FISMA 2010 and Beyond

Strategic and Tactical Risk Management and the Role of Software Assurance

Software Assurance Forum

June 21, 2010

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

The Perfect Storm

- Explosive growth and aggressive use of information technology.
- Proliferation of information systems and networks with virtually unlimited connectivity.
- Increasing sophistication of threat including exponential growth rate in malware (malicious code).

Resulting in an increasing number of penetrations of information systems in the public and private sectors…

For every complex problem, there is a simple solution and it is usually *wrong*…

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.

Information technology is our greatest *strength* and at the same time, our greatest *weakness*…

We expend far too many resources on *back-end* security…

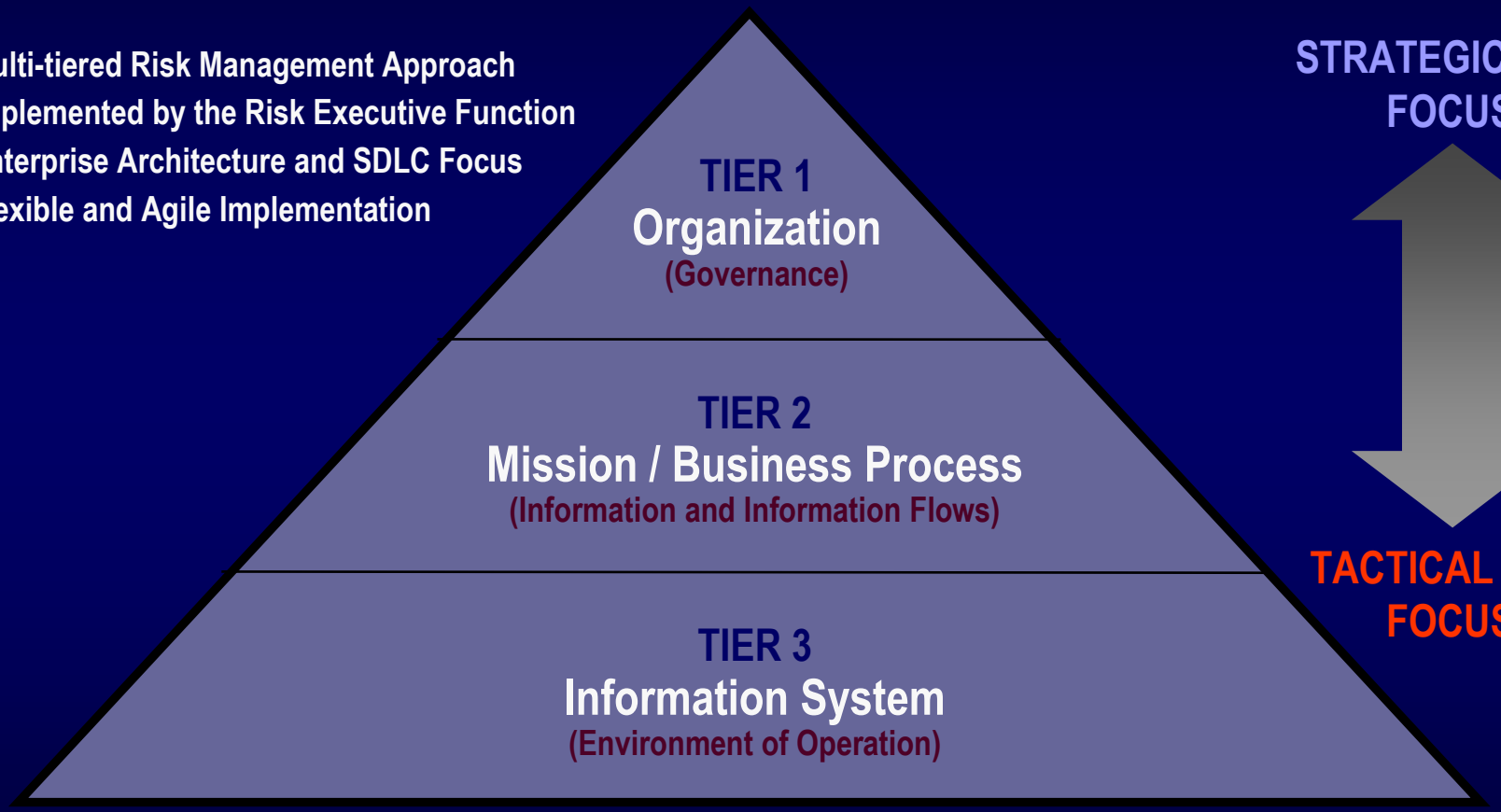
(chasing the latest vulnerabilities and patching systems)

and far too few resources on *front-end* security…

(building information security *into* IT products and systems)

Enterprise-Wide Risk Management

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



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)

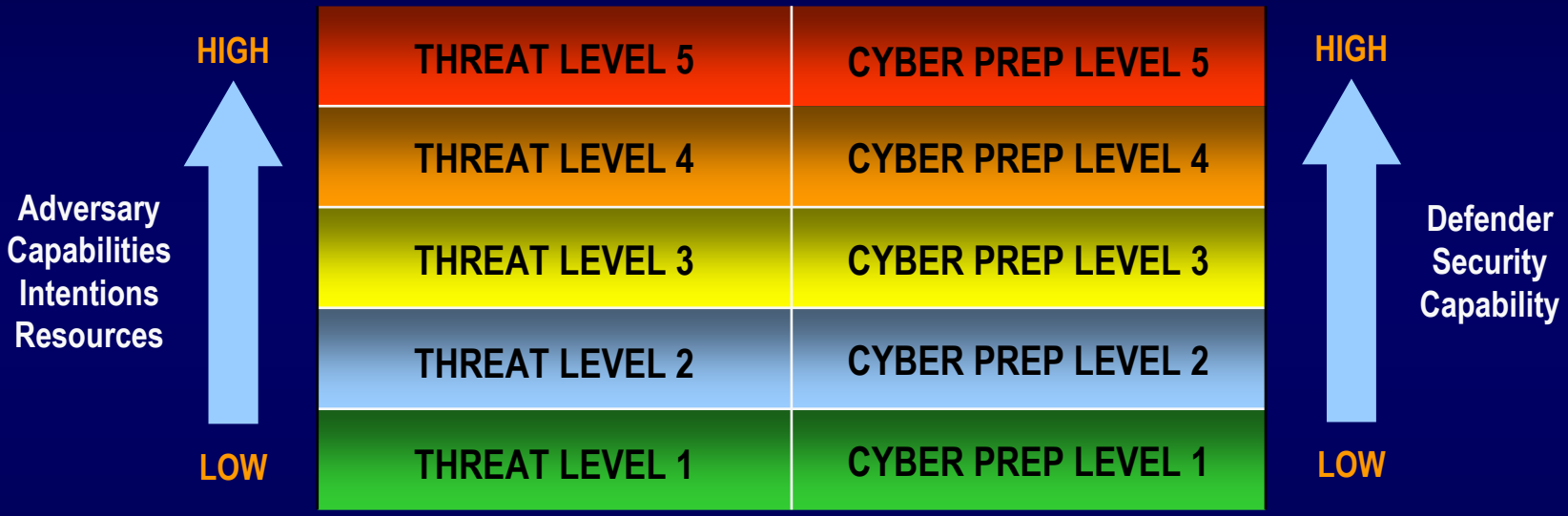
- Links risk management activities at the organization, mission, and information system levels through a risk executive (function).
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems.

Characteristics of Risk-Based Approaches

(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.

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**

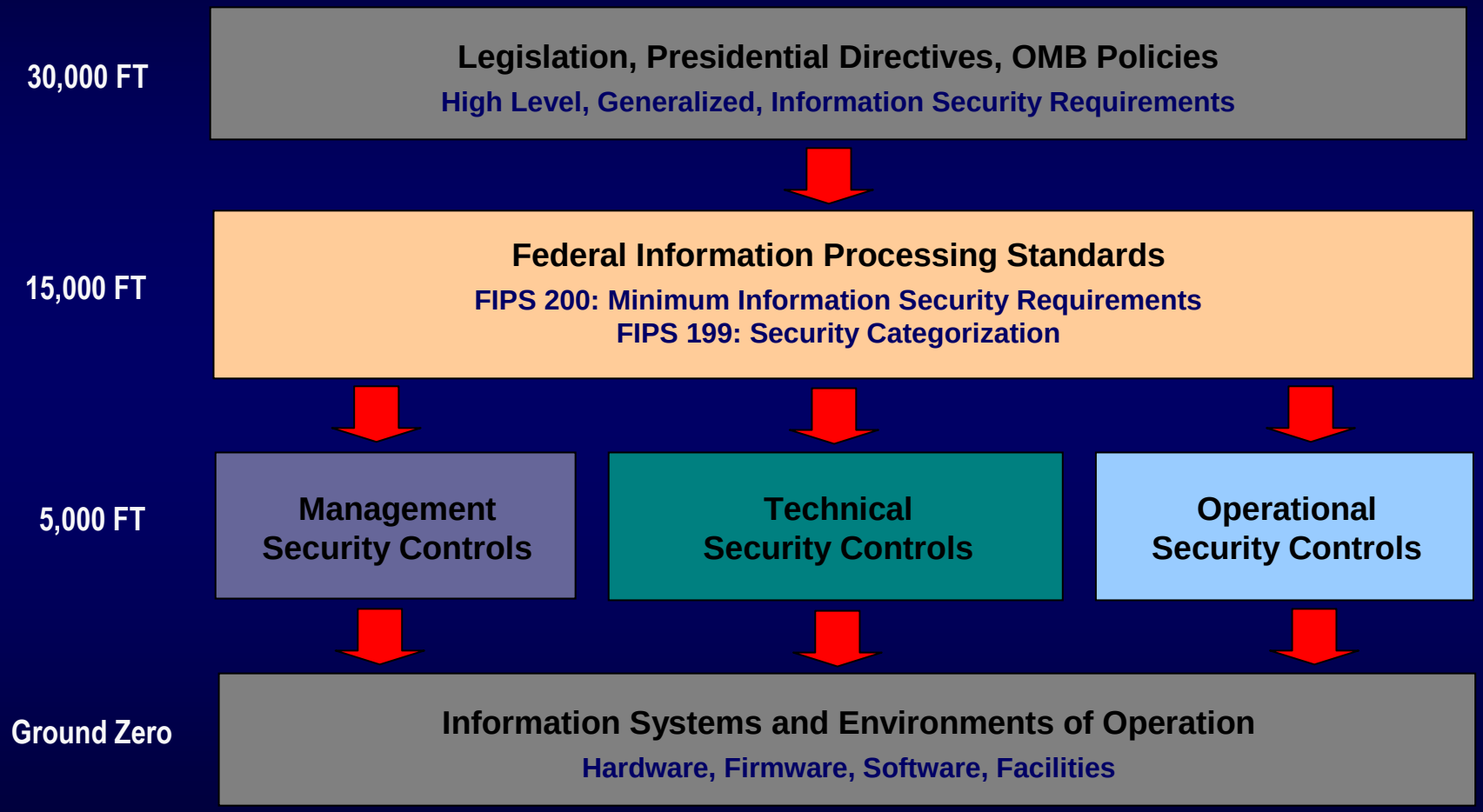
  Primary Consideration: ***Information System Resilience***
  Adversary Location: ***Inside the Defensive Perimeter***
  Objective: ***Operating while under Attack***

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…

Security Requirements Traceability



Security Control Families

Supporting Software Assurance

- Program Management
  - Mission/Business Process Definition
  - Enterprise Architecture
  - Risk Management Strategy
  - Information Security Resources
  - Information Security Measures of Performance
- System and Services Acquisition
  - Resource Allocation
  - Acquisition and Life Cycle Support
  - Security Engineering Principles
  - Developer Configuration Management and Testing
  - Trustworthiness and Critical Information System Components
  - Supply Chain

Security Control Families

Supporting Software Assurance

- Configuration Management
  - Configuration Change Control
  - Security Impact Analysis
  - Access Restrictions for Change
  - Configuration Settings
  - Least Functionality
- System and Information Integrity
  - Security Functionality Verification
  - Software and Information Integrity
  - Information Input Validation
  - Error Handling
  - Predictable Failure Prevention

Security Control Families

Supporting Software Assurance

- System and Communications Protection
  - Application Partitioning
  - Security Function Isolation
  - Information Shared Resources
  - Trusted Path
  - Transmission of Security Attributes
  - Fail in Known State
  - Thin Nodes

Assurance Requirements

Special Publication 800-53

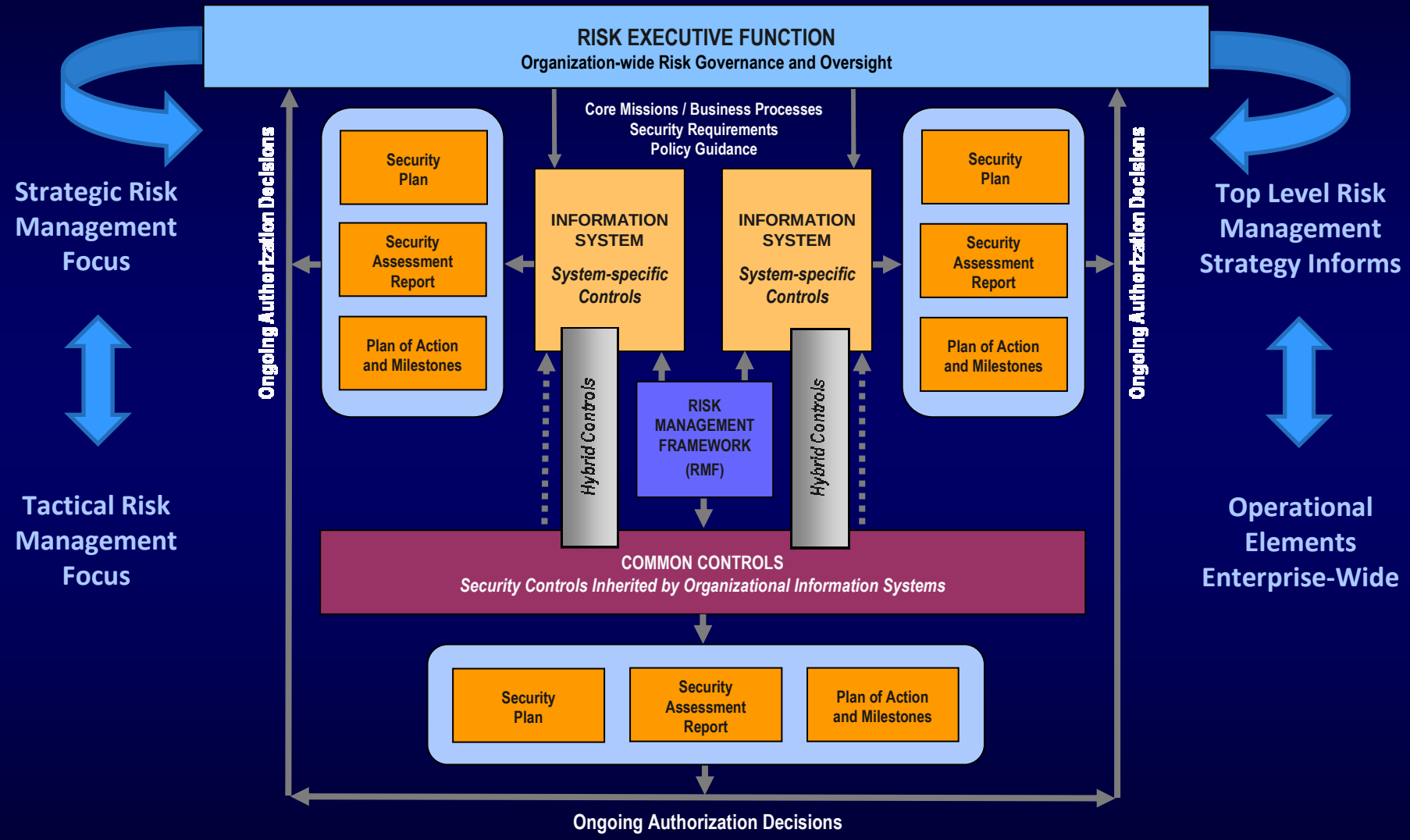
- The security control is in effect and meets explicitly identified functional requirements in the control statement.
- The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control.

Assurance Requirements

Special Publication 800-53

- The control developer/implementer includes as an integral part of the control, actions supporting increased confidence that when the control is implemented, it will continuously and consistently meet its required function or purpose and support improvement in the effectiveness of the control.
- The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.

Managing Complex Risk Activities



Federal Government Transformation

The newly emerging information security publications begin an historic government-wide transformation for risk management and information security driven by…

- Increasing sophistication and operations tempo of cyber attacks.
- Convergence of national and non-national security interests within the federal government.
- Convergence of national security and economic security interests across the Nation.
- Need for a unified framework in providing effective risk-based cyber defenses for the federal government and the Nation.

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

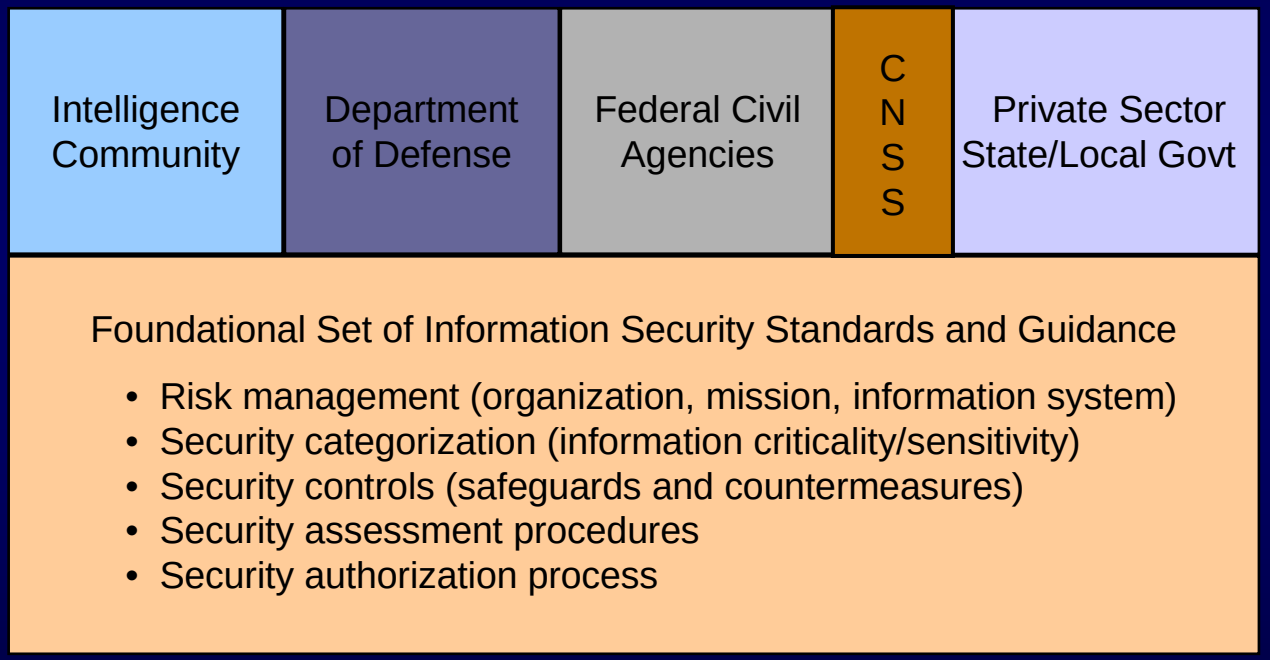
Unified Information Security Framework

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements



National security and non national security information systems

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

2010 Focus Areas and Initiatives

- Common Security Standards and Guidance
  - Joint Task Force Transformation Initiative (DoD, IC, NIST, CNSS)
  - Unified Information Security Framework
  - Core risk management and information security publications
  - Additional publications for partnership collaboration
  - Privacy Appendix for SP 800-53, Revision 3 (privacy controls)
  - Threat Appendix for SP 800-53, Revision 3 (Cyber Prep Initiative)
- Developmental Security
  - Systems and security engineering guideline
  - Application security guideline

2010 Focus Areas and Initiatives

- Operational Security
  - S-CAP Initiative and future extensions (network devices, mainframes)
  - Continuous monitoring guideline
  - Configuration management and control guideline
- Education, Training, and Awareness
  - FISMA Phase II Training Modules
  - Automated support tools
  - Outreach program to State and local governments; private sector
- Prototypes and Use Cases
  - Industrial control systems

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

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

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

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

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

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