

# SP 800-53 Security Controls Tailoring to System Environments

4th Annual Security Automation Conference

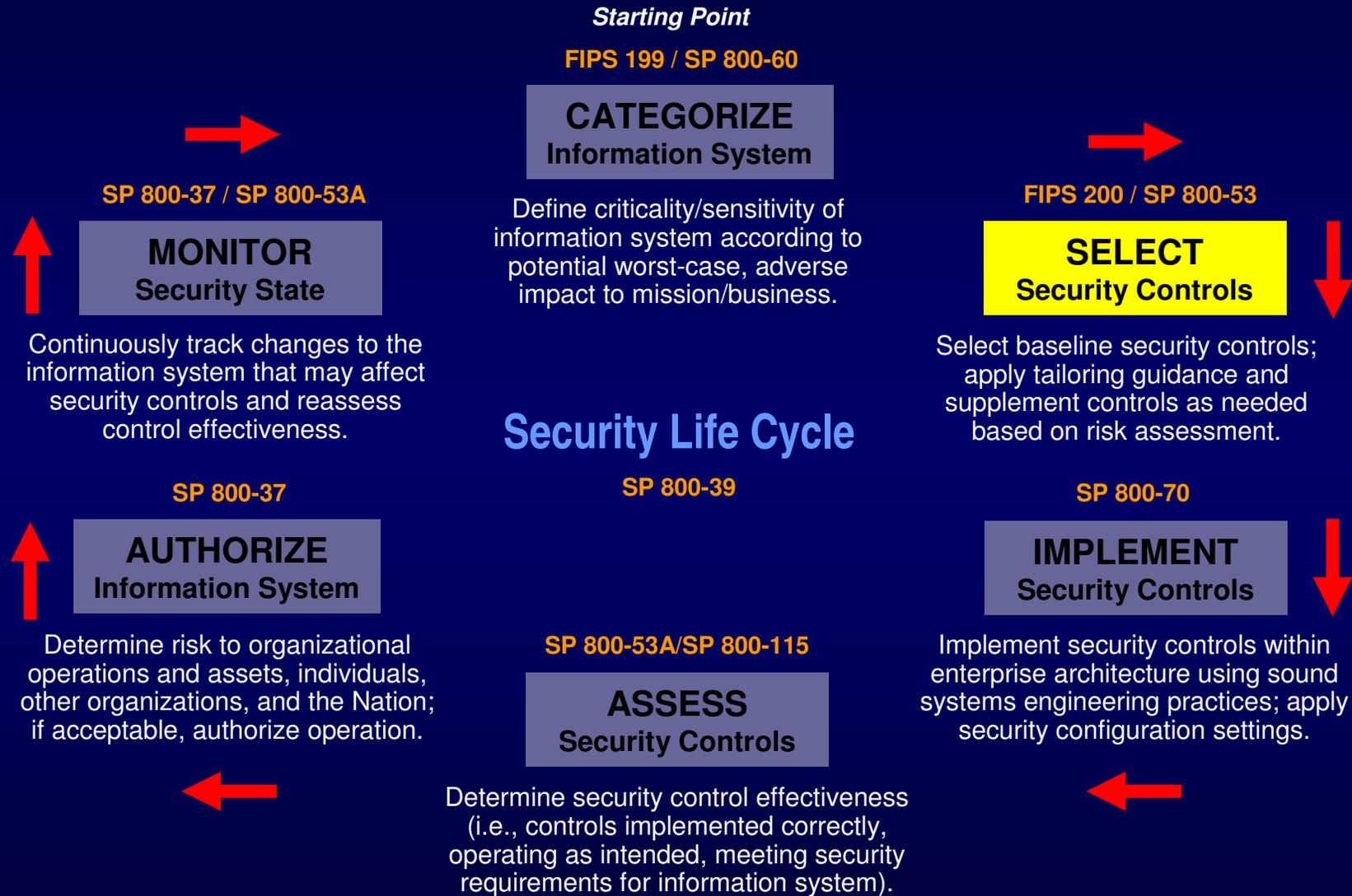
September 24, 2008

Arnold Johnson  
Computer Security Division  
Information Technology Laboratory

# Security Controls

- The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
- Selecting and Tailoring in terms of the Risk Management Framework.

# Risk Management Framework



# Special Publication 800-53

The purpose of SP 800-53 is to provide—

- Guidance on how to use a FIPS Publication 199 security categorization to identify minimum security controls (baseline) for an information system.
- A master catalog of security controls for information systems requiring additional threat and risk considerations.

# SP 800-53 Fundamentals

- Catalog of security controls
- Security control structure
  - Classes:
    - Management
    - Operational
    - Technical
  - Families (17):
    - Access Control
    - Awareness and Training
    - .....

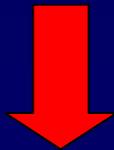
# SP 800-53 Process

- Categorize information system based on FIPS 199 and SP 800-60:
  - Low Impact;
  - Moderate Impact; or
  - High Impact.
- Selecting initial security control baseline (starting point).
- Tailoring (Scope and Compensate) initial security control baseline.
- Supplement tailored baseline.

# Selecting Minimum Security Controls Sets

*Baselines Provided by Special Publication 800-53*

Master Security Control Catalog  
Complete Set of Security Controls and Control Enhancements



Minimum Security Controls  
Low Impact  
Information Systems

## *Baseline #1*

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



Minimum Security Controls  
Moderate Impact  
Information Systems

## *Baseline #2*

Selection of a subset of security controls from the master catalog—consisting of **basic** level controls, plus additional controls and control **enhancements**, as needed



Minimum Security Controls  
High Impact  
Information Systems

## *Baseline #3*

Selection of a subset of security controls from the master catalog—consisting of **basic** level controls, plus additional controls and control **enhancements**, as needed

# Tailoring

## (Scoping and Supplementing)

- 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 capable of providing reasoned arguments to auditors.

# Scoping Guidance

- **Physical Infrastructure-related considerations**

Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system.

- **Public access-related considerations**

Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces.

# Scoping Guidance II

- Technology-related considerations
  - Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.
  - Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.
  - Security controls that can be either explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products.

# Scoping Guidance II

- Policy/regulatory-related considerations

Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

# Scoping Guidance III

- Scalability-related considerations

Security controls are scalable with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected.

- Security objective-related considerations

Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization before moving to the high water mark; (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.

# Compensating Security Controls

- A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system.
- Mission-driven considerations may require alternate solutions (e.g., AC-11 session lock not advisable in certain systems).

# Compensating Security Controls

- The organization selects a compensating control from NIST SP 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;
- The organization provides a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

# Supplement

- For each tailored security control baseline, **supplement** the security controls with additional controls and/or control enhancements based on the results of an organizational assessment of risk.

Rationale: The tailored baseline represents the starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations.

# Results In

Set of security controls for the information system that is deemed to provide adequate protection for the particular organization and information system environment.