

Integrated Enterprise-wide Risk Management

Information Security Transformation for the Federal Government

ISPAB Meeting

July 30, 2009

Department of Defense
Office of the Director of National Intelligence
National Institute of Standards and Technology

The Threat Situation

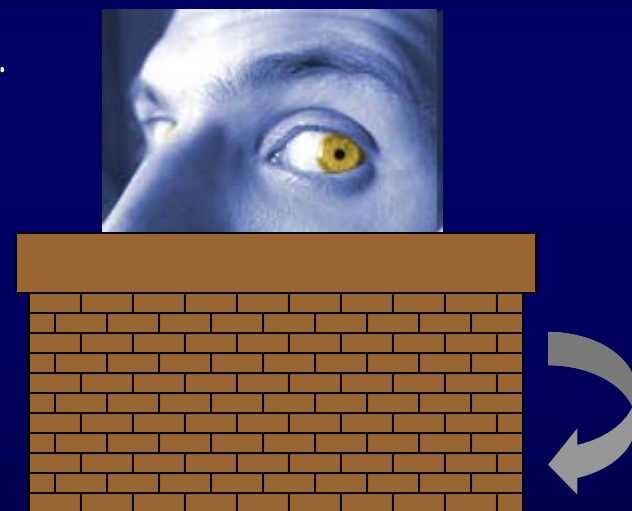
Continuing serious cyber attacks on federal information systems, large and small; targeting key federal operations and assets...

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with intentions of compromising federal information systems.
- Effective deployment of malicious software causing significant exfiltration of sensitive information (including intellectual property) and potential for disruption of critical information systems/services.

Unconventional Wisdom

NEW RULE: *Boundary protection is no longer sufficient against high-end threats capable of launching sophisticated cyber attacks...*

- Complexity of IT products and information systems.
- Insufficient penetration resistance (trustworthiness) in commercial IT products.
- Insufficient application of information system and security engineering practices.
- Undisciplined behavior and use of information technology and systems by individuals.



The Fundamentals

Fighting and winning a 21st century cyber war requires 21st century strategies, tactics, training, and technologies...

- Integration of information security into enterprise architectures and system life cycle processes.
- Common, shared information security standards for unified cyber command.
- Enterprise-wide, risk-based protection strategies.
- Flexible and agile selection / deployment of safeguards and countermeasures (maximum tactical advantage based on missions / environments of operation).
- More resilient, penetration-resistant information systems.
- Competent, capable cyber warriors.

Information Security Transformation

- Establishing a common approach to risk management.
 - Converging parallel efforts across the IC, DoD, and federal civil agencies.
 - Leveraging partnerships with CNSS and NIST.
- Benefiting the federal government and its partners.
 - Facilitating information sharing and reciprocity.
 - Achieving process efficiencies.
 - Improving communication and increasing decision advantage.
 - Promoting outreach to state and local governments and private sector (including contracting base).

Transformation Goals

- Establish a common approach to risk management.
- Define a common set of trust (impact) levels; adopt and apply those levels across the federal government.
- Adopt reciprocity as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.
- Define, document, and adopt common security controls.
- Adopt a common security lexicon—providing a common language and common understanding.

Transformation Goals

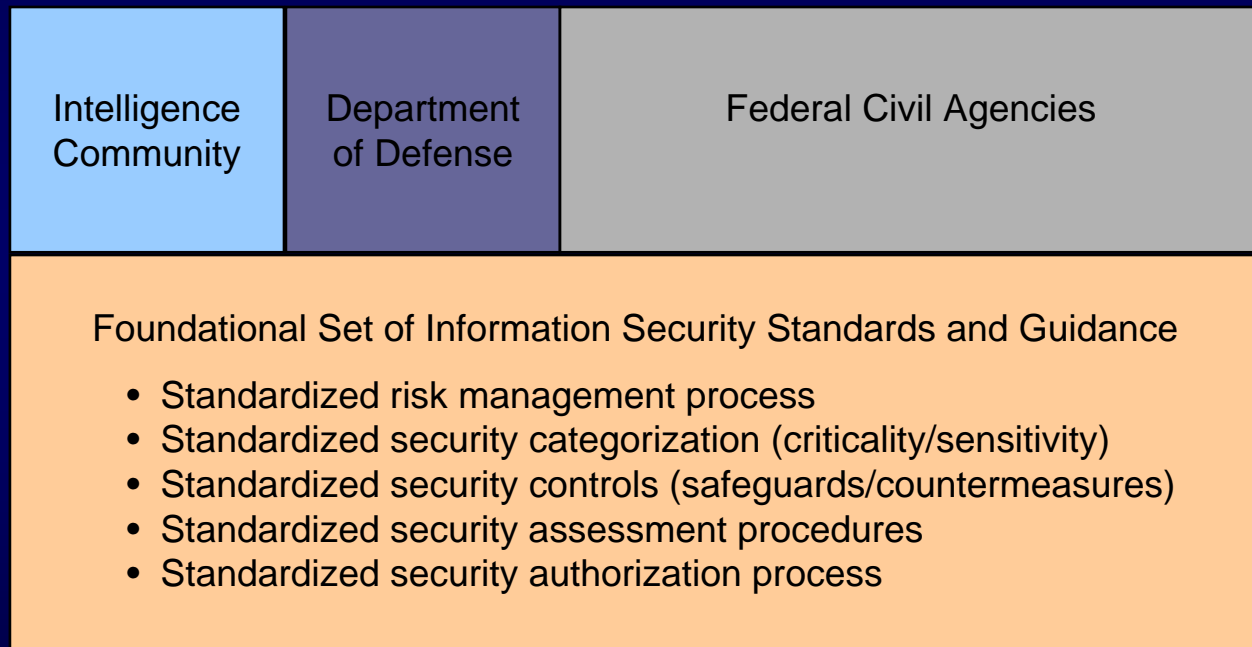
- Institute a senior risk executive function, which bases decisions on an “enterprise” view of risk considering all factors, including mission, IT, budget, and security.
- Incorporate information security into Enterprise Architectures and deliver security as common enterprise service across the federal government.
- Enable a common process that incorporates information security within the “life cycle” processes and eliminate security-specific processes.

A Unified Framework For Information Security

The Generalized Model

**Unique
Information
Security
Requirements**

The “Delta”



**Common
Information
Security
Requirements**

National security and non national security information systems

Strategic Initiatives

The Long-term View

- Build a unified information security framework for the federal government and support contractors.
- Integrate information security and privacy requirements into enterprise architectures.
- Employ systems and security engineering techniques to develop more secure (penetration-resistant) information systems.

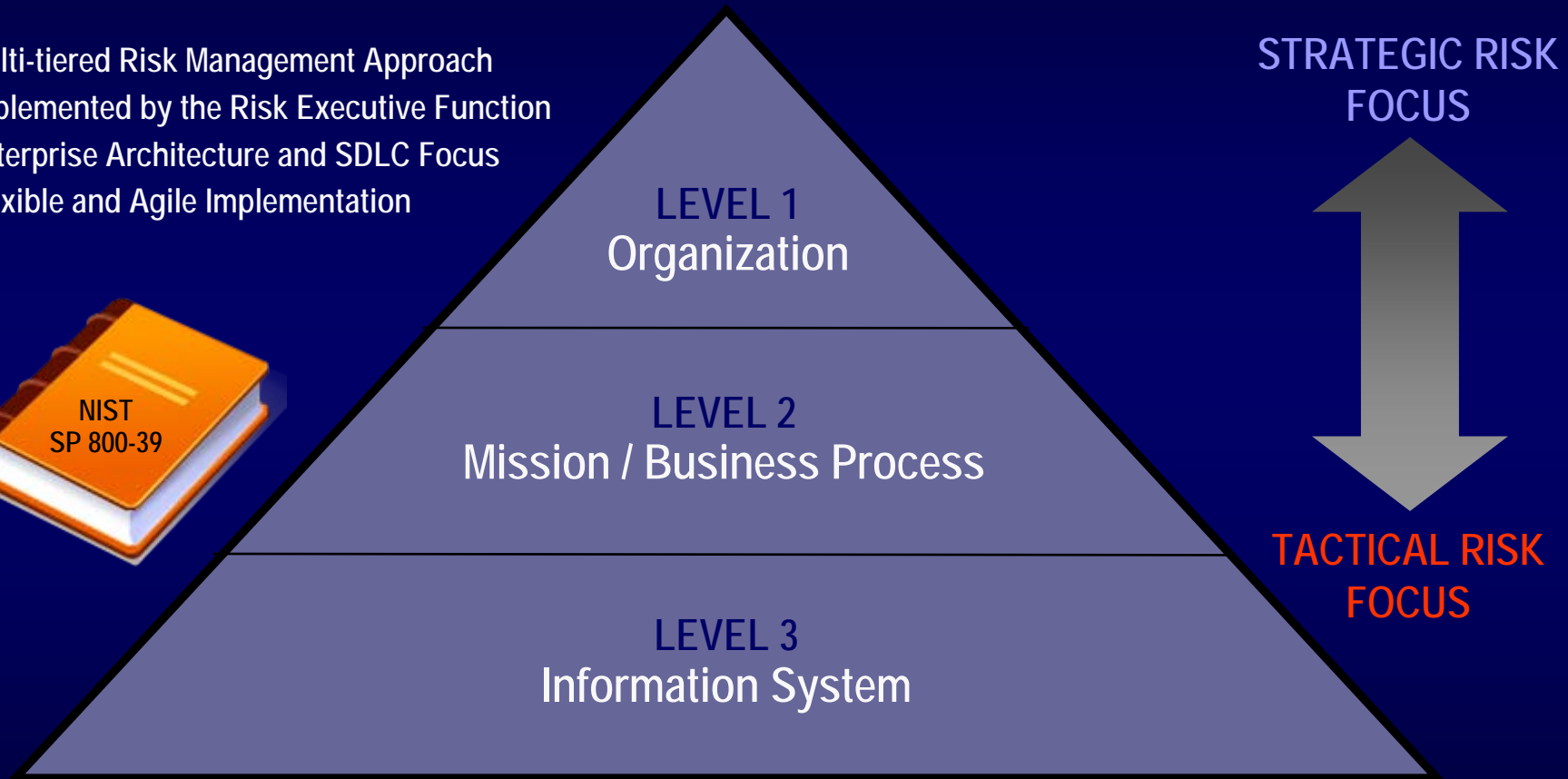
Tactical Initiatives

The Short-term View

- Update security controls catalog and baselines.
 - **Delivery vehicle: NIST Special Publication 800-53, Revision 3**
- Develop enterprise-wide risk management guidance.
 - **Delivery vehicle: NIST Special Publication 800-39**
- Restructure the current certification and accreditation process for information systems.
 - **Delivery vehicle: NIST Special Publication 800-37, Revision 1**
- Provide more targeted guidance on risk assessments.
 - **Delivery vehicle: NIST Special Publication 800-30, Revision 1**

Risk Management Hierarchy

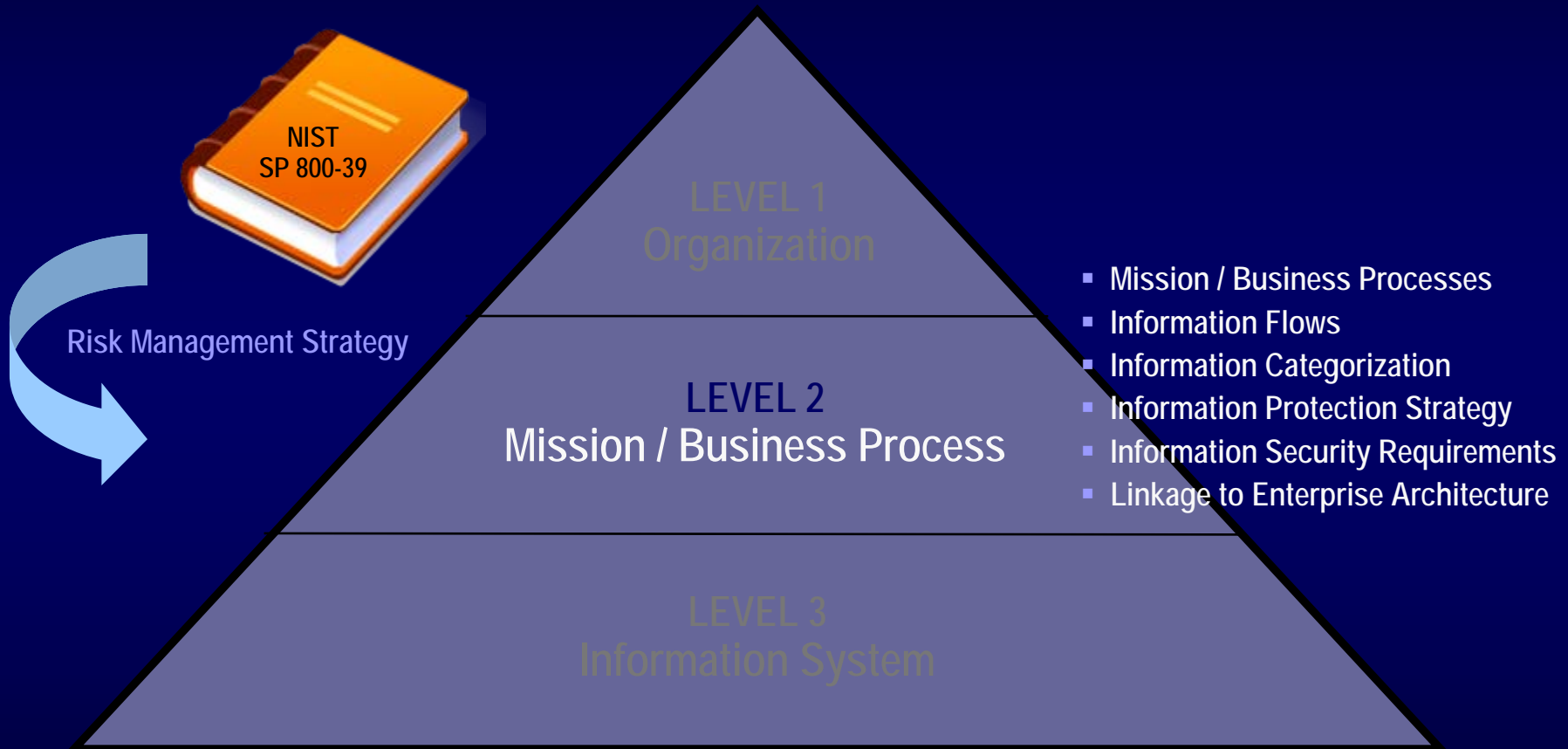
- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



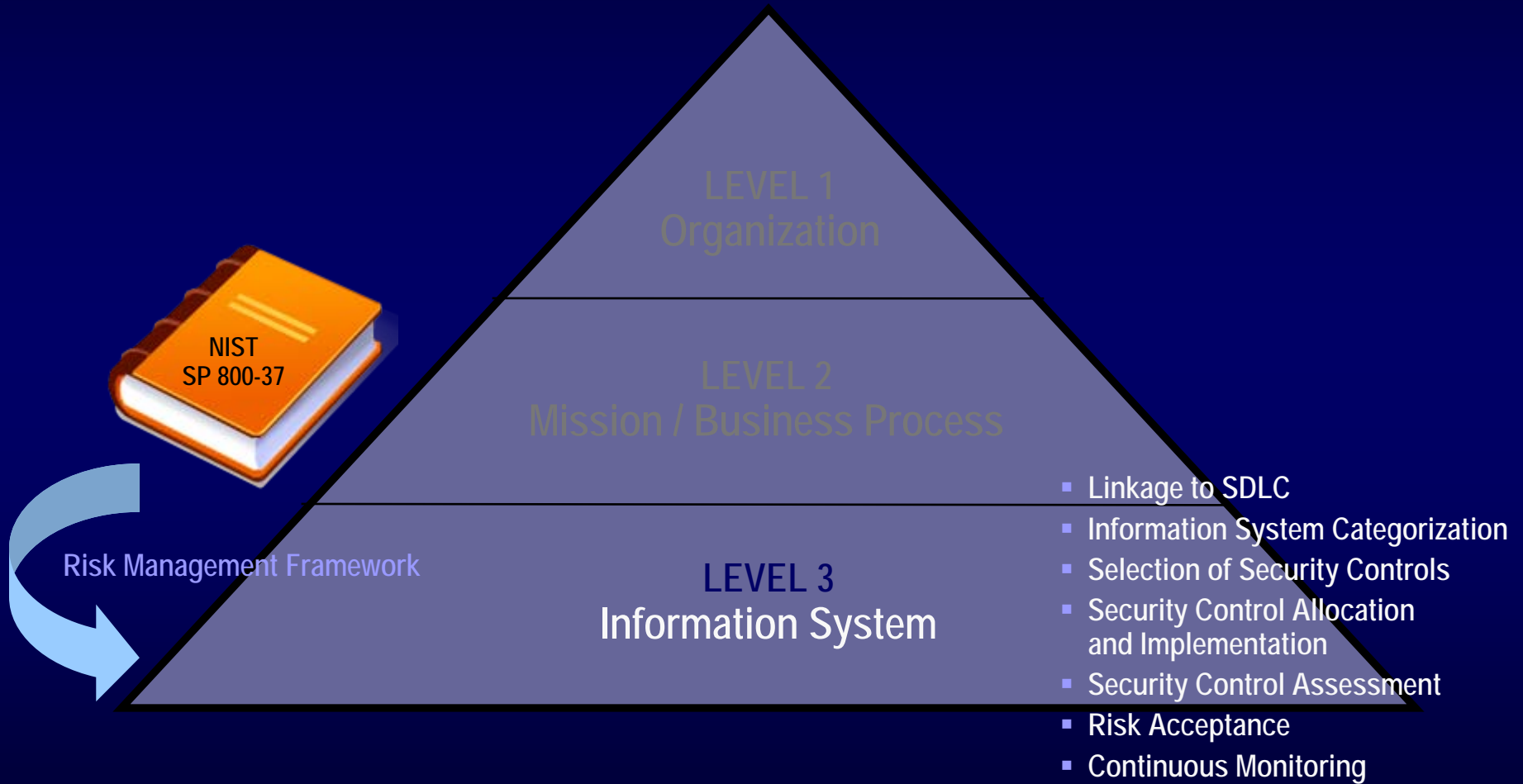
Risk Management Hierarchy



Risk Management Hierarchy



Risk Management Hierarchy

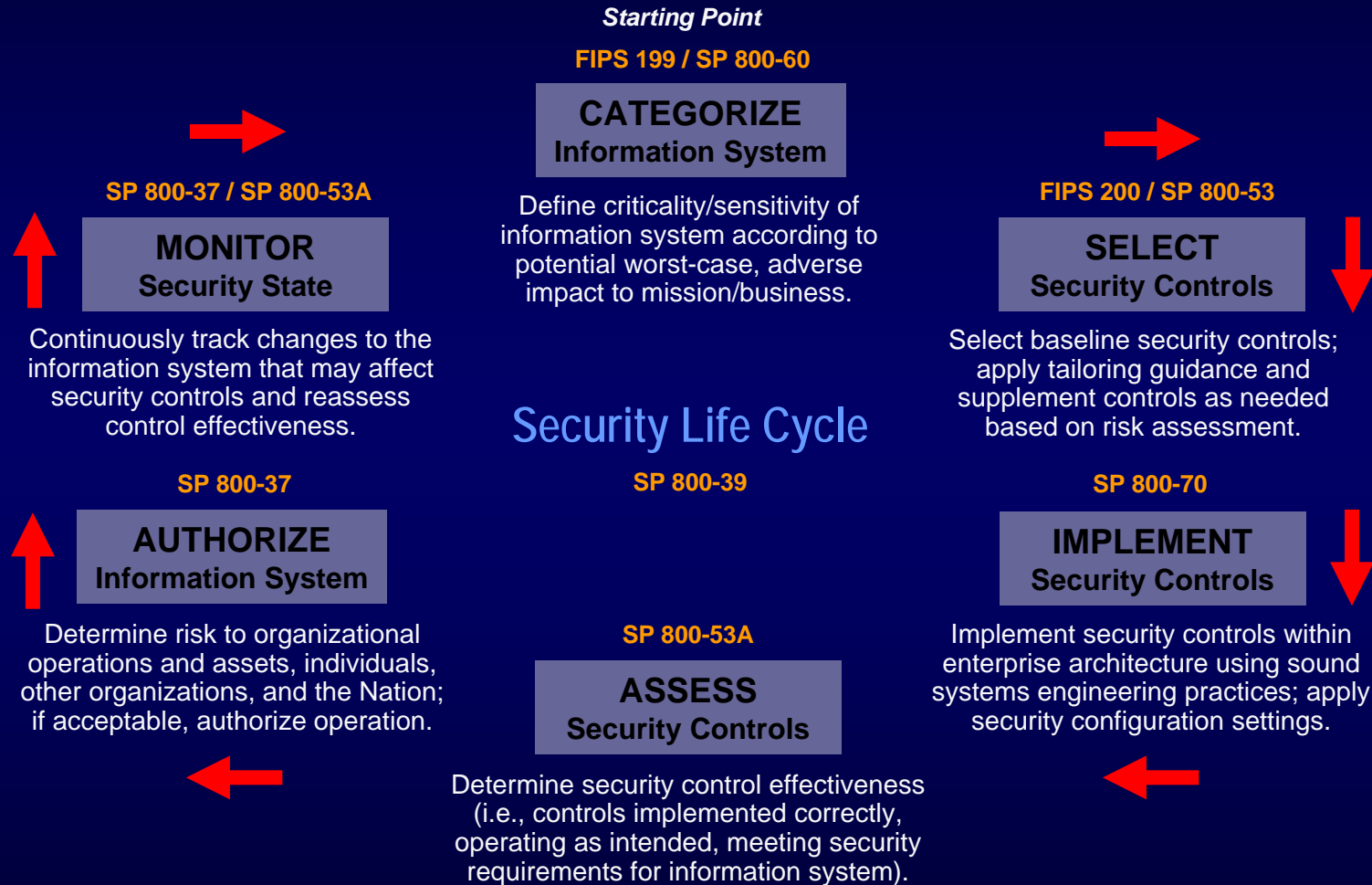


The Central Question

From Two Perspectives

- **Security Capability Perspective**
What security capability is needed to defend against a specific class of cyber threat, avoid adverse impacts, and achieve mission success? **(REQUIREMENTS DEFINITION)**
- **Threat Capability Perspective**
Given a certain level of security capability, what class of cyber threat can be addressed and is that capability sufficient to avoid adverse impacts and achieve mission success? **(GAP ANALYSIS)**

Risk Management Framework

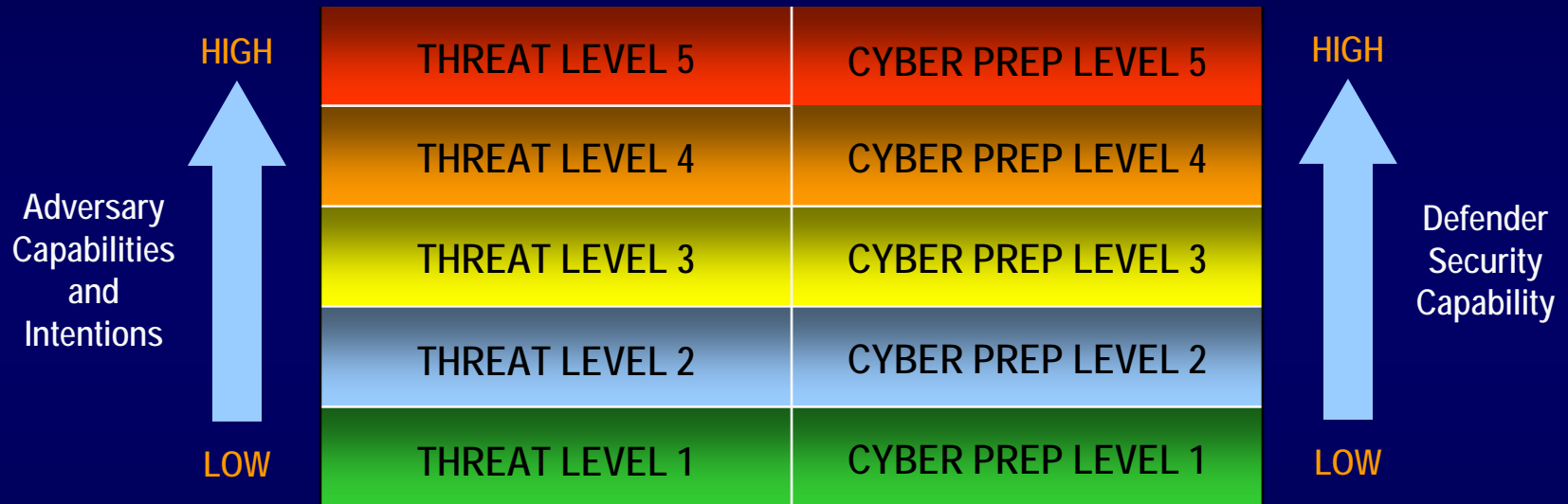


Security Control Selection

- STEP 1: Select Baseline Security Controls
(NECESSARY TO COUNTER THREATS)
- STEP 2: Tailor Baseline Security Controls
(NECESSARY TO COUNTER THREATS)
- STEP 3: Supplement Tailored Baseline
(SUFFICIENT TO COUNTER THREATS)



Cyber Preparedness



An increasingly sophisticated and motivated threat requires increasing preparedness...

Dual Protection Strategies

- **Boundary Protection**

Primary Consideration: *Penetration Resistance*

Adversary Location: *Outside the Defensive Perimeter*

Objective: *Repelling the Attack*

- **Agile Defense**

Primary Consideration: *Information System Resilience*

Adversary Location: *Inside the Defensive Perimeter*

Objective: *Operating while under Attack*

Agile Defense

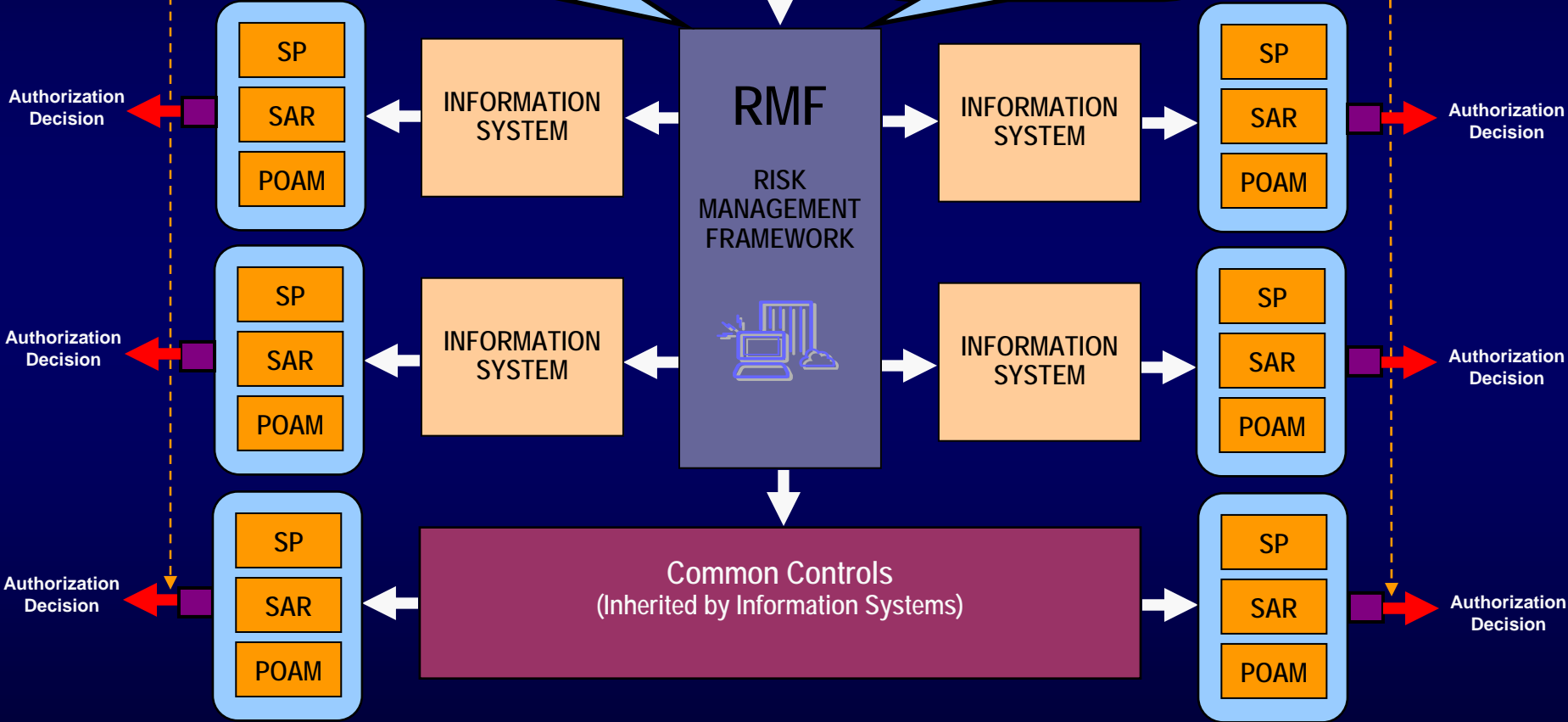
- Boundary protection is a necessary but not sufficient condition for *Agile Defense*
- Examples of *Agile Defense* measures:
 - Compartmentalization and segregation of critical assets
 - Targeted allocation of security controls
 - Virtualization and obfuscation techniques
 - Encryption of data at rest
 - Limiting of privileges
 - Routine reconstitution to known secure state

Bottom Line: Limit damage of hostile attack while operating in a (potentially) degraded mode...

RISK EXECUTIVE FUNCTION
Enterprise-wide Oversight, Monitoring, and Risk Management Strategy

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations



Authorization Decision

Authorization Decision

Authorization Decision

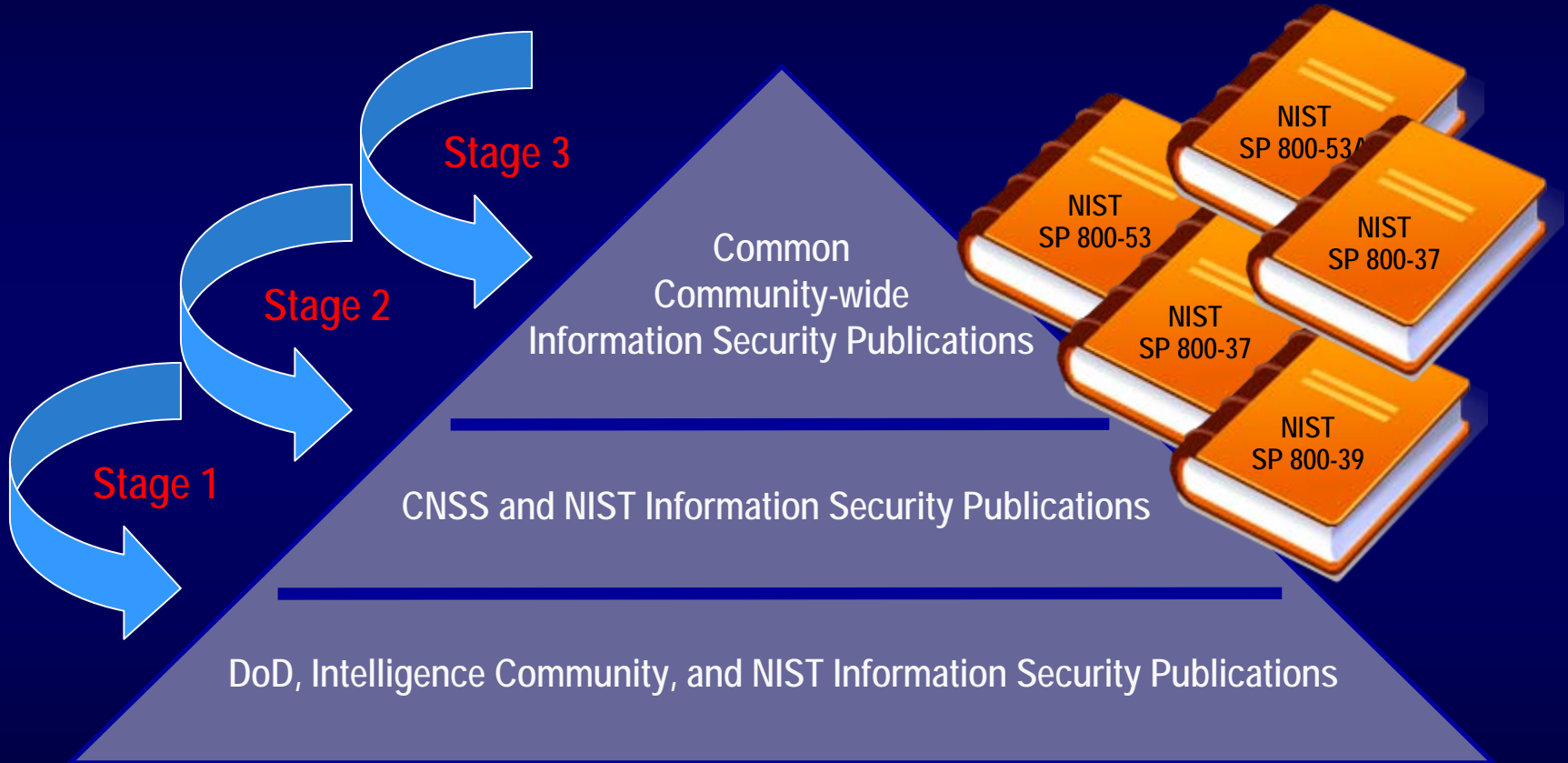
Authorization Decision

Authorization Decision

Authorization Decision



The Path to Convergence



Key Risk Management Publication

- NIST Special Publication 800-53, Revision 3
Recommended Security Controls for Federal Information Systems and Organizations

Projected: July 2009

- Updating all material from NIST Special Publication 800-53, Revision 2
- Incorporating security controls from Draft CNSS Instruction 1253
- Incorporating new security controls for advanced cyber threats
- Incorporating information security program-level controls
- Incorporating threat appendix for cyber preparedness
(Separately vetted and added to SP 800-53, Revision 3 when completed)



Key Risk Management Publication

- NIST Special Publication 800-37, Revision 1
Guide for Applying the Risk Management Framework to Federal Information Systems

Projected: October 2009

- Incorporating comments from Initial Public Draft
- Implementing guideline for Risk Management Framework
- Transforming previous certification and accreditation process
- Integrating Risk Management Framework into the SDLC
- Greater emphasis on ongoing monitoring of information system security state
- Ongoing security authorizations informed by risk executive function
- Greater accountability and assurances for common (inherited) controls
- Increased use of automated support tools



Key Risk Management Publication

- NIST Special Publication 800-39
*Integrated Enterprise-wide Risk Management
Organization, Mission, and Information Systems View*
Projected: December 2009
 - Incorporating public comments from NIST Special Publication 800-39, Second Public Draft
 - Incorporating three-tiered risk management approach: organization, mission/business process, and information system views
 - Incorporating cyber preparedness information
 - Providing ISO/IEC 27001 mapping to risk management publications



Key Risk Management Publication

- NIST Special Publication 800-53A, Revision 1
Guide for Assessing the Security Controls in Federal Information Systems and Organizations
Projected: January 2010
 - Updating all assessment procedures to ensure consistency with NIST Special Publication 800-53, Revision 3
 - Developing new assessment procedures for information security program management controls
 - Updating web-based assessment cases for inventory of assessment procedures



Key Risk Management Publication

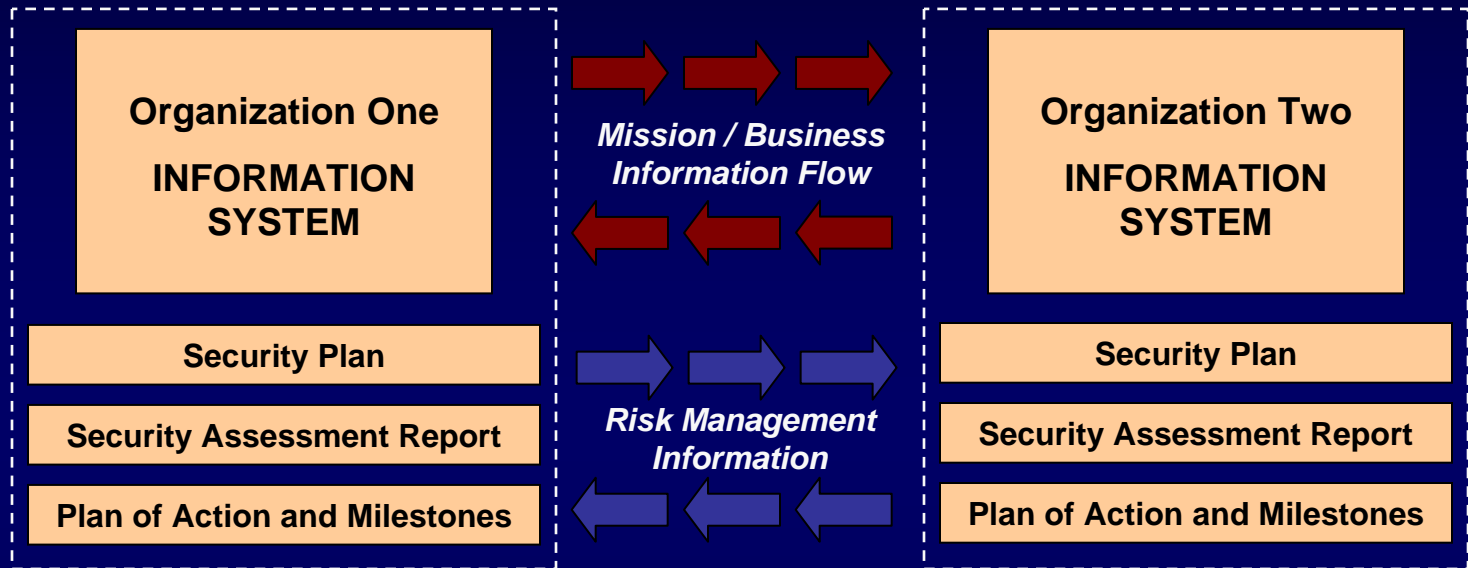
- NIST Special Publication 800-30, Revision 1 (Initial Public Draft)
Guide for Conducting Risk Assessments

Projected: January 2010

- Down scoping current publication from risk management focus to risk assessment focus
- Providing guidance for conducting risk assessments at each step in the Risk Management Framework
- Incorporating threat information for cyber preparedness



Trust and Reciprocity



Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

The objective is to achieve transparency of prospective partner's information security programs and processes...establishing trust relationships based on common, shared risk management principles.

Transformation... Getting There

Current State

- Lack of reciprocity in authorization and assessment results
- Resource intensive
- Redundant and duplicative activities
- Inconsistent policy and process implementation
- Lack of automation (for both workflow and testing tools)
- Lack of standardized documentation and artifacts to facilitate informed decisions
- Three-year "Paperwork Drill"

The Future

- Enabled reciprocity and information sharing
- Improve security postures (architecture and information)
- Streamline processes and improve end-product quality
- Uniform set of policies and practices
- Consistent implementation and use of automated tools
- More effective resource allocation; reduce costs
- Continuous monitoring

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

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

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