FISMA Implementation

The Strategy, Challenges, and Roadmap Ahead

Computer Security Division
Information Technology Laboratory

The Global Threat

- Information security is not just a paperwork drill…there are dangerous adversaries out there capable of launching serious attacks on our information systems that can result in severe or catastrophic damage to the nation’s critical information infrastructure and ultimately threaten our economic and national security…

U.S. Critical Infrastructures

Definition

- "...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)

U.S. Critical Infrastructures

Examples

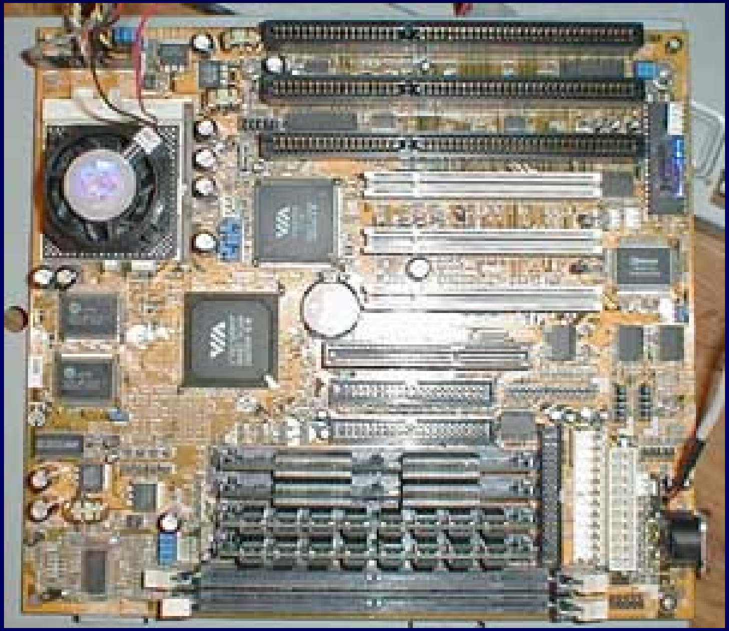
- Energy (electrical, nuclear, gas and oil, dams)
- Transportation (air, road, rail, port, waterways)
- Public Health Systems / Emergency Services
- Information and Telecommunications
- Defense Industry
- Banking and Finance
- Postal and Shipping
- Agriculture / Food / Water
- Chemical

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

Threats to Security

Connectivity



Complexity

Key Security Challenges

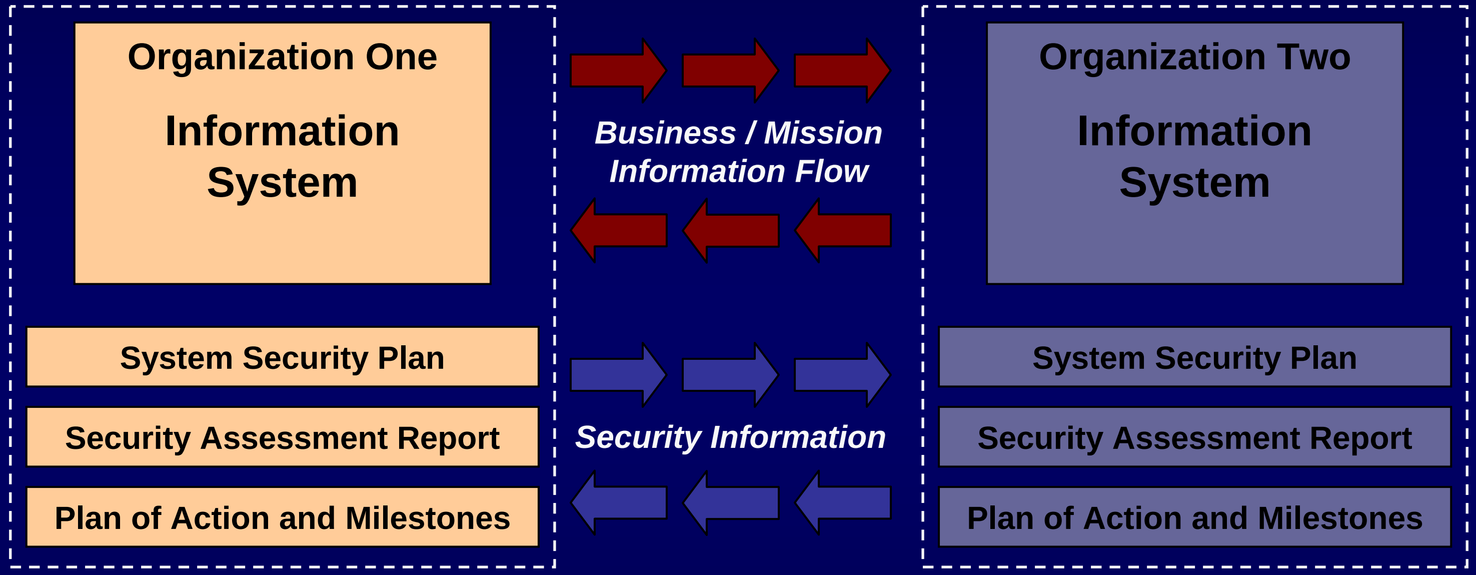
- Adequately protecting enterprise information systems within constrained budgets
- Changing the current culture of:

  "Connect first…ask security questions later"

- Bringing standardization to:
  - ✓ Information system security control selection and specification
  - ✓ Methods and procedures employed to assess the correctness and effectiveness of those controls

The Desired End State

Security Visibility Among Business/Mission Partners



Organization One

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Business / Mission Information Flow

Security Information

Organization Two

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Determining the risk to the first organization's operations and assets and the acceptability of such risk

Determining the risk to the second organization's operations and assets and the acceptability of such risk

The objective is to achieve *visibility* into prospective business/mission partners information security programs BEFORE critical/sensitive communications begin…establishing levels of security due diligence and trust.

Legislative and Policy Drivers

- Public Law 107-347 (Title III)
  Federal Information Security Management Act of 2002
- Homeland Security Presidential Directive #7
  Critical Infrastructure Identification, Prioritization, and Protection
- OMB Circular A-130 (Appendix III)
  Security of Federal Automated Information Resources
- OMB Memorandum M-06-16
  Protection of Sensitive Information

FISMA Legislation

Overview

> “Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…”

-- Federal Information Security Management Act of 2002

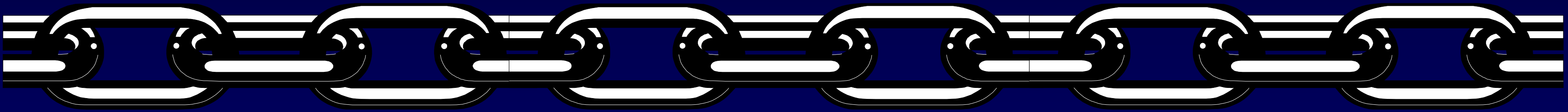
FISMA Vision

- We are building a solid foundation of information security across the largest information technology infrastructure in the world based on comprehensive security standards and technical guidance.
- We are institutionalizing a comprehensive Risk Management Framework that promotes flexible, cost-effective information security programs for federal agencies.
- We are establishing a fundamental level of “security due diligence” for federal agencies and their contractors based on minimum security requirements and security controls.

FISMA Challenges

- Federal agencies are at various levels of maturity with respect to assimilating the new security standards and guidance; an extensive and important investment that will take time to fully implement.
- There is no consistency in the evaluation criteria used by auditors across the federal government when assessing the effectiveness of security controls in federal information systems; thus results vary widely.
- We (collectively) underestimate the complexity and the enormity of the task of building a higher level of security into the federal information technology infrastructure; expectations and measures of success vary.

Information Security Program



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

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Physical security
- ✓ Personnel security
- ✓ Certification, accreditation, and security assessments

- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls and network security mechanisms
- ✓ Intrusion detection systems
- ✓ Security configuration settings
- ✓ Anti-viral software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk resulting from the operation of an information system:
  - ✓ **Categorize** the information system (criticality/sensitivity)
  - ✓ **Select** and tailor minimum (baseline) security controls
  - ✓ **Supplement** the security controls based on risk assessment
  - ✓ **Document** security controls in system security plan
  - ✓ **Implement** the security controls in the information system
  - ✓ **Assess** the security controls for effectiveness
  - ✓ **Determine** agency-level risk and risk acceptability
  - ✓ **Authorize** information system operation
  - ✓ **Monitor** security controls on a continuous basis

NIST Publications

Security Standards and Guidelines

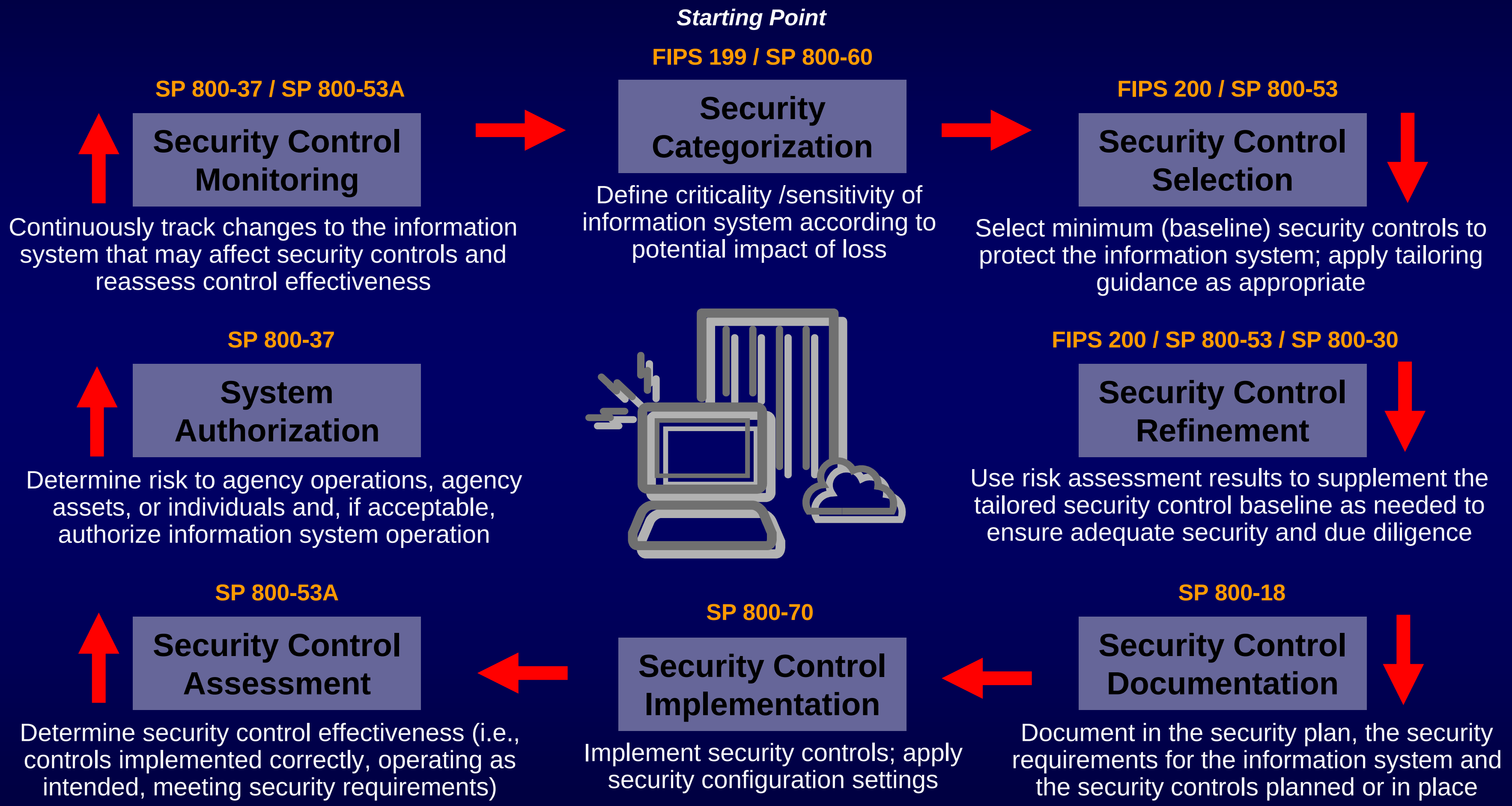
- Federal Information Processing Standards (FIPS)
  - Developed by NIST in accordance with FISMA.
  - Approved by the Secretary of Commerce.
  - Compulsory and binding for federal agencies; not waiverable.
- NIST Guidance (Special Publication 800-Series)
  - OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* states that for other than national security programs and systems, agencies must follow NIST guidance.
- Other security-related publications
  - NIST Interagency and Internal Reports and Information Technology Laboratory Bulletins provide technical information about NIST's activities.
  - Mandatory only when so specified by OMB.

Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (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)

Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation…

The Risk Framework



Starting Point

FIPS 199 / SP 800-60

Security Categorization

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

FIPS 200 / SP 800-53 / SP 800-30

Security Control Refinement

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

Security Control Documentation

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

Security Control Implementation

Implement security controls; apply security configuration settings

SP 800-53A

Security Control Assessment

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

SP 800-37

System Authorization

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37 / SP 800-53A

Security Control Monitoring

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

Security Categorization

Example: An Enterprise Information System

Mapping Information Types to FIPS 199 Security Categories

SP 800-60

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

Security Categorization

Example: An Enterprise Information System

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

FIPS 200

Minimum Security Controls for Moderate Impact Systems

SP 800-53

Minimum Security Requirements

FISMA Requirement

- Develop minimum information security requirements for information and information systems in each security category defined in FIPS 199
- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 200, “Minimum Security Requirements for Federal Information and Information Systems”
  - ✓ Final Publication: March 2006

Minimum Security Controls

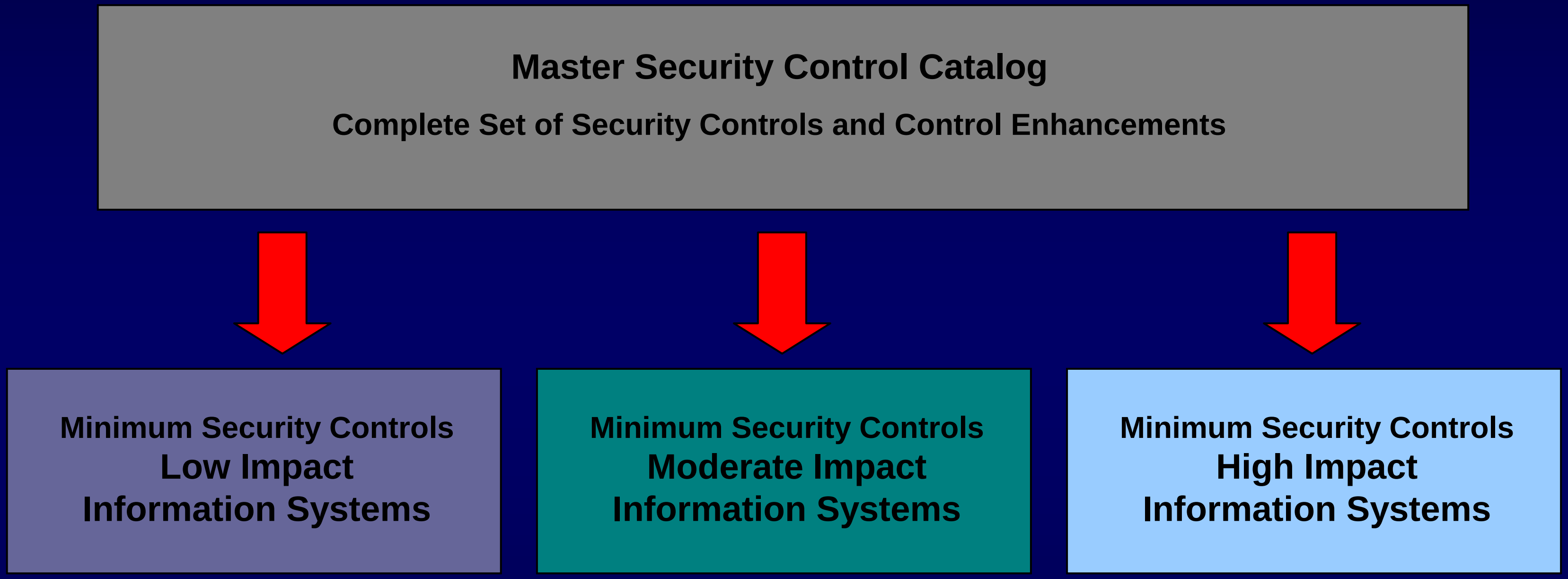
- Develop minimum security controls (management, operational, and technical) to meet the minimum security requirements in FIPS 200
- Publication status:
  - ✓ NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems"
  - ✓ Final Publication: February 2005*

* SP 800-53, Revision 1(Second public draft) to be published in July 2006.

Minimum Security Controls

- Minimum security controls, or baseline controls, defined for low-impact, moderate-impact, and high-impact information systems—
  - Provide a ***starting point*** for organizations in their security control selection process
  - Are used in conjunction with ***tailoring guidance*** that allows the baseline controls to be adjusted for specific operational environments
  - Support the organization's ***risk management process***

Security Control Baselines



Master Security Control Catalog

Complete Set of Security Controls and Control Enhancements

Minimum Security Controls
Low Impact
Information Systems

Minimum Security Controls
Moderate Impact
Information Systems

Minimum Security Controls
High Impact
Information Systems

Baseline #1

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls

Baseline #2

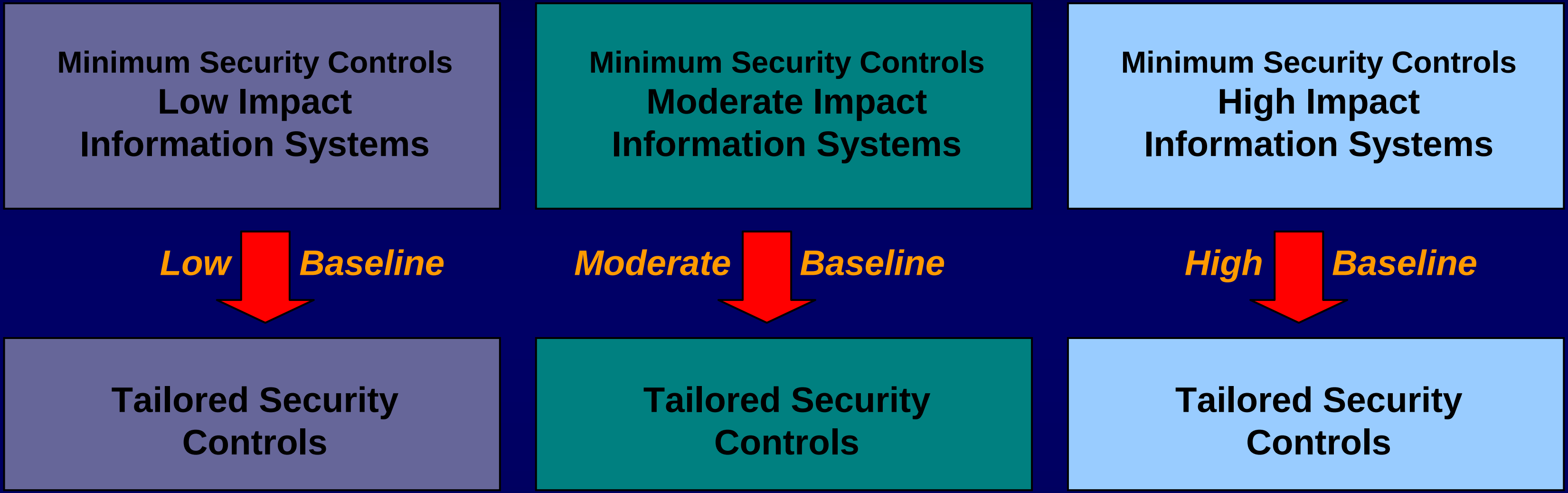
Builds on low baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Baseline #3

Builds on moderate baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



Minimum Security Controls
Low Impact
Information Systems

Low *Baseline*

Tailored Security Controls

Minimum Security Controls
Moderate Impact
Information Systems

Moderate *Baseline*

Tailored Security Controls

Minimum Security Controls
High Impact
Information Systems

High *Baseline*

Tailored Security Controls

Enterprise #1

Operational Environment #1

Enterprise #2

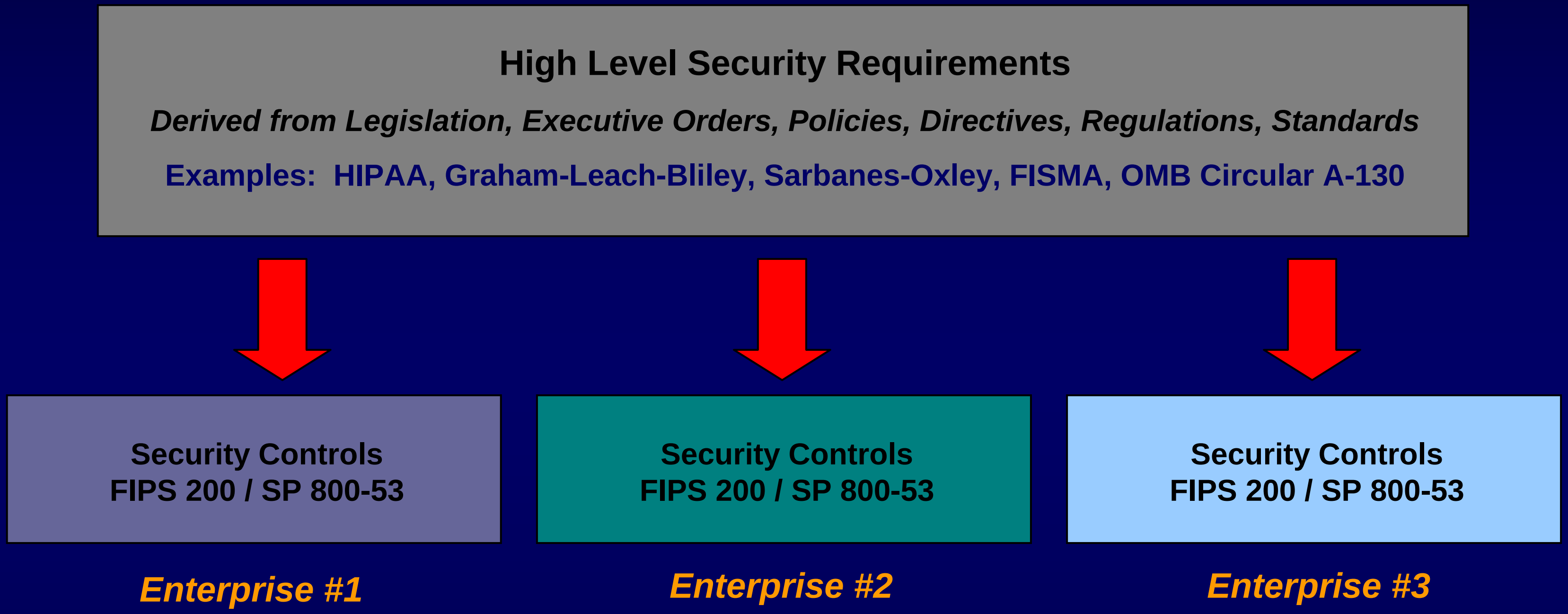
Operational Environment #2

Enterprise #3

Operational Environment #3

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

Requirements Traceability



High Level Security Requirements

Derived from Legislation, Executive Orders, Policies, Directives, Regulations, Standards

Examples: HIPAA, Graham-Leach-Bliley, Sarbanes-Oxley, FISMA, OMB Circular A-130

Security Controls
FIPS 200 / SP 800-53

Enterprise #1

Security Controls
FIPS 200 / SP 800-53

Enterprise #2

Security Controls
FIPS 200 / SP 800-53

Enterprise #3

What set of security controls, if implemented within an information system and determined to be effective, can show compliance to a particular set of security requirements?

Compliance Schedule

NIST Security Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.*
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

* The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Compliance

NIST Standards and Guidelines

- While agencies are required to follow NIST ***guidance*** in accordance with OMB policy, there is flexibility in how agencies apply the guidance.
- Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some ***latitude*** in their application.
- Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of ***adequate security*** for federal information systems.

Compliance

NIST 800-Series Guidelines

- When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider:
  - The intent of the security concepts and principles articulated within the particular guidance document; and
  - How the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

FISMA Implementation Tips

Key strategies for successful implementation—

- Conduct FIPS 199 ***impact analyses*** as a corporate-wide exercise with the participation of key officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Officials, System Owners).

Rationale: The agency is heavily dependent upon its information systems and information technology infrastructure to successfully conduct critical missions. Therefore, the protection of those critical missions is of the highest priority. An incorrect information system impact analysis (i.e., incorrect FIPS 199 security categorization) results in the agency either over protecting the information system and wasting valuable security resources or under protecting the information system and placing important operations and assets at risk.

FISMA Implementation Tips

Key strategies for successful implementation—

- For each security control baseline (low, moderate, or high) identified in NIST Special Publication 800-53, apply the ***tailoring guidance*** to modify the set of controls to meet the specific operational requirements of the agency.

Rationale: Application of the tailoring guidance in Special Publication 800-53 can eliminate unnecessary security controls, incorporate compensating controls when needed, and specify agency-specific parameters. Tailoring activities and associated tailoring decisions should be well documented with appropriate justification and rationale capable of providing reasoned arguments to auditors. The tailored security control baseline is supplemented with additional security controls and/or control enhancements based on the results of an organizational assessment of risk.

FISMA Implementation Tips

Key strategies for successful implementation—

- Conduct the selection of ***common security controls*** (i.e., agency infrastructure-related controls or controls for common hardware/software platforms) as a corporate-wide exercise with the participation of key officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Officials, System Owners).

Rationale: The careful selection of common security controls can save the agency significant resources and facilitate a more consistent application of security controls enterprise-wide. Agency officials must assign responsibility for the development, implementation, and assessment of the common controls and ensure that the resulting information is available to all interested parties.

New Initiatives

- Applying FISMA security standards and guidance to Industrial Control/SCADA Systems—
    - Completed two-day workshop at NIST involving major federal entities with Industrial Control/SCADA systems or having significant interest in those types of systems (e.g., Bonneville Power Administration, Tennessee Valley Authority, Western Area Power Administration, Federal Energy Regulatory Commission, Department of Interior Bureau of Land Management)
    - Analyzed the impact of applying the security controls in NIST SP 800-53 to Industrial Control/SCADA Systems; soliciting recommendations for additional security controls and/or developing control interpretations.

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 case 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
- Be a good consumer—beware of vendors trying to sell "single point solutions" for enterprise security problems

The Golden Rules

Building an Effective Enterprise Information Security Program

- 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

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