

# Next Generation Risk Management

*Information Security Transformation for the Federal Government*

Webex Seminar

March 30, 2010

Dr. Ron Ross

*Computer Security Division  
Information Technology Laboratory*

# Risk and Security

- What is the difference between risk and security?

- **Information Security**

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Risk**

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

- Types of Threats

***Purposeful attacks, environmental disruptions, and human errors.***

# The Cyber Threat Situation

*Continuing serious cyber attacks on public and private sector information systems, large and small; targeting key 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.

# What is at Risk?

- Federal information systems supporting Defense, Civil, and Intelligence agencies within the federal government.
- Information systems supporting critical infrastructures within the United States (public and private sector).
- Private sector information systems supporting U.S. industry and businesses (intellectual capital).

***Producing both national security and economic security concerns for the Nation...***

# Need Broad-Based Security Solutions

- Over 90% of critical infrastructure systems/applications owned and operated by non federal entities.
- Key sectors:
  - 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



# The Fundamentals

*Combating 21<sup>st</sup> century cyber attacks requires 21<sup>st</sup> century strategies, tactics, training, and technologies...*

- Integration of information security into enterprise architectures and system life cycle processes.
- Unified information security framework and common, shared security standards and guidance.
- Enterprise-wide, risk-based protection strategies.
- Flexible and agile selection and deployment of security controls (i.e., safeguards and countermeasures).
- More resilient, penetration-resistant information systems.
- Competent, capable cyber warriors.

# 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

# Unified Information Security Framework

## The Generalized Model

**Unique  
Information  
Security  
Requirements**

*The "Delta"*

Intelligence Community	Department of Defense	Federal Civil Agencies	C N S S	Private Sector State/Local Govt
---------------------------	--------------------------	---------------------------	------------------	------------------------------------

**Common  
Information  
Security  
Requirements**

Foundational Set of Information Security Standards and Guidance

- Risk management (organization, mission, information system)
- Security categorization (information criticality/sensitivity)
- Security controls (safeguards and countermeasures)
- Security assessment procedures
- Security authorization process

**National security and non national security information systems**

# Characteristics of Risk-Based Approaches

(1 of 3)

- Integrates information security more closely into the enterprise architecture and system development life cycle.
- Provides equal emphasis on the security control selection, implementation, assessment, and monitoring, and the authorization of information systems.
- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.

# Characteristics of Risk-Based Approaches

(2 of 3)

- Links risk management activities at the organization, mission, and information system levels through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems.

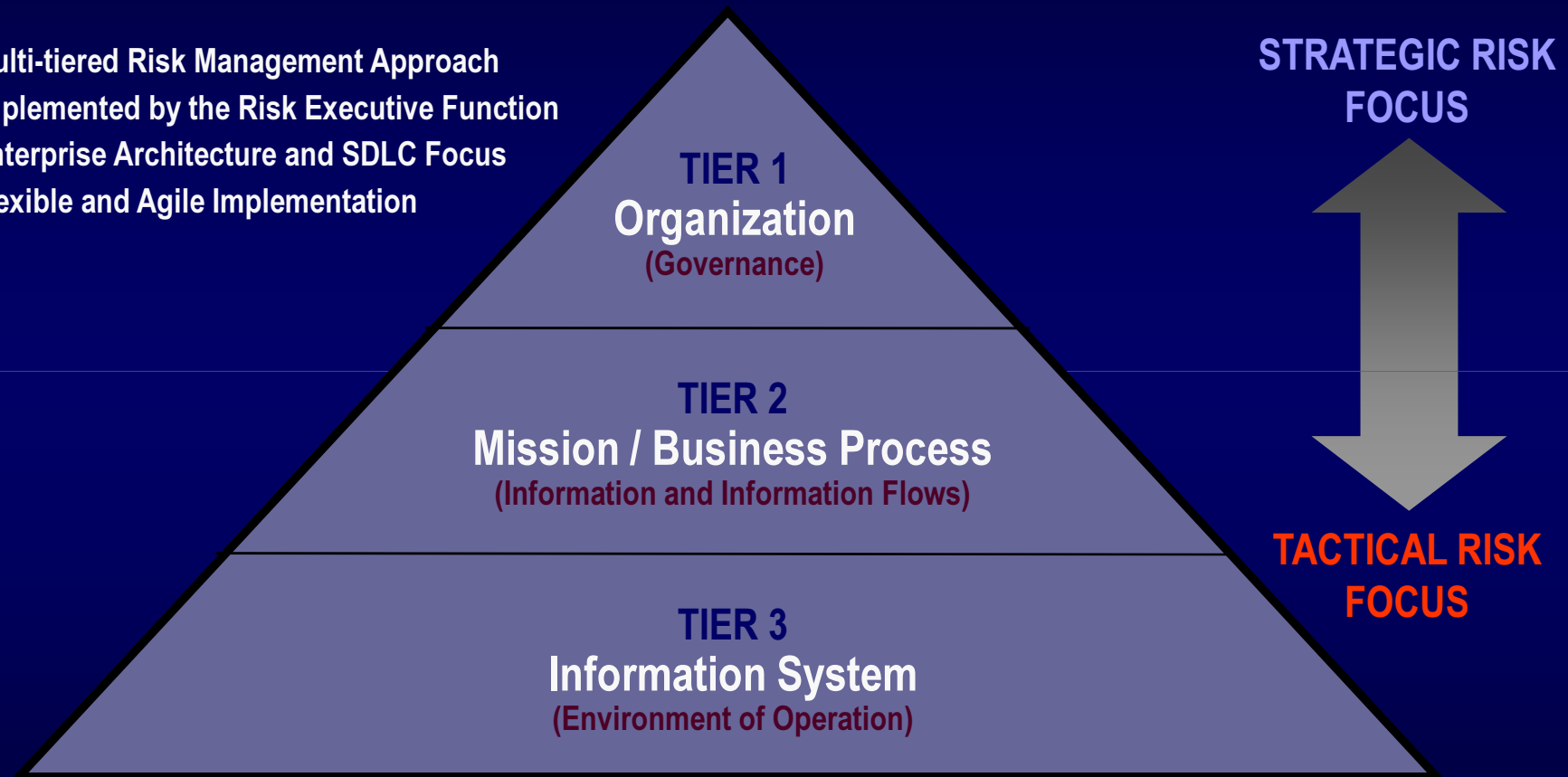
# Characteristics of RMF-Based Process

(3 of 3)

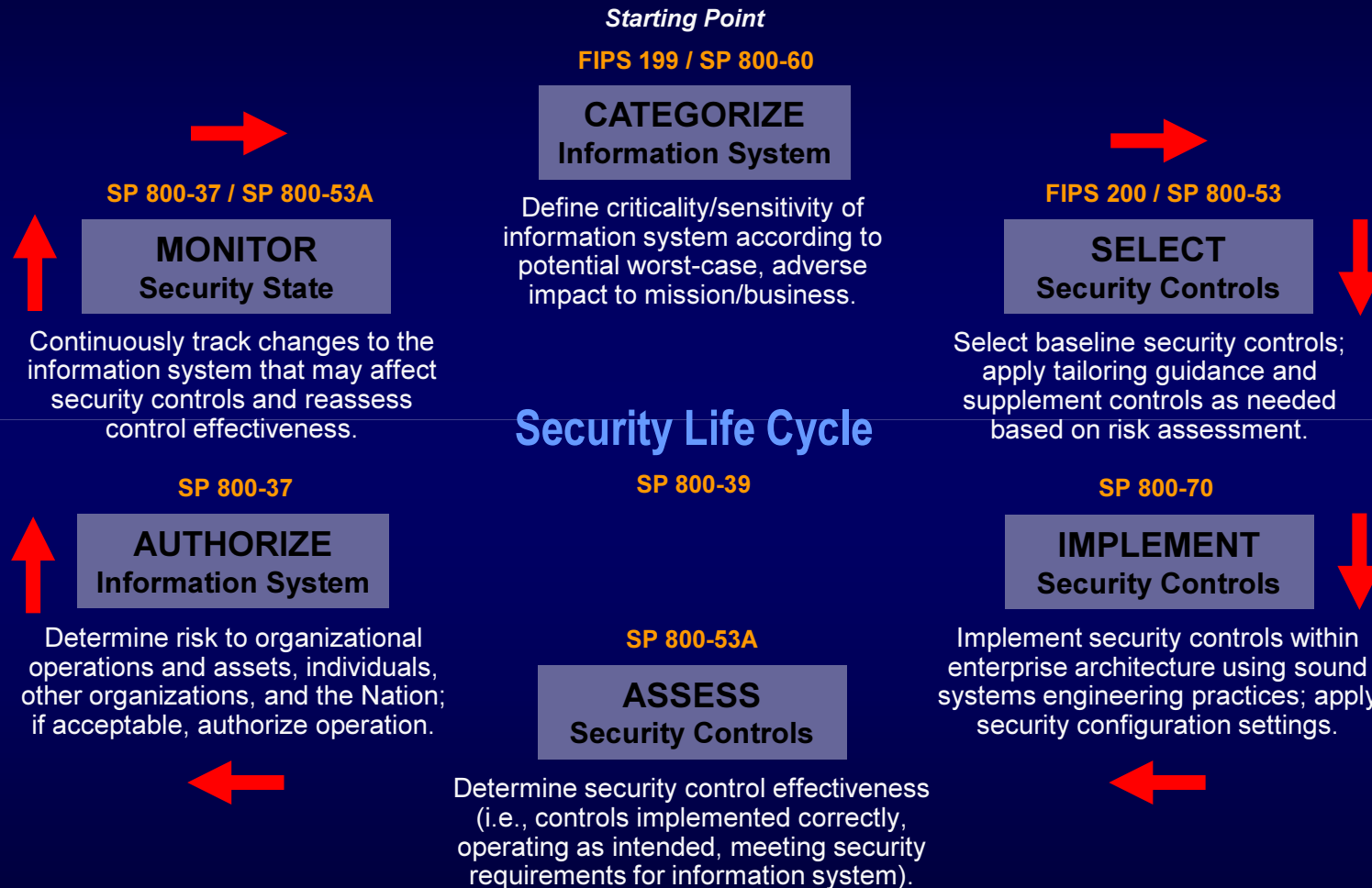
- Encourages the use of automation to:
  - Increase consistency, effectiveness, and timeliness of security control implementation and functionality; and
  - Provide senior leaders the necessary information to take credible, risk-based decisions with regard to the information systems supporting their core missions and business functions.

# Enterprise-Wide Risk Management

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

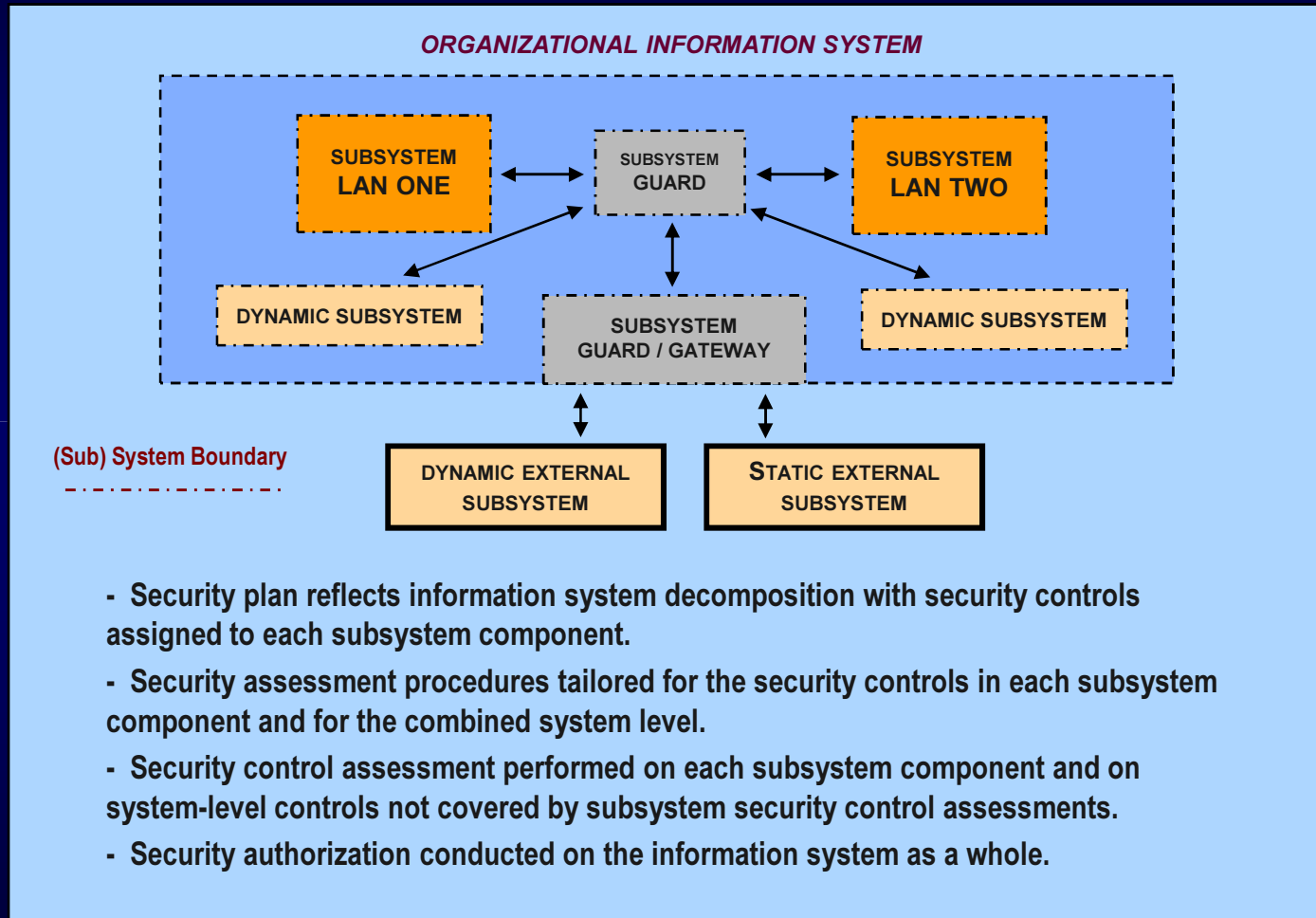


# Risk Management Framework

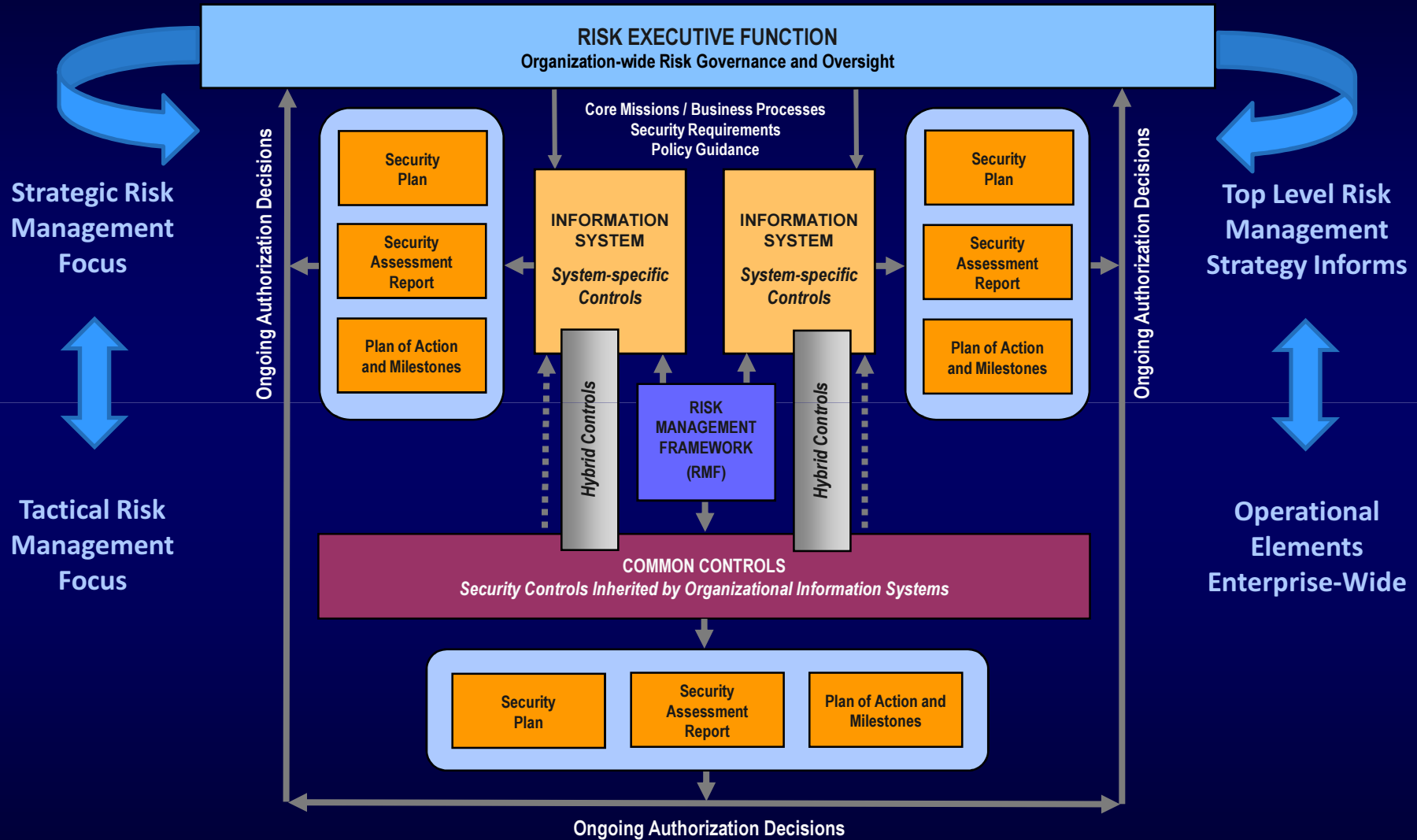


# Large and Complex Systems

(Including System of Systems)



# Security Control Allocation



# References

---

# Joint Task Force Transformation Initiative

## Core Risk Management Publications

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



Completed

- NIST Special Publication 800-37, Revision 1  
*Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach*



Completed

- NIST Special Publication 800-53A, Revision 1  
*Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

*Projected June 2010*

# Joint Task Force Transformation Initiative

## *Core Risk Management Publications*

- NIST Special Publication 800-39  
*Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View*  
*Projected November 2010*
- NIST Special Publication 800-30, Revision 1  
*Guide for Conducting Risk Assessments*  
*Projected November 2010*

# 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)

Kelley Dempsey  
(301) 975-2827  
[kelley.dempsey@nist.gov](mailto:kelley.dempsey@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)

Web: [csrc.nist.gov/sec-cert](http://csrc.nist.gov/sec-cert)

Comments: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)