

# Federal Information Security Management Act

*Applying NIST Information Security Standards and Guidelines*

Presented to the State of California

April 20, 2008

Dr. Ron Ross

*Computer Security Division  
Information Technology Laboratory*

# The Current Landscape

- Public and private sector enterprises today are *highly dependent* on information systems to carry out their missions and business functions.
- To achieve mission and business success, enterprise information systems must be *dependable* in the face of serious cyber threats.
- To achieve information system dependability, the systems must be appropriately *protected*.

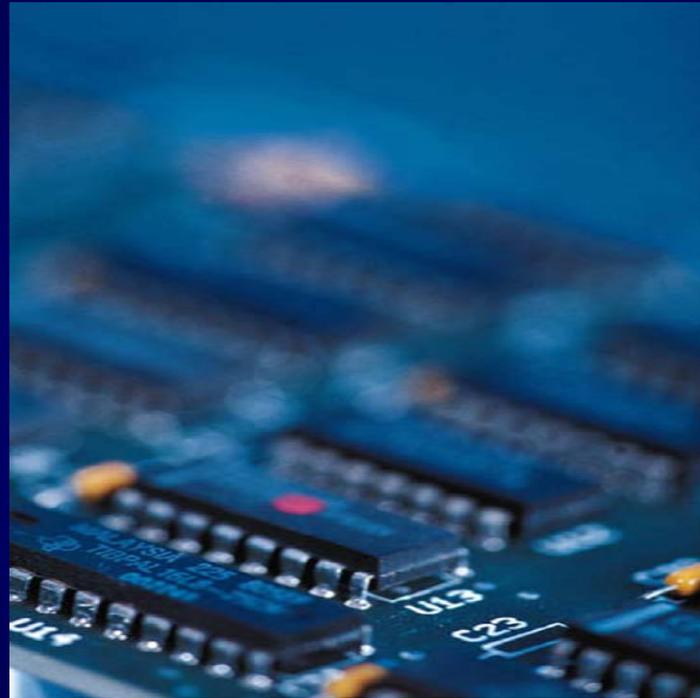
# The Threat Situation

*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.
- Significant exfiltration of critical and sensitive information and implantation of malicious software.

# Unconventional Threats to Security

*Connectivity*



*Complexity*

# Asymmetry of Cyber Warfare

*The weapons of choice are—*

- Laptop computers, hand-held devices, cell phones.
- Sophisticated attack tools and techniques downloadable from the Internet.
- World-wide telecommunication networks including telephone networks, radio, and microwave.

*Resulting in low-cost, highly destructive attack potential.*

# What is at Risk?

- Federal information systems supporting Defense, Civil, and Intelligence agencies within the federal government.
- Private sector information systems supporting U.S. industry and businesses (intellectual capital).
- Information systems supporting critical infrastructures within the United States (public and private sector) including:
  - Energy (electrical, nuclear, gas and oil, dams)
  - Transportation (air, road, rail, port, waterways)
  - Public Health Systems / Emergency Services
  - Information and Telecommunications
  - Defense Industry
  - Banking and Finance
  - Postal and Shipping
  - Agriculture / Food / Water / Chemical

# U.S. Critical Infrastructures

- "...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

-- *USA Patriot Act (P.L. 107-56)*

# Critical Infrastructure Protection

- The U.S. critical infrastructures are over 90% owned and operated by the private sector.
- Critical infrastructure protection must be a partnership between the public and private sectors.
- Information security solutions must be broad-based, consensus-driven, and address the ongoing needs of government and industry.

# A National Imperative

*For economic and national security reasons, we need—*

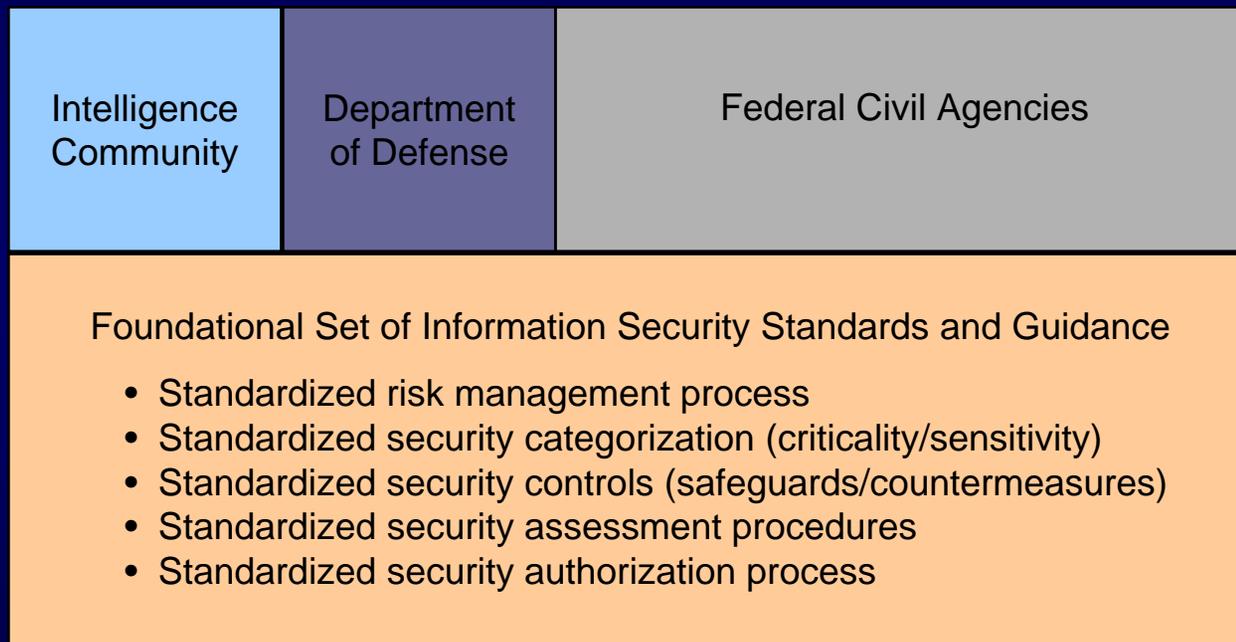
- State-of-the-art cyber defenses for public and private sector enterprises.
- Adequate security for organizational operations (mission, functions, image, and reputation), organizational assets, individuals, other organizations (in partnership with the organization), and the Nation.
- A process for managing cyber risks in a dynamic environment where threats, vulnerabilities, missions, information systems, and operational environments are constantly changing.

# 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

# Risk-Based Protection Strategy

- Enterprise missions and business processes drive security requirements and associated safeguards and countermeasures for organizational information systems.
- Highly flexible implementation; recognizing diversity in mission/business processes and operational environments.
- Senior leaders take ownership of their security plans including the safeguards/countermeasures for the information systems.
- Senior leaders are both responsible and accountable for their information security decisions; understanding, acknowledging, and explicitly accepting resulting mission/business risk.

# Information Security Programs

## Links in the Security Chain: Management, Operational, and Technical Controls

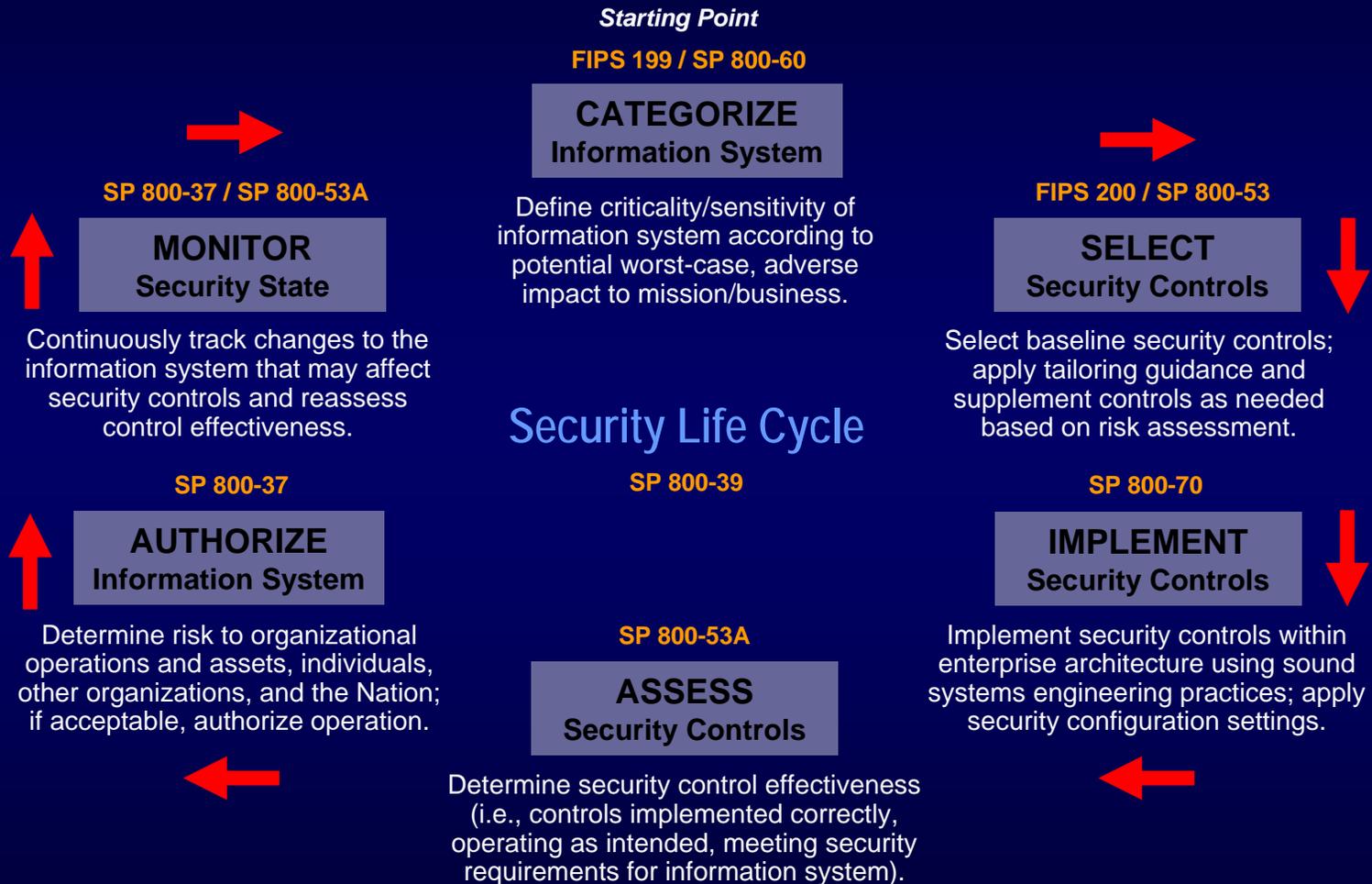
- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification and accreditation
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

Adversaries attack the weakest link...where is yours?

# Strategic Planning Considerations

- Consider vulnerabilities of new information technologies and system integration before deployment.
- Diversify information technology assets.
- Reduce information system complexity.
- Apply a balanced set of management, operational, and technical security controls in a defense-in-depth approach.
- Detect and respond to breaches of information system boundaries.
- Reengineer mission/business processes, if necessary.

# Risk Management Framework



# RMF Characteristics

- The NIST *Risk Management Framework* and the associated security *standards* and *guidance* documents provide a process that is:
  - Disciplined
  - Flexible
  - Extensible
  - Repeatable
  - Organized
  - Structured

*“Building information security into the infrastructure of the organization... so that critical enterprise missions and business cases will be protected.”*

# Security Categorization

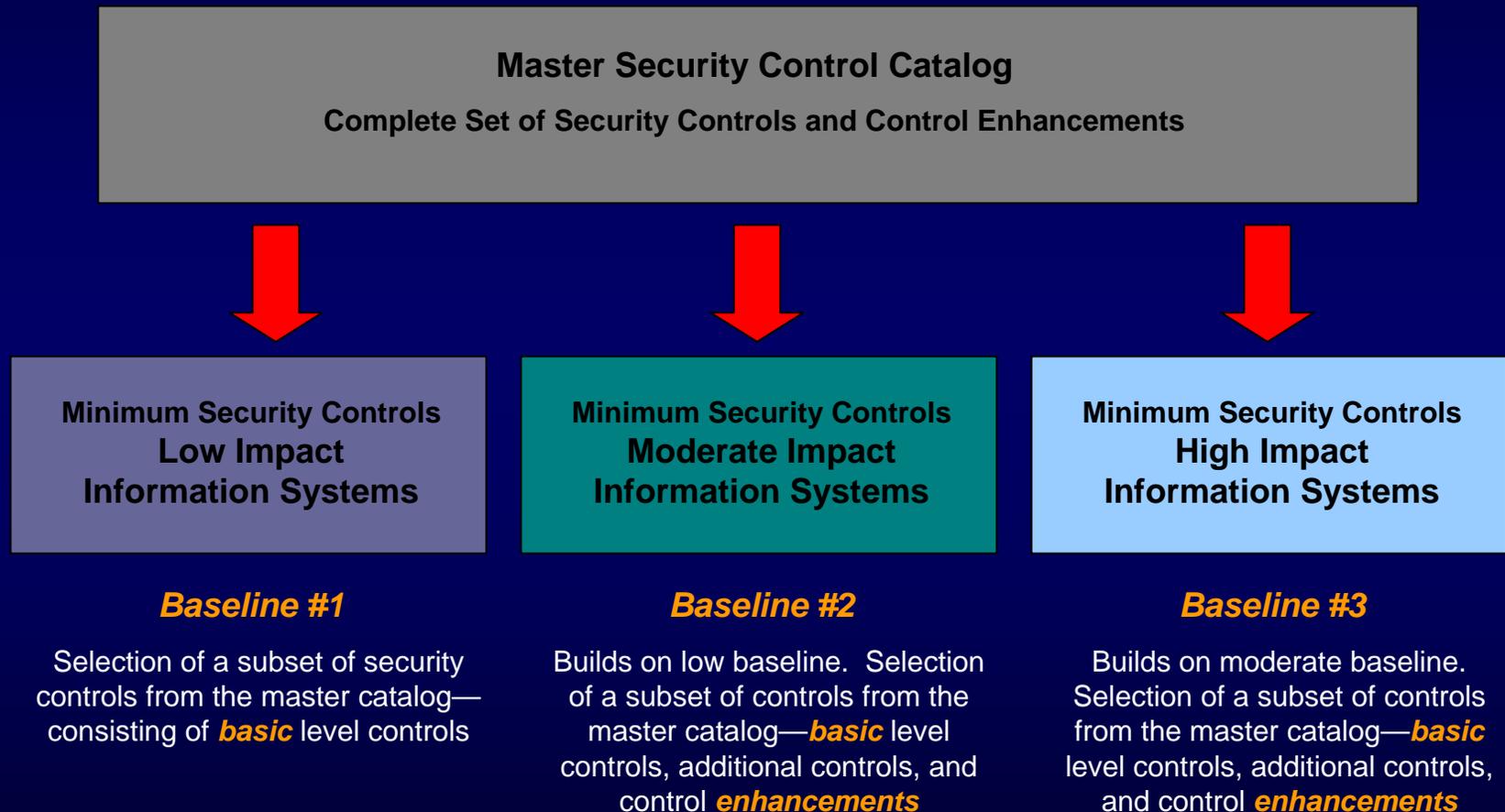
*Example: An Enterprise Information System*

Mapping  
Information  
Types to FIPS  
199 Security  
Categories



FIPS 199	LOW	MODERATE	HIGH
<b>Confidentiality</b>	The loss of confidentiality could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Integrity</b>	The loss of integrity could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b>Availability</b>	The loss of availability could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

# Security Control Baselines

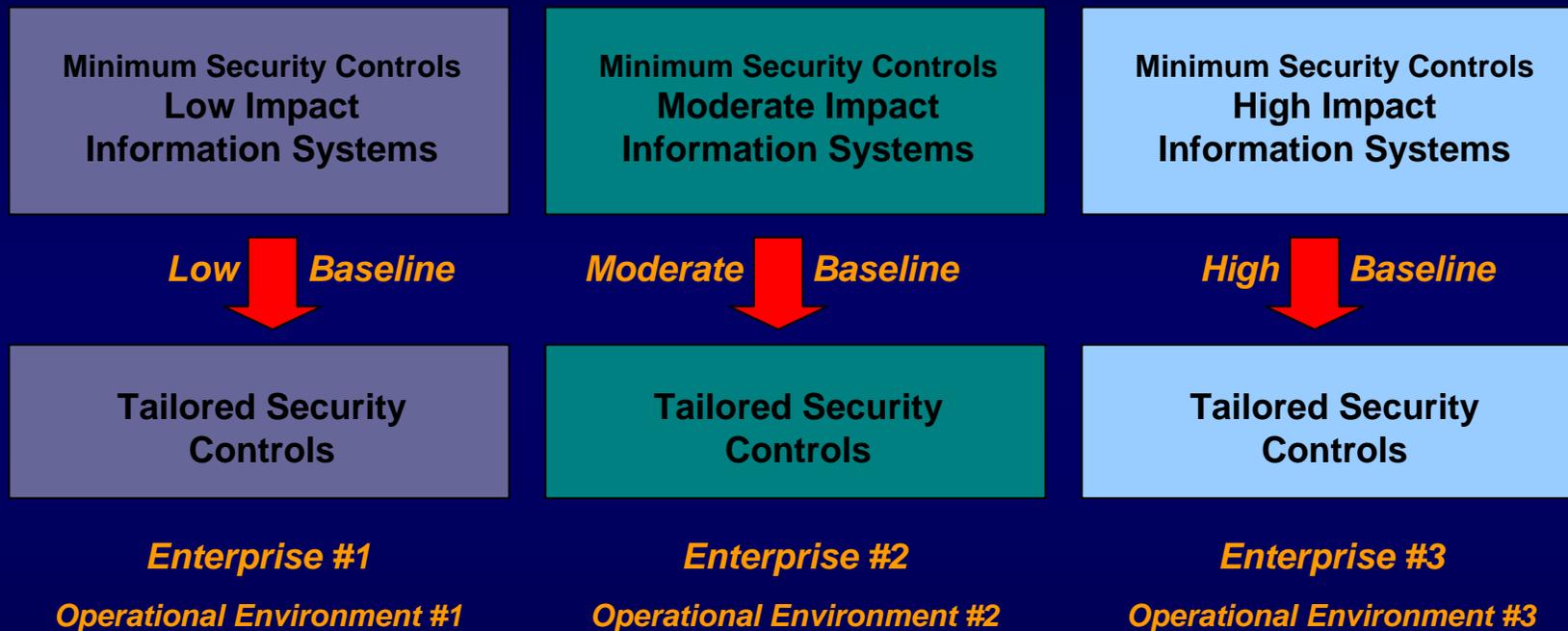


# Tailoring Guidance

- FIPS 200 and SP 800-53 provide significant flexibility in the security control selection and specification process:
  - Scoping guidance;
  - Compensating security controls; and
  - Organization-defined security control parameters.

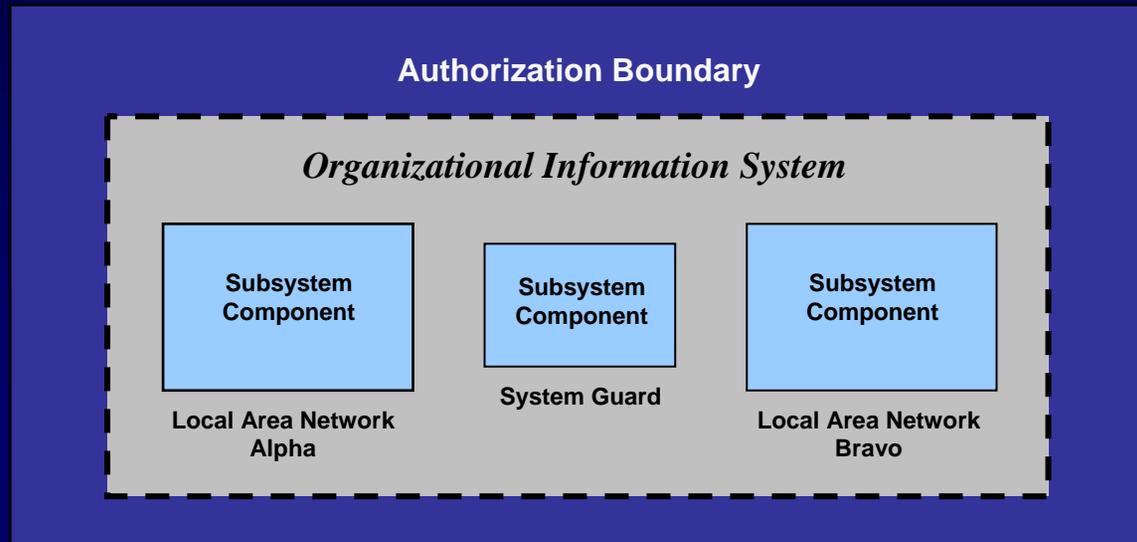
# Tailoring Security Controls

*Scoping, Parameterization, and Compensating Controls*



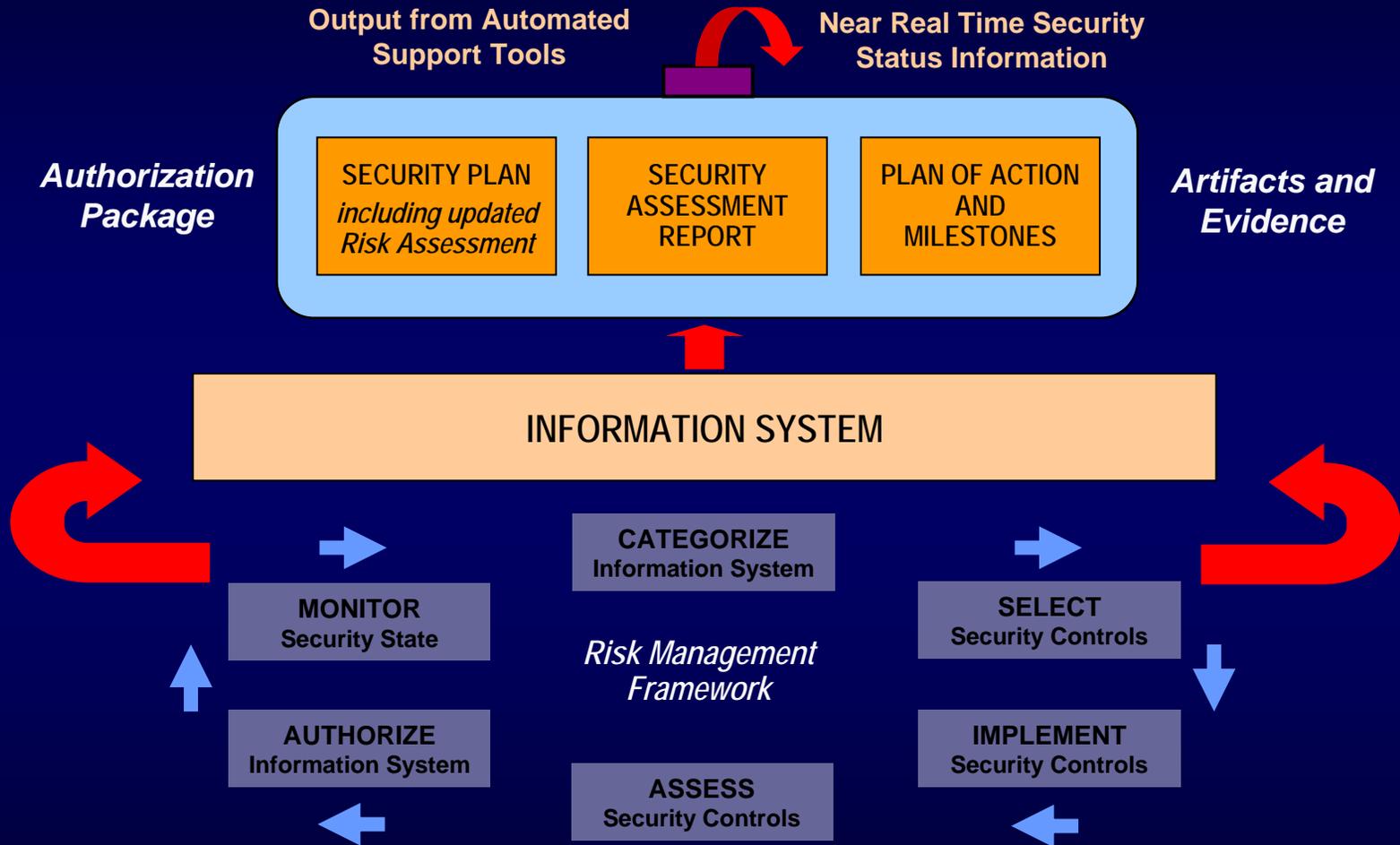
Cost effective, risk-based approach to achieving adequate information security...

# Large and Complex Systems

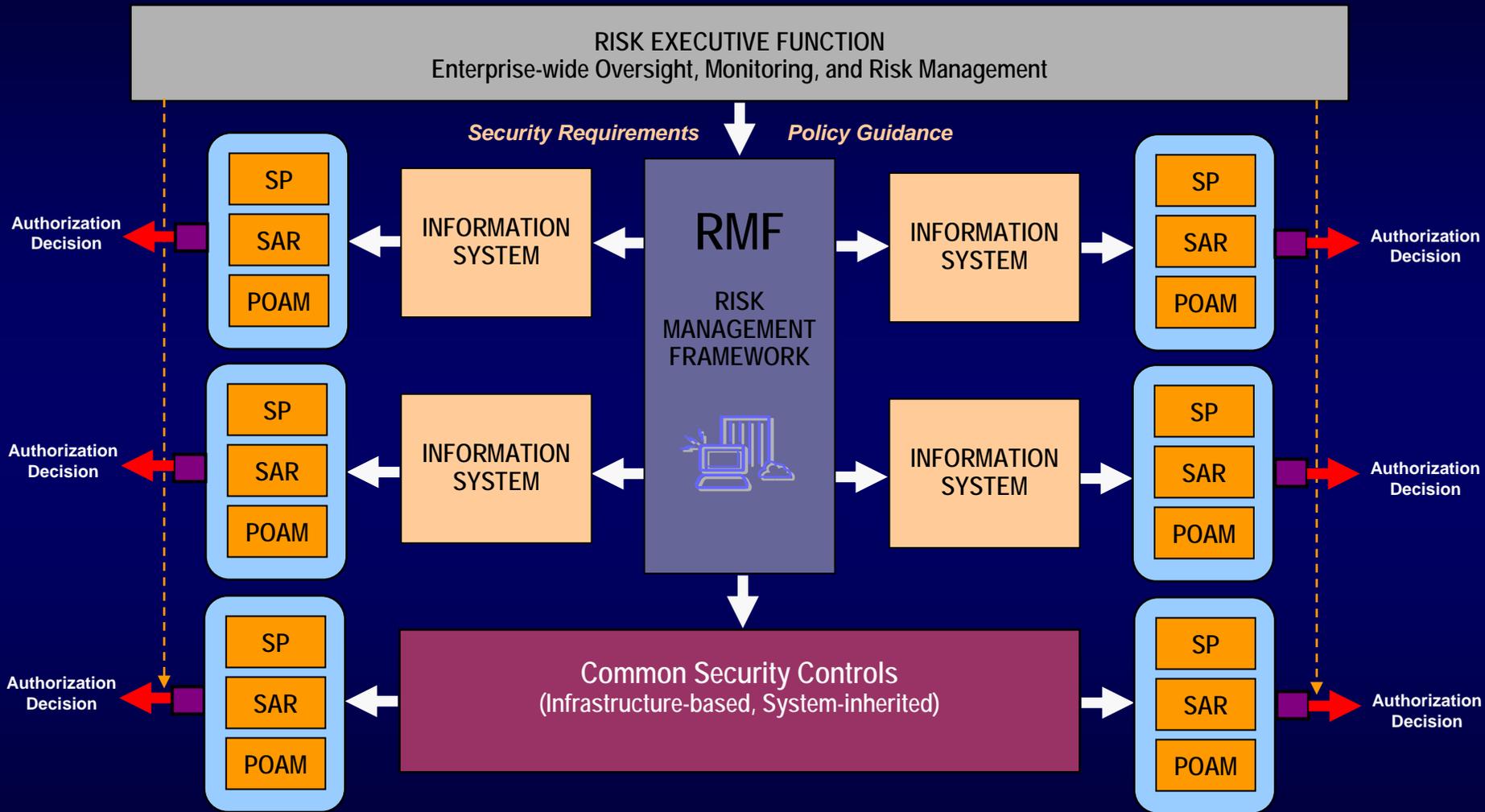


- System security plan reflects information system decomposition with adequate security controls assigned to each subsystem component.
- Security assessment procedures tailored for the security controls in each subsystem component and for the combined system-level controls.
- Security assessment performed on each subsystem component and on system-level controls not covered by subsystem assessments.
- Security authorization performed on the information system as a whole.

# Applying the Risk Management Framework to Information Systems

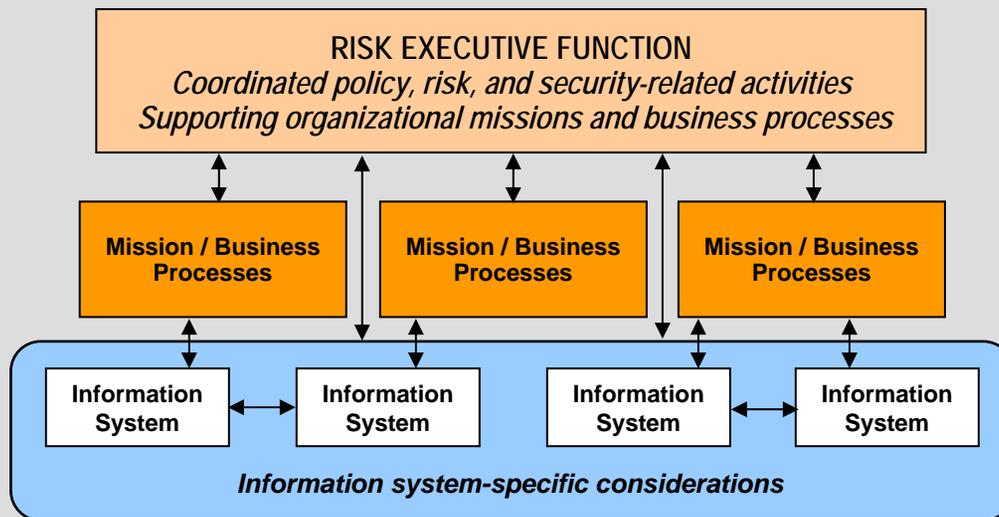


# Extending the Risk Management Framework to Organizations



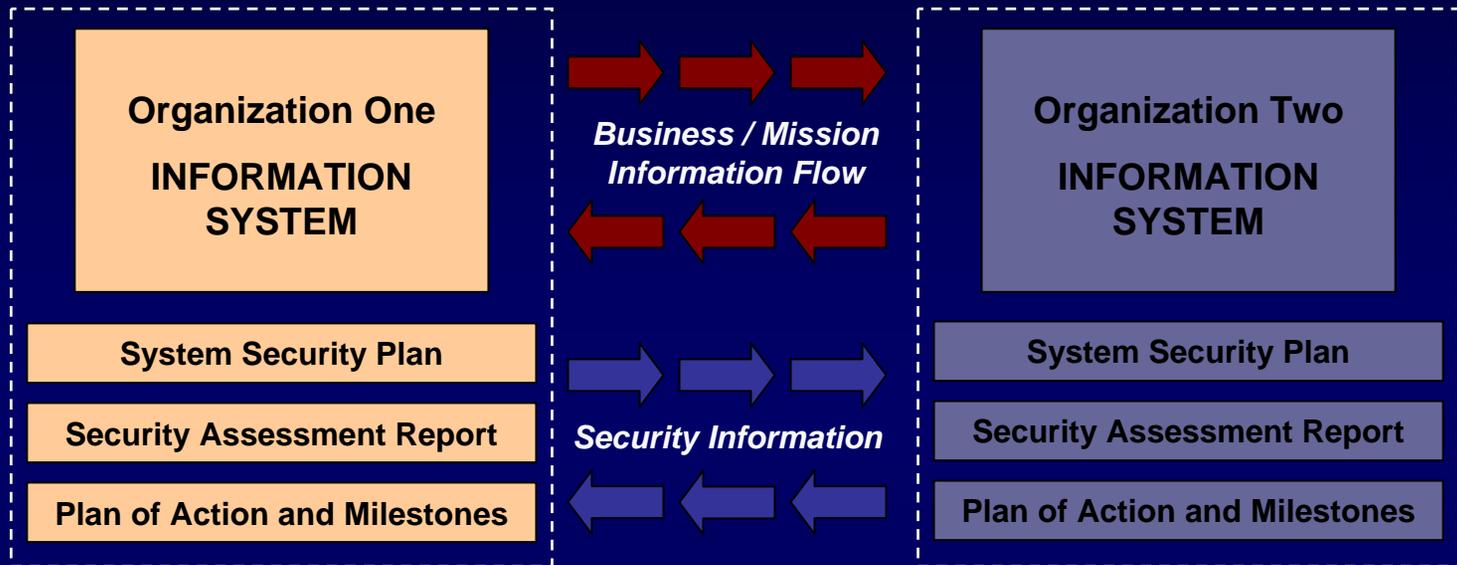
# Risk Executive Function

## *Managing Risk at the Organizational Level*



- Establish organizational information security priorities.
- Allocate information security resources across the organization.
- Provide oversight of information system security categorizations.
- Identify and assign responsibility for common security controls.
- Provide guidance on security control selection (tailoring and supplementation).
- Define common security control inheritance relationships for information systems.
- Establish and apply mandatory security configuration settings.
- Identify and correct systemic weaknesses and deficiencies in information systems.

# Trust Relationships



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 *visibility* into and *understanding* of prospective partner's information security programs...establishing a trust relationship based on the trustworthiness of their information systems.

# Main Streaming Information Security

- Information security requirements must be considered *first order requirements* and are critical to mission and business success.
- An effective organization-wide information security program helps to ensure that security considerations are specifically addressed in the *enterprise architecture* for the organization and are integrated early into the *system development life cycle*.

# Enterprise Architecture

- Provides a common language for discussing information security in the context of organizational missions, business processes, and performance goals.
- Defines a collection of interrelated reference models that are focused on lines of business including Performance, Business, Service Component, Data, and Technical.
- Uses a security and privacy profile to describe how to integrate the Risk Management Framework into the reference models.

# System Development Life Cycle

- The Risk Management Framework should be integrated into all phases of the SDLC.
  - **Initiation** (RMF Steps 1 and 2)
  - **Development and Acquisition** (RMF Step 2)
  - **Implementation** (RMF Steps 3 through 5)
  - **Operations and Maintenance** (RMF Step 6)
  - **Disposition** (RMF Step 6)
- Reuse system development artifacts and evidence (e.g., design specifications, system documentation, testing and evaluation results) for risk management activities.

# FISMA Phase I Publications

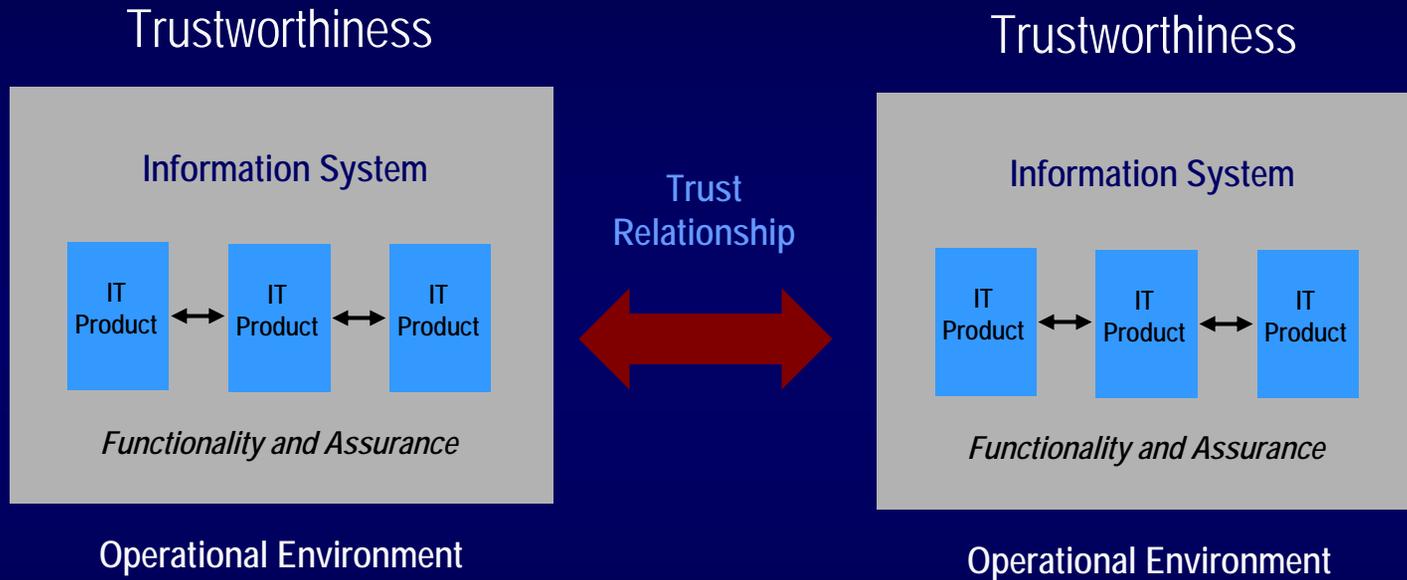
- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment)
- NIST Special Publication 800-39 (Risk Management)
- NIST Special Publication 800-37 (Certification & 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)

# FISMA Phase II

*Demonstrating competence to provide information security services including—*

- Assessments of Information Systems  
*(Operational environments)*
  - *Security controls*
  - *Configuration settings*
  
- Assessments of Information Technology Products  
*(Laboratory environments)*
  - *Security functionality (features)*
  - *Configuration settings*

# FISMA Phase II



*Producing evidence that supports the grounds for confidence in the design, development, implementation, and operation of information systems.*

# Training Initiative

- Information security training initiative underway to provide increased support to organizations using FISMA-related security standards and guidelines.
- Training initiative includes three components—
  - *Frequently Asked Questions*
  - *Publication Summary Guides (Quickstart Guides)*
  - *Formal Curriculum and Training Courses*
- NIST will provide initial training in order to fine-tune the curriculum; then transition to other providers.

# The Golden Rules

## *Building an Effective Enterprise Information Security Program*

- Develop an enterprise-wide information security strategy and game plan.
- Get corporate “buy in” for the enterprise information security program—effective programs start at the top.
- Build information security into the infrastructure of the enterprise.
- Establish level of “due diligence” for information security.
- Focus initially on mission/business process impacts—bring in threat information only when specific and credible.

# The Golden Rules

## *Building an Effective Enterprise Information Security Program*

- Create a balanced information security program with management, operational, and technical security controls.
- Employ a solid foundation of security controls first, then build on that foundation guided by an assessment of risk.
- Avoid complicated and expensive risk assessments that rely on flawed assumptions or unverifiable data.
- Harden the target; place multiple barriers between the adversary and enterprise information systems.

# The Golden Rules

## *Building an Effective Enterprise Information Security Program*

- Be a good consumer—beware of vendors trying to sell single point solutions for enterprise security problems.
- Don't be overwhelmed with the enormity or complexity of the information security problem—take one step at a time and build on small successes.
- Don't tolerate indifference to enterprise information security problems.

*And finally...*

- Manage enterprise risk—don't try to avoid it!

# Contact Information

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

## ***Project Leader***

**Dr. Ron Ross**  
**(301) 975-5390**  
[ron.ross@nist.gov](mailto:ron.ross@nist.gov)

## ***Administrative Support***

**Peggy Himes**  
**(301) 975-2489**  
[peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

## ***Senior Information Security Researchers and Technical Support***

**Marianne Swanson**  
**(301) 975-3293**  
[marianne.swanson@nist.gov](mailto:marianne.swanson@nist.gov)

**Dr. Stu Katzke**  
**(301) 975-4768**  
[skatzke@nist.gov](mailto:skatzke@nist.gov)

**Pat Toth**  
**(301) 975-5140**  
[patricia.toth@nist.gov](mailto:patricia.toth@nist.gov)

**Arnold Johnson**  
**(301) 975-3247**  
[arnold.johnson@nist.gov](mailto:arnold.johnson@nist.gov)

**Matt Scholl**  
**(301) 975-2941**  
[matthew.scholl@nist.gov](mailto:matthew.scholl@nist.gov)

**Information and Feedback**  
**Web: [csrc.nist.gov/sec-cert](http://csrc.nist.gov/sec-cert)**  
**Comments: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)**