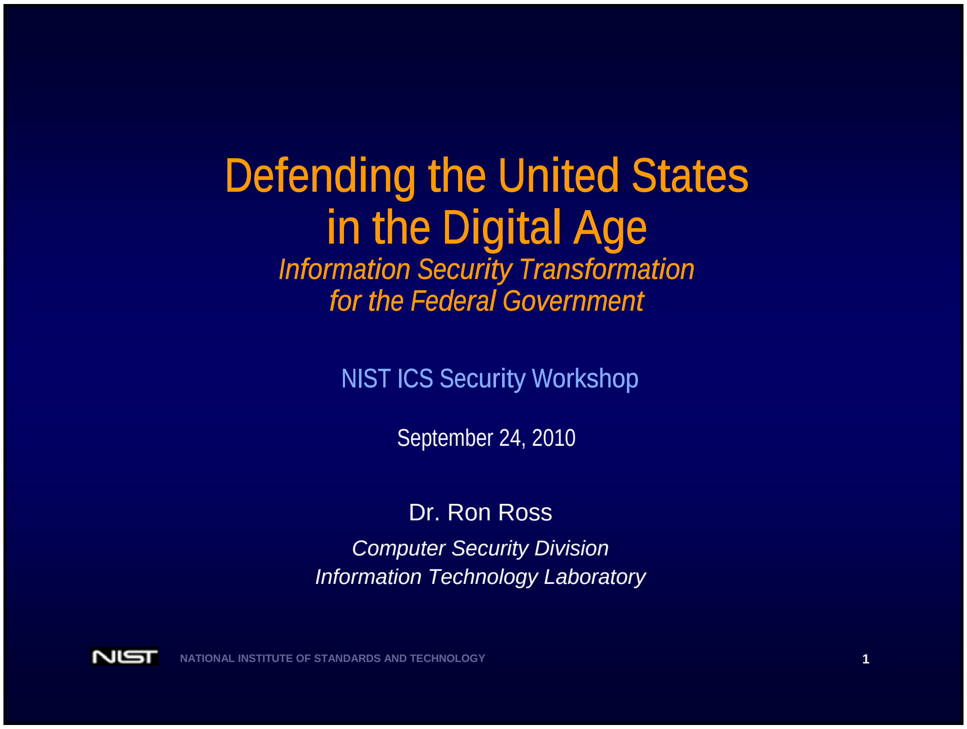


Defending the United States in the Digital Age

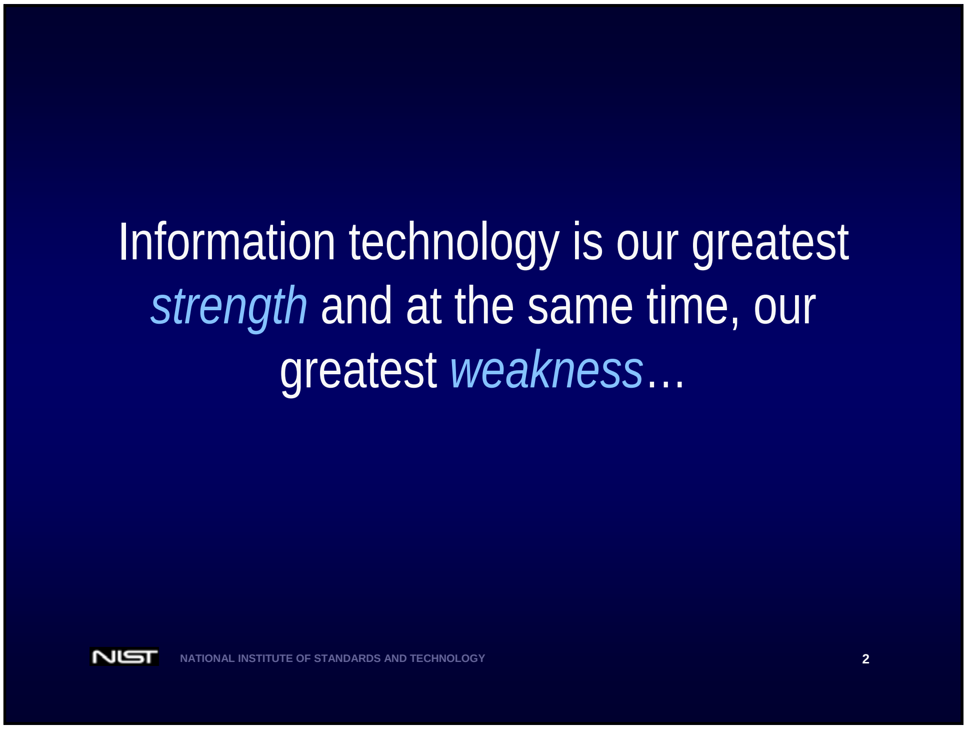
Information Security Transformation for the Federal Government

NIST ICS Security Workshop

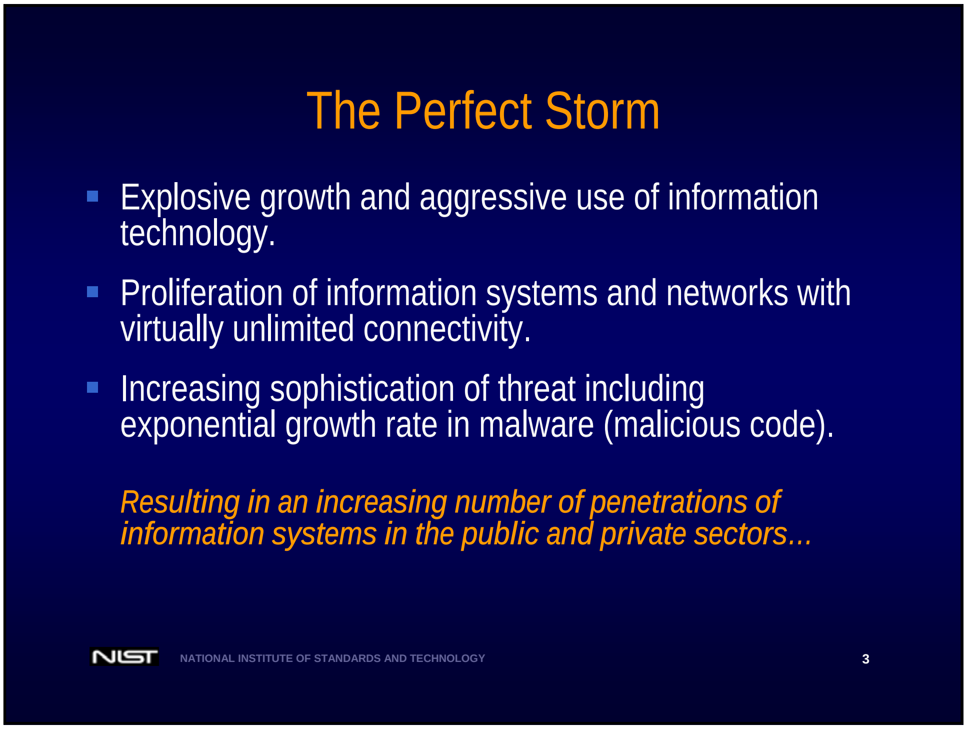
September 24, 2010

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory



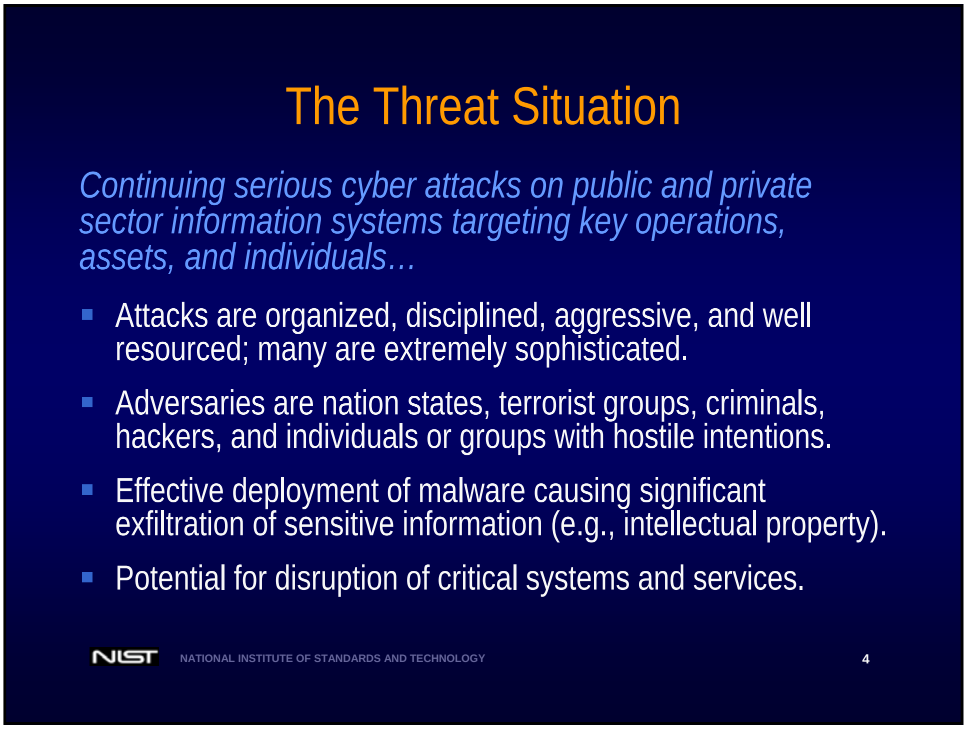
Information technology is our greatest *strength* and at the same time, our greatest *weakness*…



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…



The Threat Situation

Continuing serious cyber attacks on public and private sector information systems targeting key operations, assets, and individuals…

- 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 hostile intentions.
- Effective deployment of malware causing significant exfiltration of sensitive information (e.g., intellectual property).
- Potential for disruption of critical systems and services.

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.

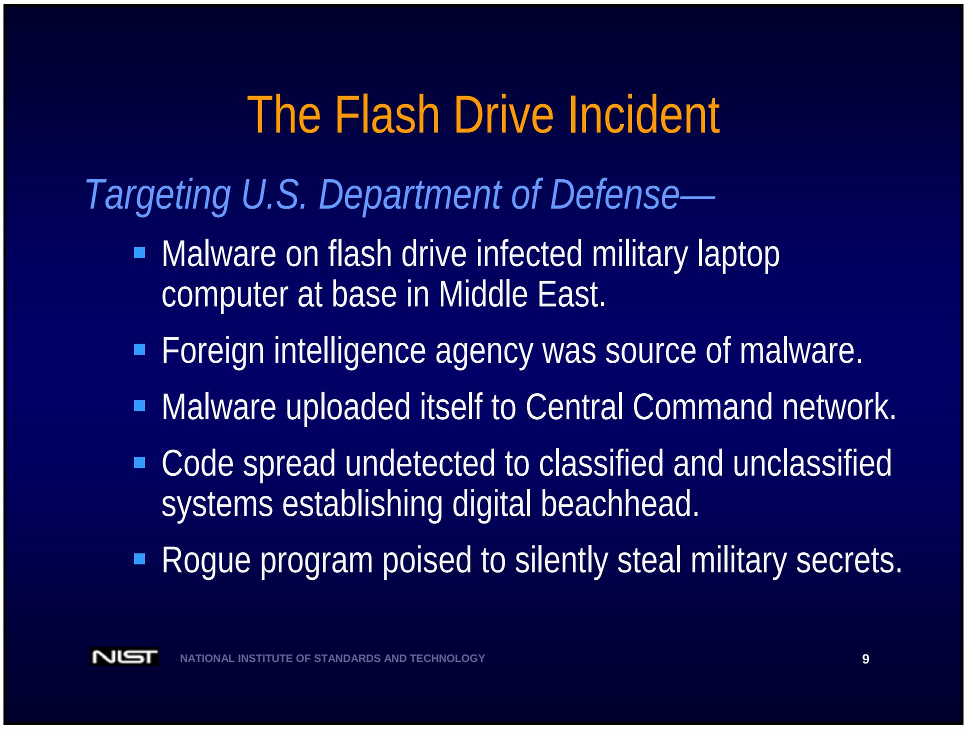
Resulting in low-cost, highly destructive attack potential.

Sometimes adversaries do it to us…
and sometimes we do it to ourselves…

The Stuxnet Worm

Targeting critical infrastructure companies—

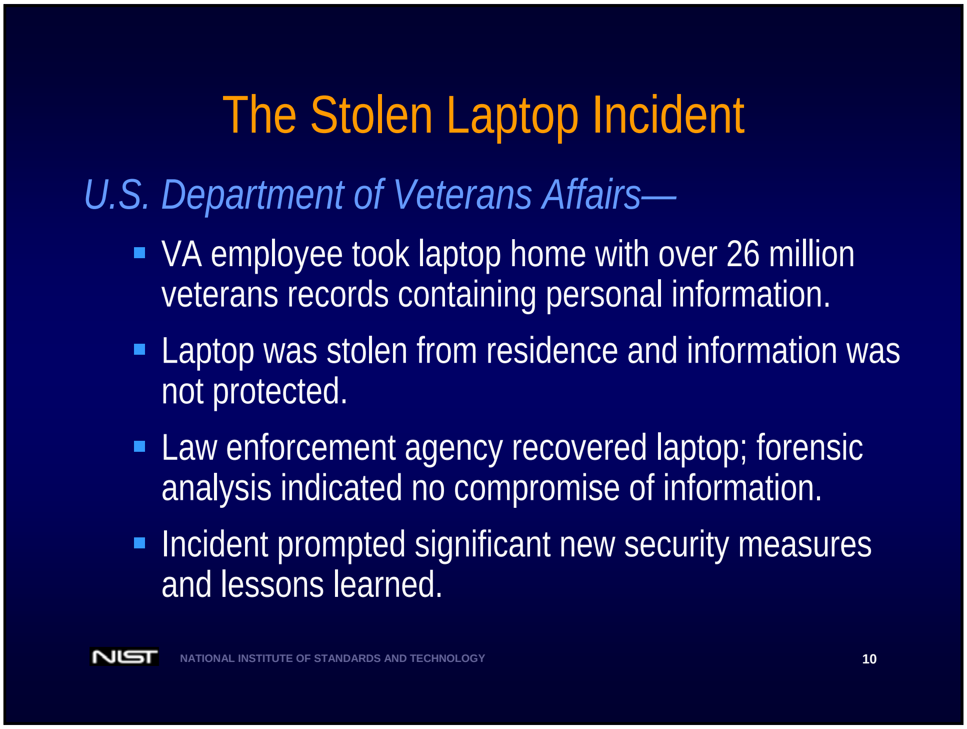
- Infected industrial control systems around the world.
- Uploads payload to Programmable Logic Controllers.
- Gives attacker control of the physical system.
- Provides back door to steal data and remotely and secretly control critical plant operations.
- Found in Siemens Simatic Win CC software used to control industrial manufacturing and utilities.



The Flash Drive Incident

Targeting U.S. Department of Defense—

- Malware on flash drive infected military laptop computer at base in Middle East.
- Foreign intelligence agency was source of malware.
- Malware uploaded itself to Central Command network.
- Code spread undetected to classified and unclassified systems establishing digital beachhead.
- Rogue program poised to silently steal military secrets.



The Stolen Laptop Incident

U.S. Department of Veterans Affairs—

- VA employee took laptop home with over 26 million veterans records containing personal information.
- Laptop was stolen from residence and information was not protected.
- Law enforcement agency recovered laptop; forensic analysis indicated no compromise of information.
- Incident prompted significant new security measures and lessons learned.

We have to do business in a dangerous world…
Managing risk as we go.

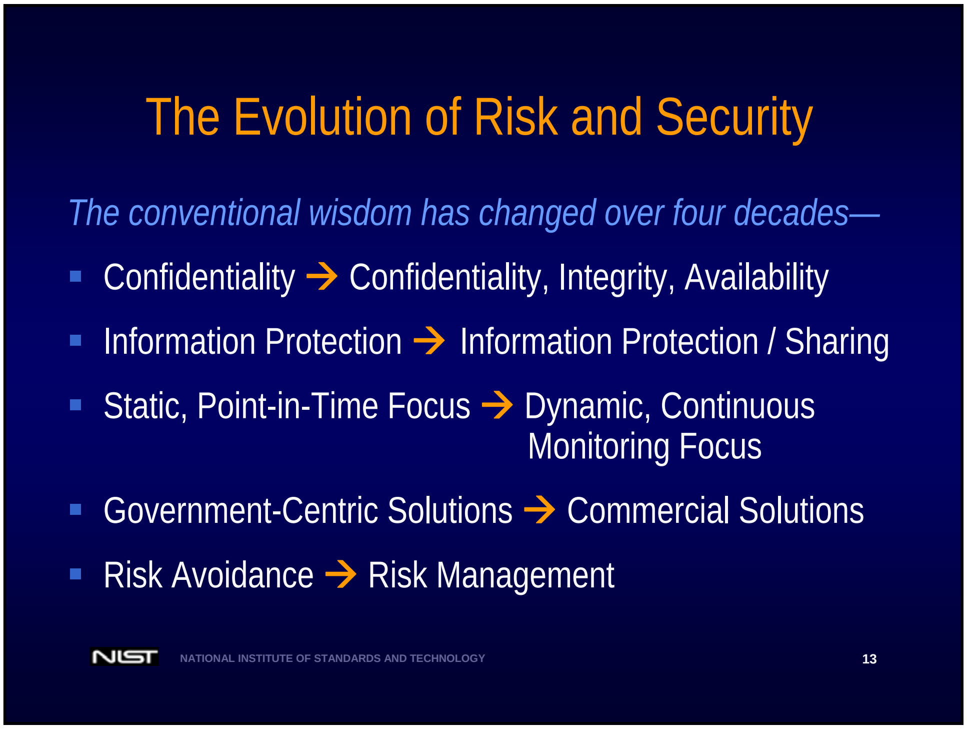
Risk and Security

- 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

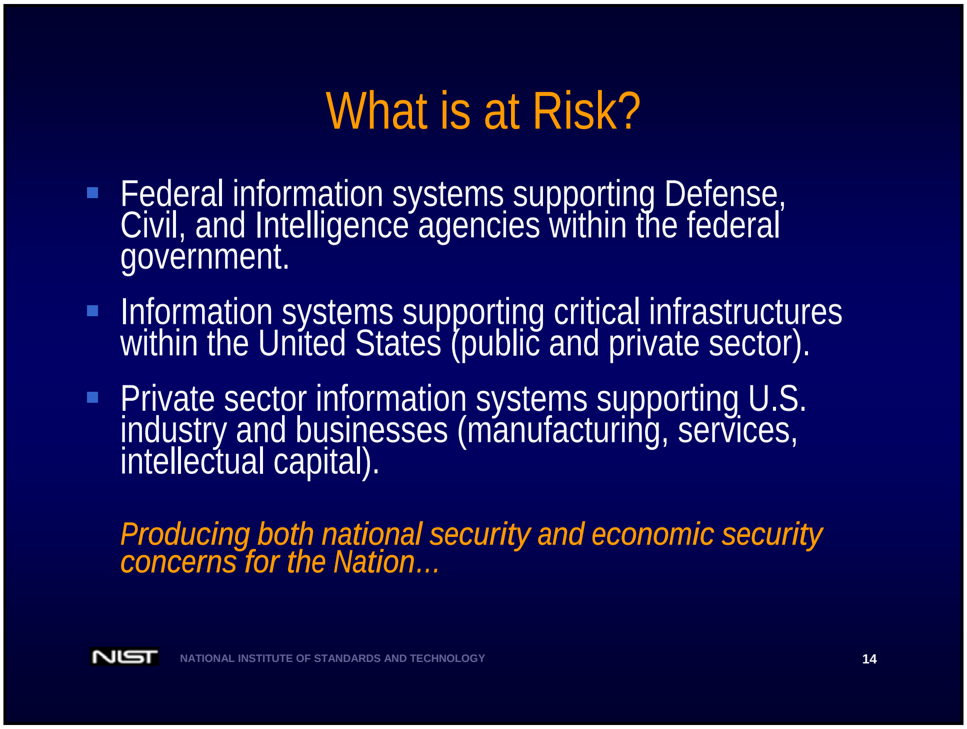
  Purposeful attacks, environmental disruptions, and human errors.



The Evolution of Risk and Security

The conventional wisdom has changed over four decades—

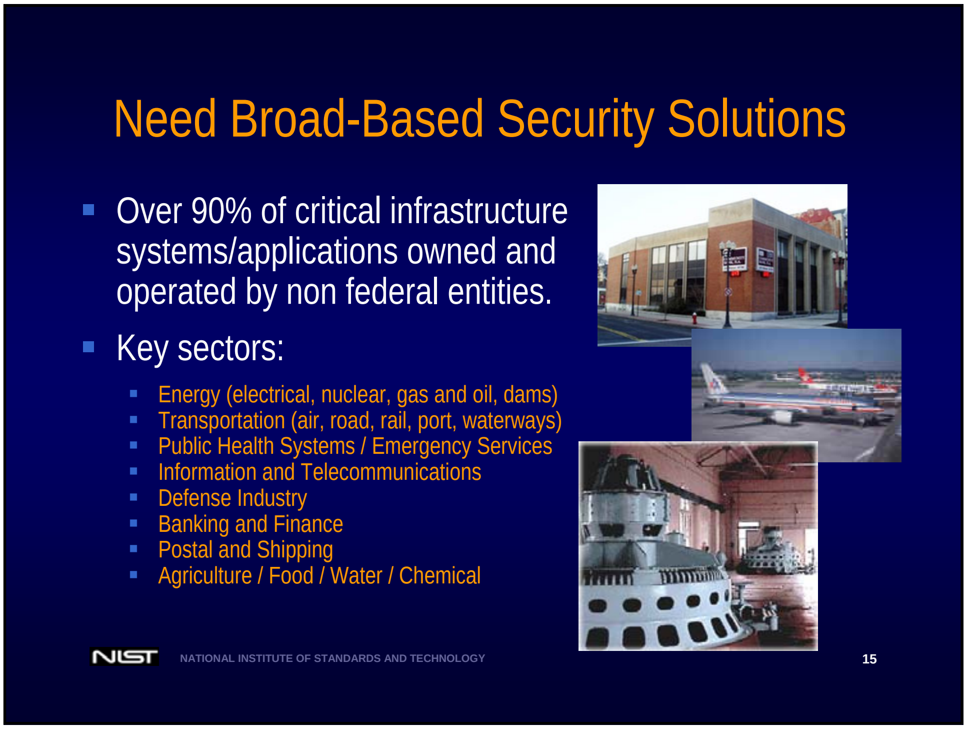
- Confidentiality → Confidentiality, Integrity, Availability
- Information Protection → Information Protection / Sharing
- Static, Point-in-Time Focus → Dynamic, Continuous Monitoring Focus
- Government-Centric Solutions → Commercial Solutions
- Risk Avoidance → Risk Management



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 (manufacturing, services, 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

Enough bad news…

What is the cyber security vision for the future?

The Fundamentals

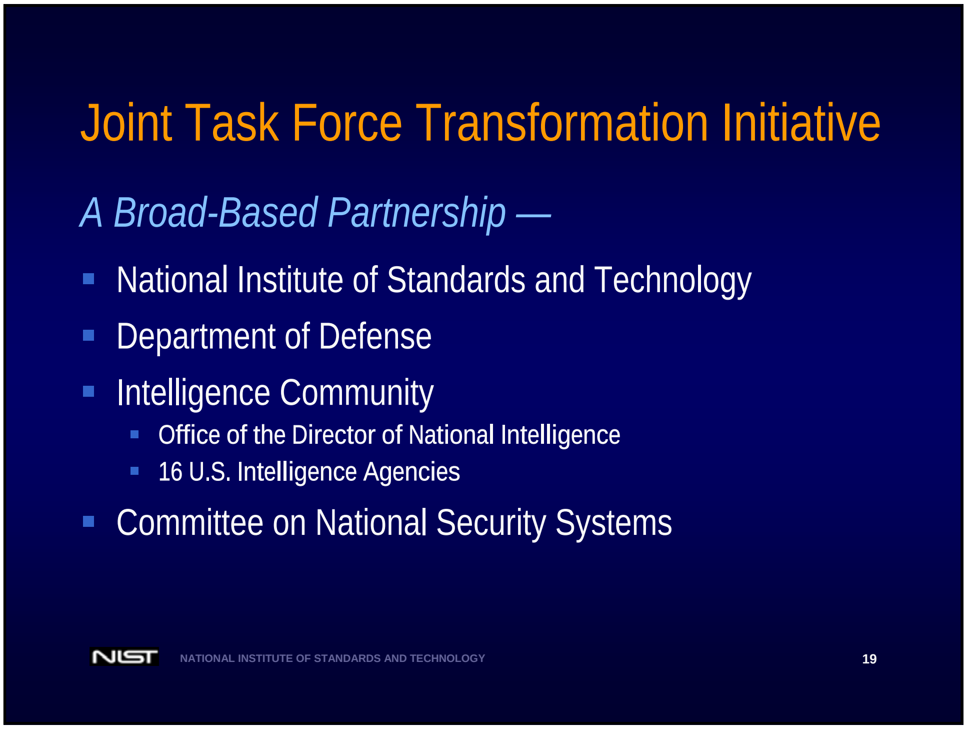
Combating 21st century cyber attacks requires 21st century strategies, tactics, training, and technologies…

- 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 deployment of safeguards and countermeasures.
- More resilient, penetration-resistant information systems.
- Competent, capable cyber warriors.

Federal Government Transformation

An historic government-wide transformation for risk management and information security driven by…

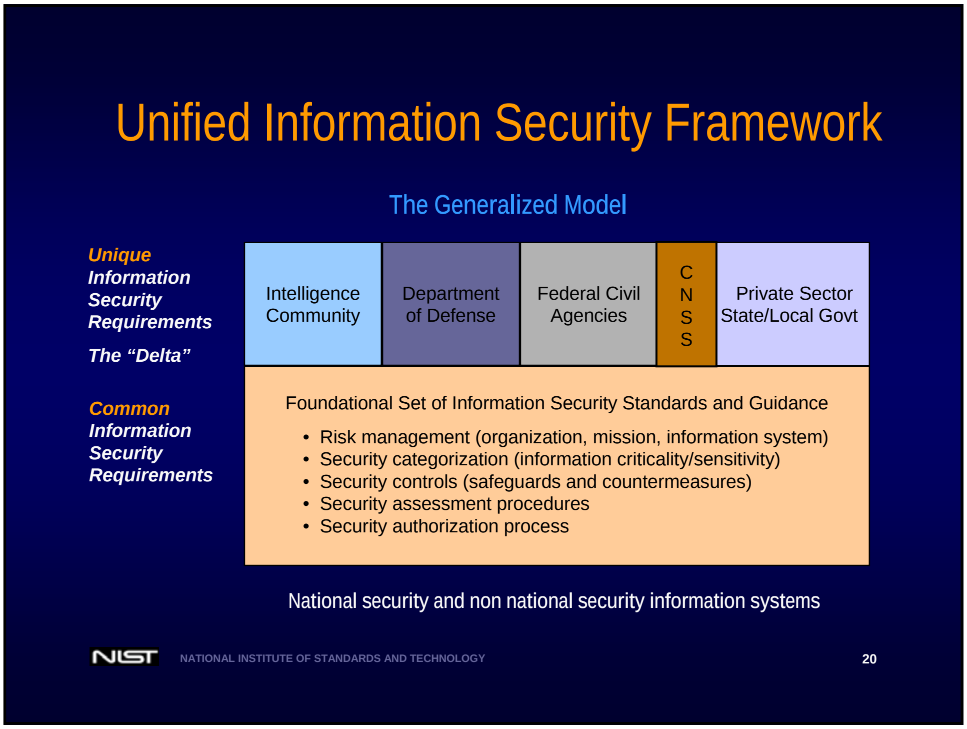
- Increasing sophistication and tempo of cyber attacks.
- Convergence of national and non-national security interests within the federal government.
- Convergence of national security and economic security interests across the Nation.
- Need unified approach in providing effective risk-based cyber defenses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

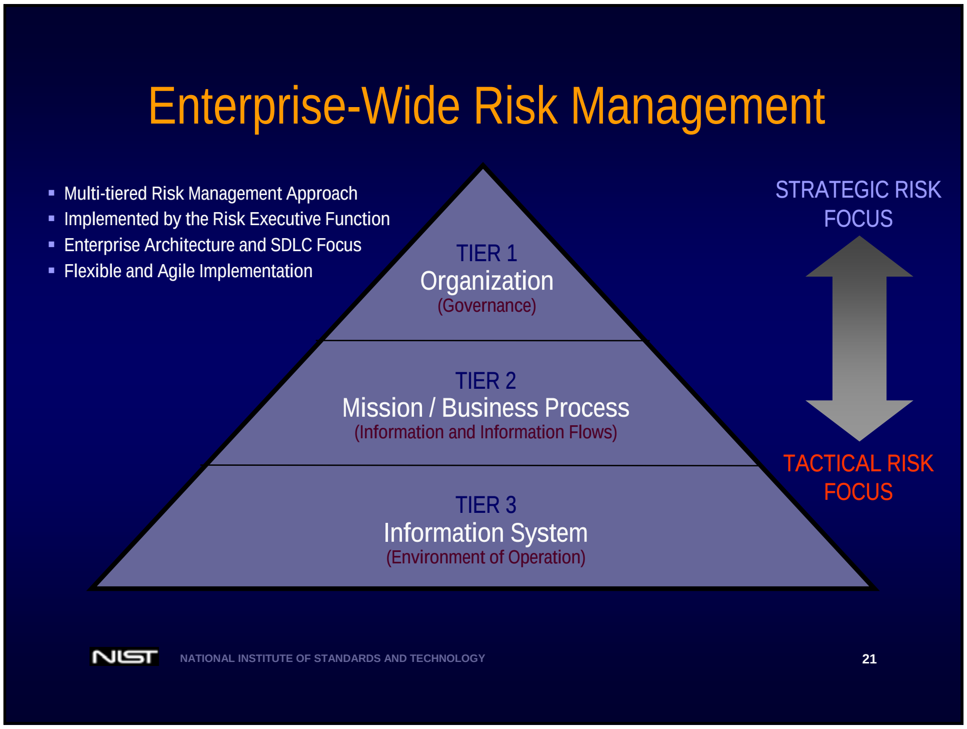
Intelligence Community	Department of Defense	Federal Civil Agencies	C N S S	Private Sector State/Local Govt

***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



Enterprise-Wide Risk Management

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

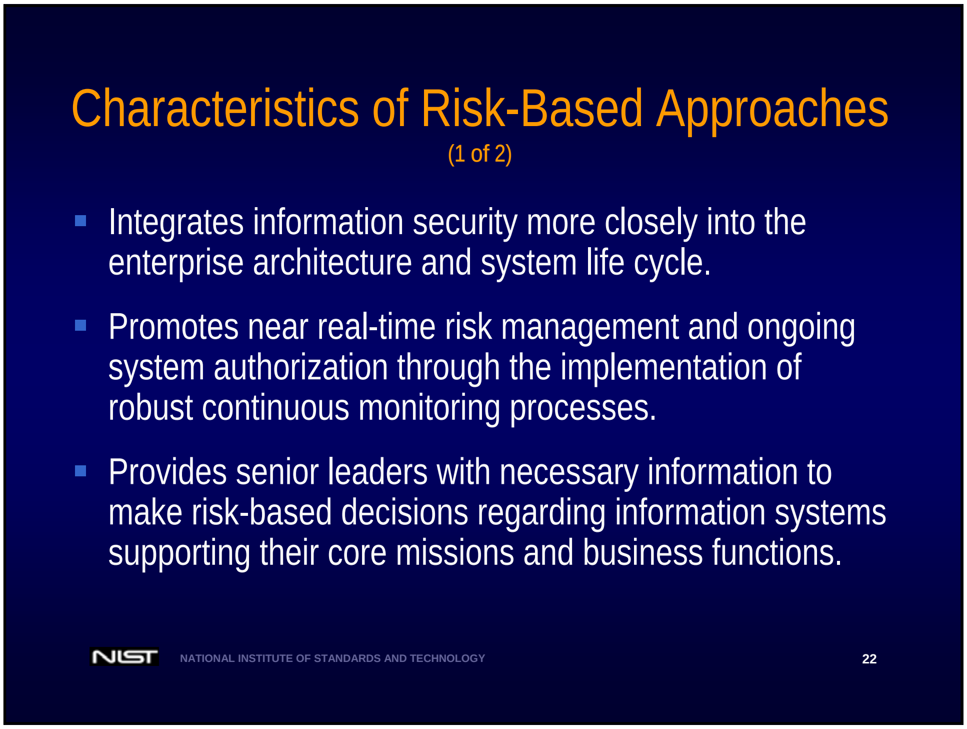
TIER 1
Organization
(Governance)

TIER 2
Mission / Business Process
(Information and Information Flows)

TIER 3
Information System
(Environment of Operation)

STRATEGIC RISK FOCUS

TACTICAL RISK FOCUS



Characteristics of Risk-Based Approaches

(1 of 2)

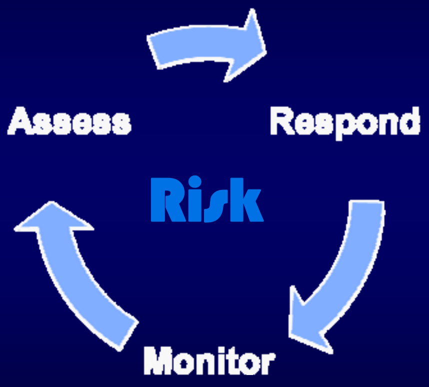
- Integrates information security more closely into the enterprise architecture and system life cycle.
- Promotes near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes.
- Provides senior leaders with necessary information to make risk-based decisions regarding information systems supporting their core missions and business functions.

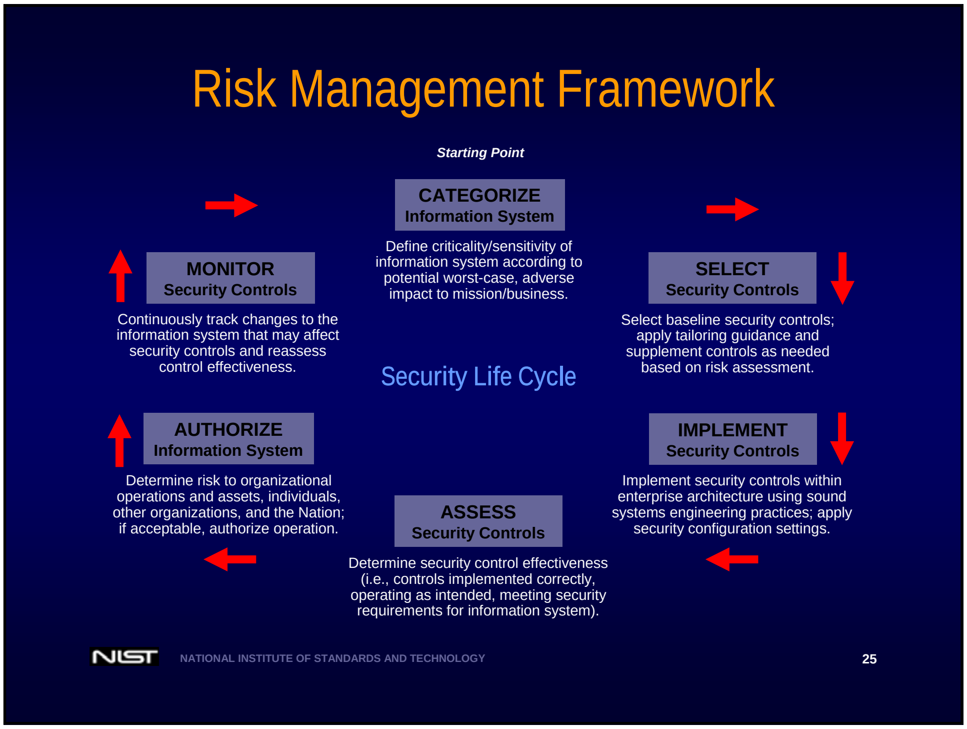
Characteristics of Risk-Based Approaches

(2 of 2)

- 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 information systems.
- Encourages the use of automation to increase consistency, effectiveness, and timeliness of security control implementation.

Risk Management Process





Risk Management Framework

Starting Point

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

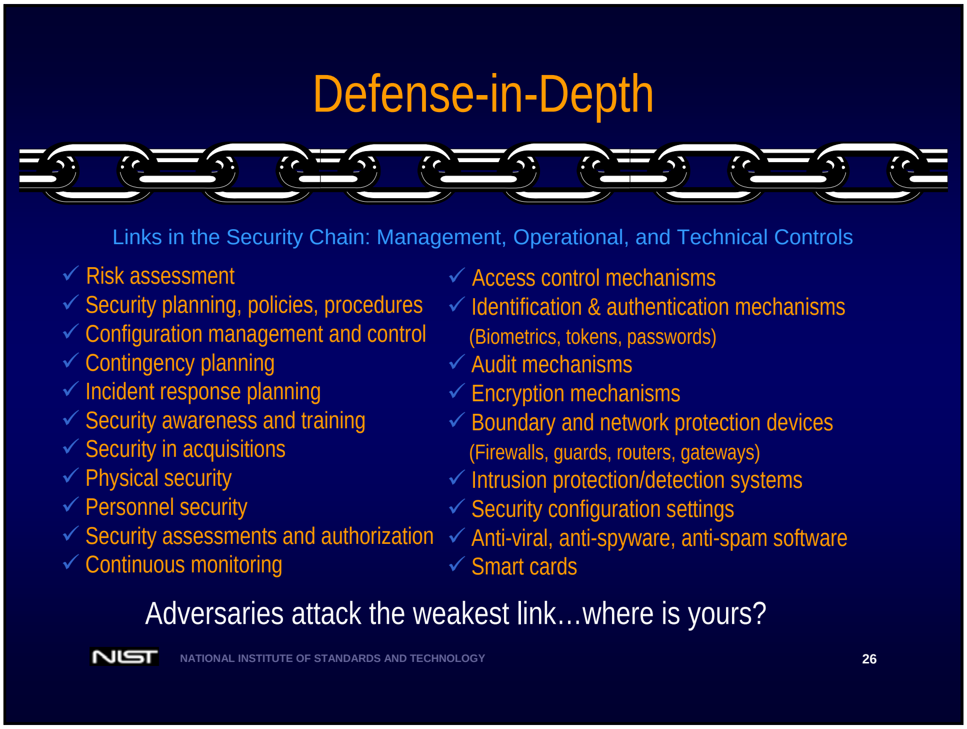
AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

MONITOR
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle



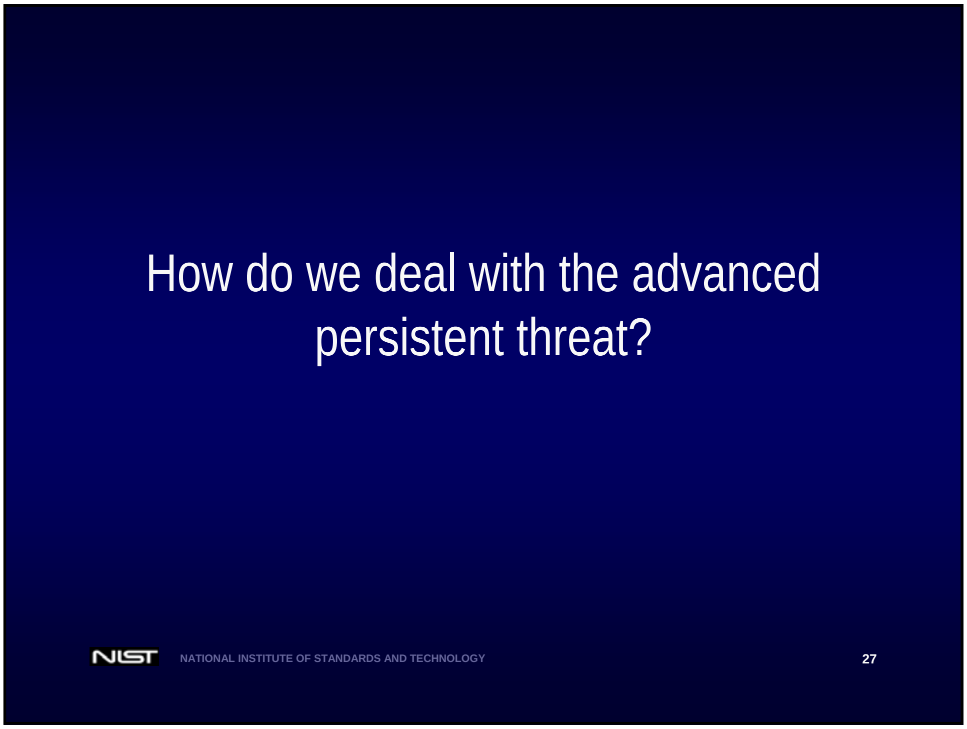
Defense-in-Depth

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

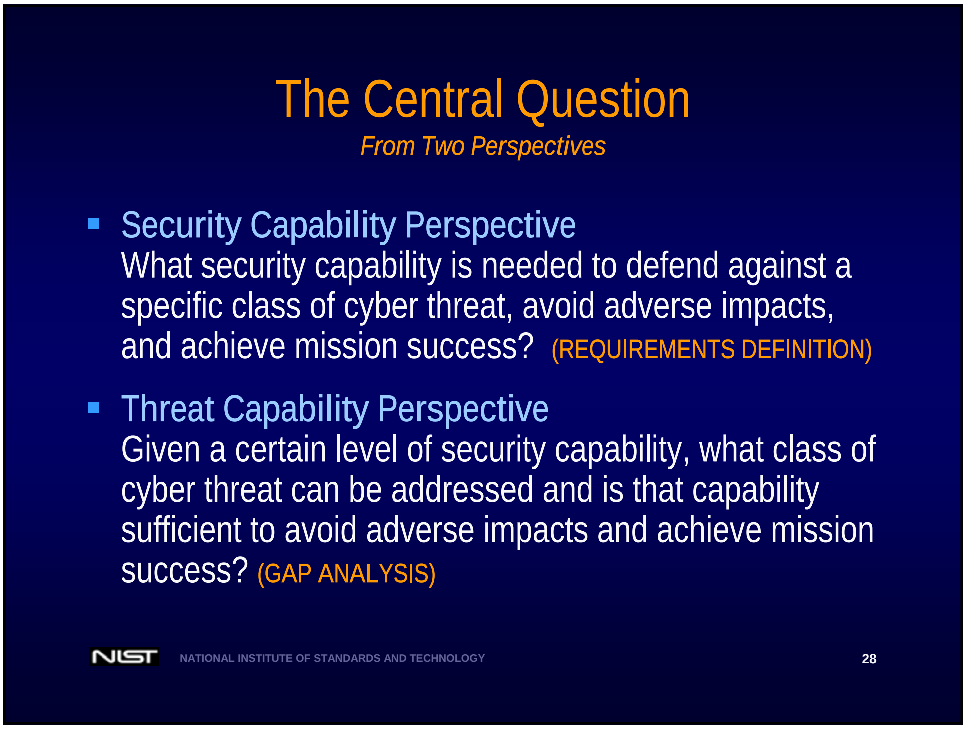
- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments and authorization
- ✓ Continuous monitoring

- ✓ 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?



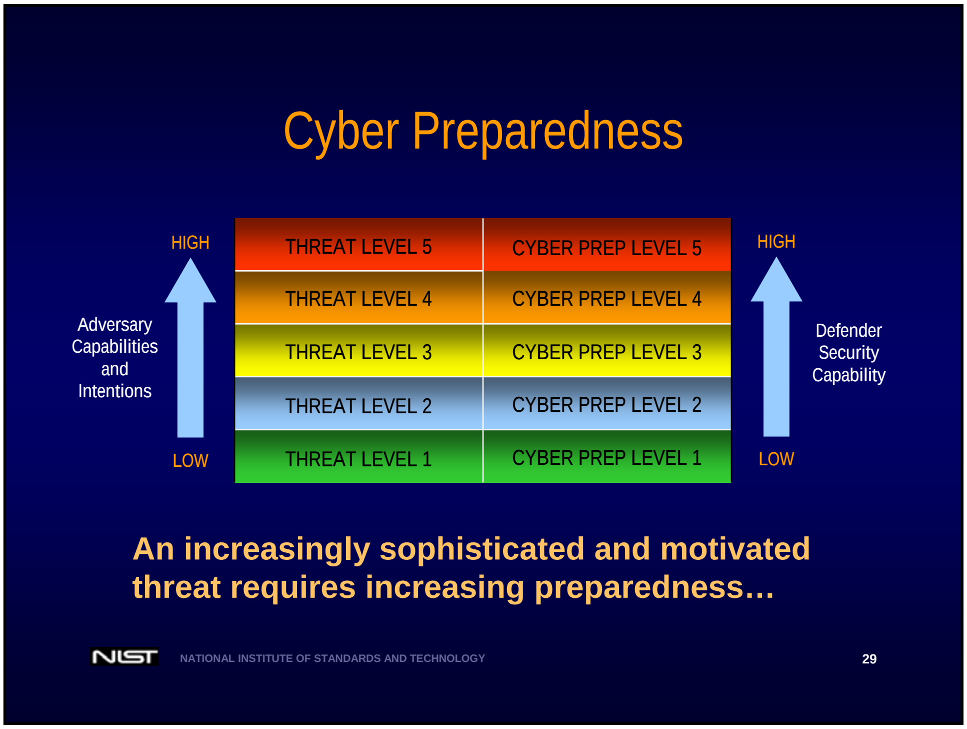
How do we deal with the advanced persistent threat?



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)



Cyber Preparedness

HIGH

Adversary Capabilities and Intentions

LOW

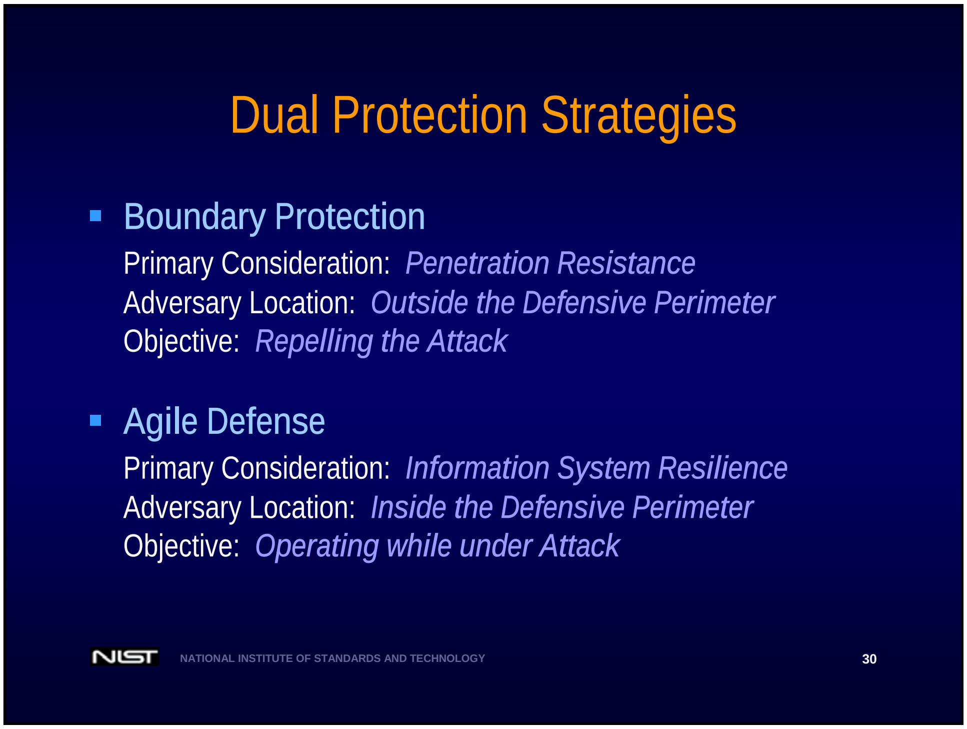
THREAT LEVEL 5	CYBER PREP LEVEL 5
THREAT LEVEL 4	CYBER PREP LEVEL 4
THREAT LEVEL 3	CYBER PREP LEVEL 3
THREAT LEVEL 2	CYBER PREP LEVEL 2
THREAT LEVEL 1	CYBER PREP LEVEL 1

HIGH

Defender Security Capability

LOW

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*

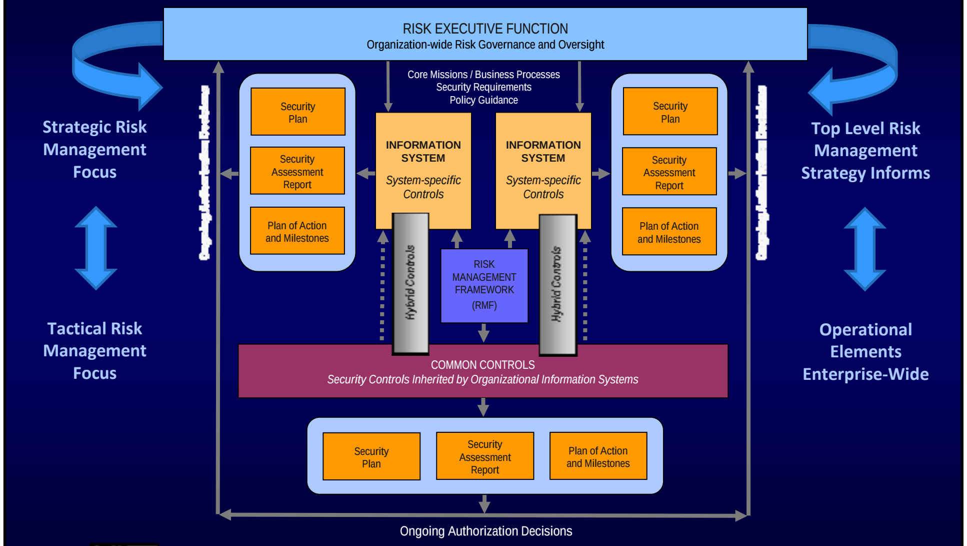
- Agile Defense
  Primary Consideration: *Information System Resilience*
  Adversary Location: *Inside the Defensive Perimeter*
  Objective: *Operating while under Attack*

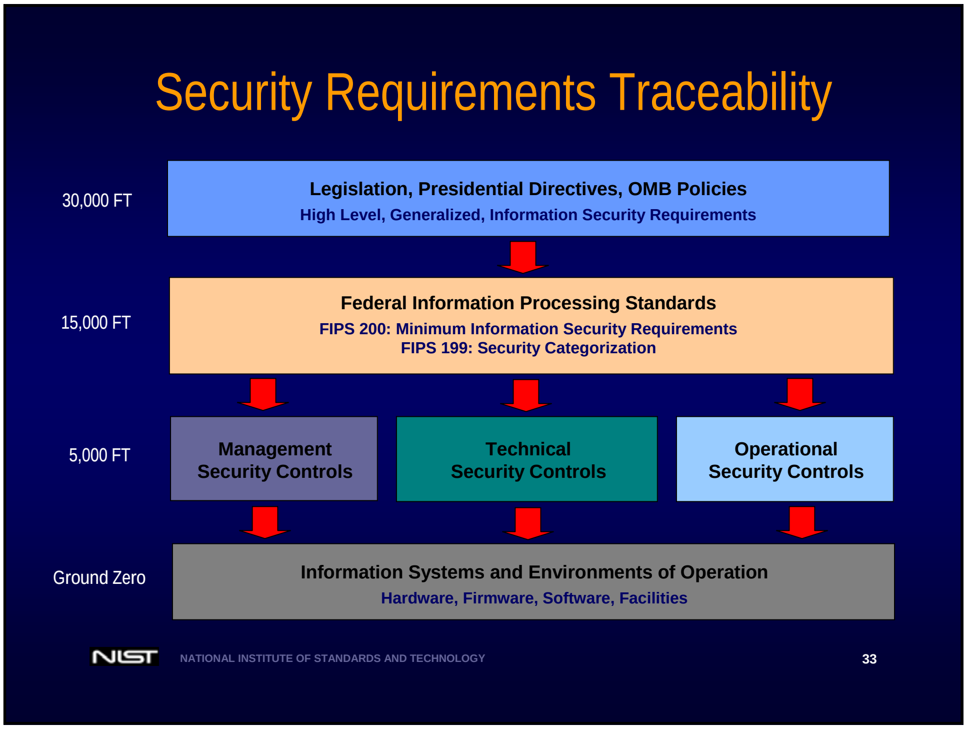
Agile Defense

- 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…

Defense-in-Breadth


RISK EXECUTIVE FUNCTION
Organization-wide Risk Governance and Oversight
Strategic Risk Management Focus
Tactical Risk Management Focus
Top Level Risk Management Strategy Informs
Operational Elements Enterprise-Wide
Core Missions / Business Processes
Security Requirements
Policy Guidance
Security Plan
Security Assessment Report
Plan of Action and Milestones
INFORMATION SYSTEM
System-specific Controls
INFORMATION SYSTEM
System-specific Controls
Security Plan
Security Assessment Report
Plan of Action and Milestones
Hybrid Controls
RISK MANAGEMENT FRAMEWORK (RMF)
Hybrid Controls
COMMON CONTROLS
Security Controls Inherited by Organizational Information Systems
Security Plan
Security Assessment Report
Plan of Action and Milestones
Ongoing Authorization Decisions



Security Requirements Traceability

30,000 FT

Legislation, Presidential Directives, OMB Policies
High Level, Generalized, Information Security Requirements

15,000 FT

Federal Information Processing Standards
FIPS 200: Minimum Information Security Requirements
FIPS 199: Security Categorization

5,000 FT

Management Security Controls

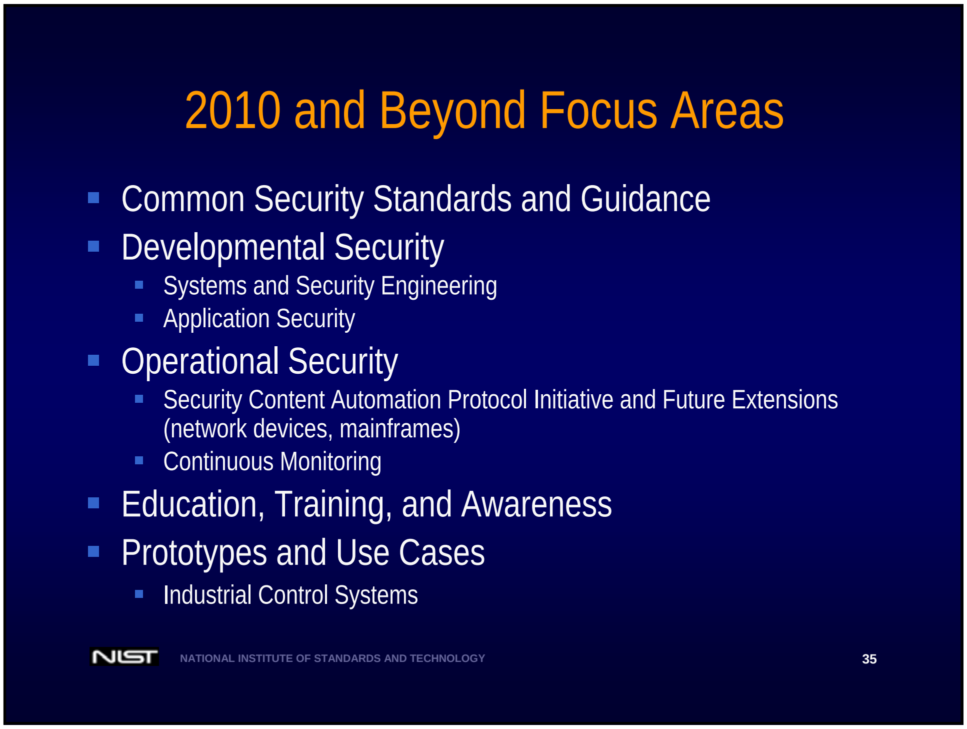
Technical Security Controls

Operational Security Controls

Ground Zero

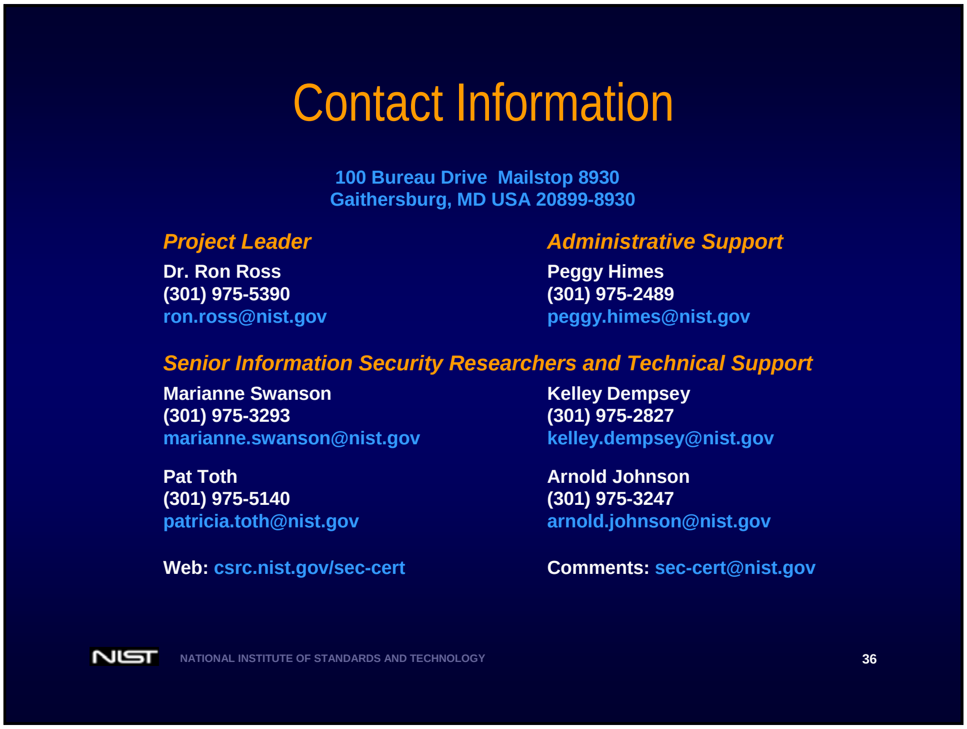
Information Systems and Environments of Operation
Hardware, Firmware, Software, Facilities

What’s in the game plan moving forward?



2010 and Beyond Focus Areas

- Common Security Standards and Guidance
- Developmental Security
  - Systems and Security Engineering
  - Application Security
- Operational Security
  - Security Content Automation Protocol Initiative and Future Extensions (network devices, mainframes)
  - Continuous Monitoring
- Education, Training, and Awareness
- Prototypes and Use Cases
  - Industrial Control Systems



Contact Information

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

Project Leader	***Administrative Support***
Dr. Ron Ross **(301) 975-5390** **ron.ross@nist.gov**	**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**	**Kelley Dempsey** **(301) 975-2827** **kelley.dempsey@nist.gov**
Pat Toth **(301) 975-5140** **patricia.toth@nist.gov**	**Arnold Johnson** **(301) 975-3247** **arnold.johnson@nist.gov**
Web: csrc.nist.gov/sec-cert	**Comments: sec-cert@nist.gov**