined by:
  - Information and system categorization (L, M, H)
  - Organizational risk assessment and risk tolerance
  - System level risk assessment
- Baselines are a *starting point* and should be tailored to fit the mission and system environment
  - Parameters
  - Scoping/Compensating
  - Supplementing

Why are Some Controls NOT in Baselines?

- 800-53 provides a comprehensive set of security controls, BUT every system does not need to implement every control (risk *management*)
- Controls and enhancements not selected in a baseline are available as compensating or supplemental controls to strengthen the level of protection IAW:
  - Assessment of risk for the system and environment of operation; and
  - Organizational risk tolerance
  - Overlay requirements for specific communities

RMF Step 3 - Implement

- Follow Step 3 tasks in SP 800-37R1
- Many publications are available to provide implementation guidance on a wide range of controls and control types (csrc.nist.gov)
- Many automated tools are available to implement specific controls
- Plan for control implementation during the development phase of the SDLC – BAKE IT IN

NIST Special Publication 800-34

Revision 1

Contingency Planning Guide for Federal Information Systems

- Implementation (RMF Step 3) guidance for Contingency Planning (CP) controls from 800-53
- Business Impact Analysis
- Identifies three phases:
  - Activation/Notification Phase
  - Recovery Phase
  - Reconstitution Phase
- Roles and responsibilities
- Suggested appendices for contingency plans

NIST SP 800-61

Revision 2

Computer Security Incident Handling Guide

- Implementation (RMF Step 3) guidance for Incident Response (IR) controls from 800-53
- Identifies four phases:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-Incident Activity
- Coordination and information sharing
- Also see SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

NIST SP 800-128

Guide for Security-Focused Configuration Management of Information Systems

- Implementation guidance (RMF Step 3) for Configuration Management (CM) family controls from 800-53
- Four Phases
  1. Planning
  2. Identifying and Implementing Configurations
  3. Controlling Configuration Change
  4. SecCM Monitoring

RMF Step 4
Assess

NIST Special Publication 800-53A

Revision 1

Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

- Supports RMF Step 4 (Assess)
- Is a *companion* document to 800-53
- Is updated after 800-53 is updated
- Describes high level procedures for assessing security controls for effectiveness
- Three assessment methods
  - Interview
  - Examine
  - Test

RMF Step 5 – Authorize

- Follow Step 5 tasks in SP 800-37R1
- The Authorizing Official (AO) examines the output of the security controls assessment to determine whether or not the risk is acceptable
- The AO may consult with the RE(F), the CIO, the SISO, etc. since aggregate risk should also be considered for the authorization decision
- After the initial authorization, ongoing authorization is put in place using output from continuous monitoring

RMF Step 6
Monitor

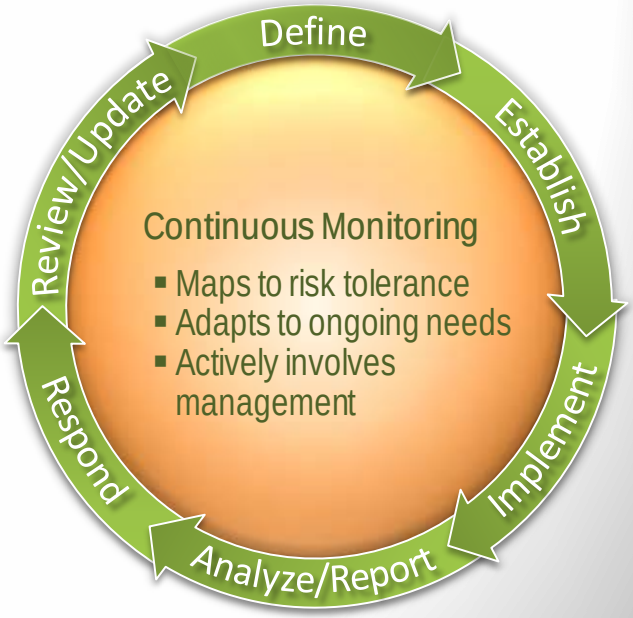
NIST Special Publication 800-137

Information Security Continuous Monitoring for Federal Information Systems and Organizations

- Supports RMF Step 6 (Monitor)
- Management level guidance on developing an information security continuous monitoring (ISCM) strategy and implementing an ISCM program
- ISCM is **maintaining ongoing awareness** of information security, vulnerabilities, and threats to **support organizational risk management decisions**

ISCM Process Steps

1. Define continous monitoring strategy
2. Establish continuous monitoring program
   a) Determine metrics
   b) Determine monitoring frequencies
   c) Develop ISCM architecture
3. Implement the monitoring program
4. Analyze security-related information (data) and report findings
5. Respond with mitigation actions OR reject/avoid, transfer, or accept risk
6. Review and update monitoring strategy and program



ISCM Automation: The Need for Caution

- Automated tools may lead to a false sense of security by **not** providing a complete picture of the overall security posture
- Automated tools must be installed and configured correctly and require ongoing maintenance for accuracy and integrity

HIPAA and NIST SP 800-66

- Health Insurance Portability and Accountability Act of 1996/Public Law 104-191
- Required HHS Secretary to adopt security standards – the HIPAA Security Rule
- NIST SP 800-66 Revision 1 (2008):
  - Summarizes HIPAA security standards
  - Explains structure, organization, and terms in the Security Rule
  - Discusses relevant NIST guidance but use of NIST guidance is NOT required for compliance

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 Researcher and Technical Support

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

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov