NIST
Information Technology Laboratory (ITL)
The Cyber Maryland Showcase

NIST
National Institute of
Standards and Technology

The Federal Information Security Management Act of 2002

FISMA 2002, Summary of NIST Responsibilities

- Information Security Standards that-
  - Provide minimum information security requirements
  - Are otherwise necessary to improve the security of federal information and information systems

  - NIST has the mission of developing standards, guidelines and associated methods and techniques for information systems:
    - Standards to be used by all agencies to categorize all information and information systems....according to a range of risk levels
    - Guidelines recommending the types of information and information systems to be included in each category
    - Minimum information security requirements for information and information systems in each such category
    - Provide technical assistance to agencies, upon request
    - Conduct research, as needed
    - Assist the private sector, upon request

Show Me Your FIMSA?

Has the Government COR/COTR/CO/PM Ever Asked you:

- How is your FISMA?
- Do you Do FISMA?
- We need you to do FISMA.

What are They Talking About and How Do You Answer?

NIST Standards and Guidelines

- Consistent and Know Method to Express Security Requirements to Industry Partners.
- Ability to Understand Expectations of Government.
- Negotiated Discussion for Implementation Specifics.
- RESPONSBILITY CAN NEVER BE OUTSOURCED.

NIST Standards and Guidelines

- Standards for the US Federal Government
  - Required for “other than national security systems”
- Guidelines for Security Program Implementation Assistance

Both Used By Organizations at All Levels Across the Country and the World.

Risk-Based Protection

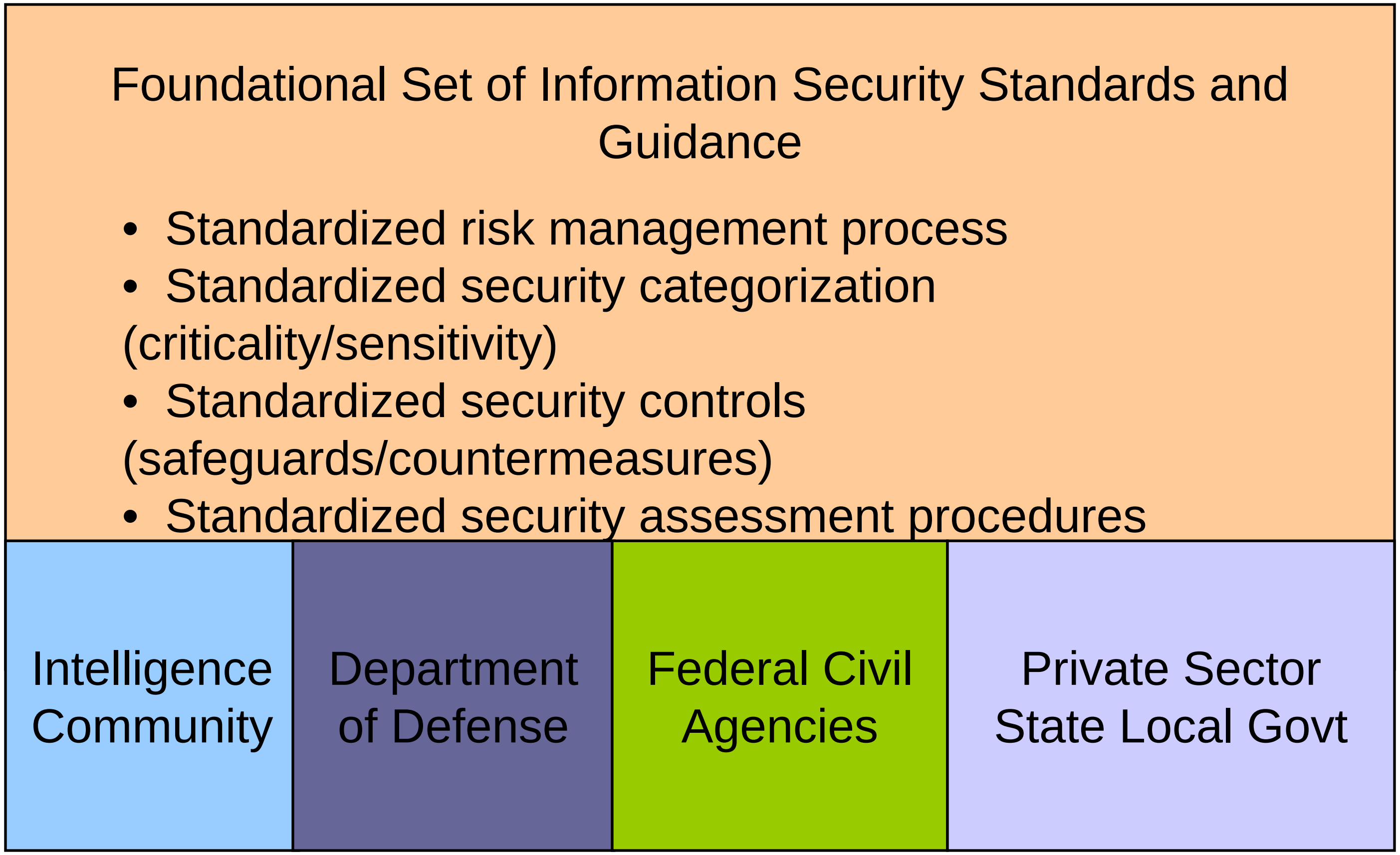
- ***Enterprise missions and business processes drive security*** requirements and associated safeguards and countermeasures for organizational information systems.
- ***Highly flexible implementation; recognizing diversity*** in missions/business processes and operational environments.
- ***Senior leaders take ownership*** of their security plans including the safeguards/countermeasures for the information systems.
- Senior leaders are both ***responsible and accountable*** for their information security decisions; understanding, acknowledging, and explicitly accepting resulting mission/business risk.

NIST Method
Open, Transparent, Inclusive

- Standards and Guidelines
  - Developed in an Open and Transparent Manner
  - Includes Public and Government Participation
  - Involves Best Practices and Open Exchange of Ideas
  - Results in Products Better Then The Sum of the Authors

Strategic Partnerships

For Information Security



Common Information Security Requirements

Foundational Set of Information Security Standards and Guidance

- Standardized risk management process
- Standardized security categorization (criticality/sensitivity)
- Standardized security controls (safeguards/countermeasures)
- Standardized security assessment procedures

Unique Information Security Requirements

The "Delta"

Intelligence Community

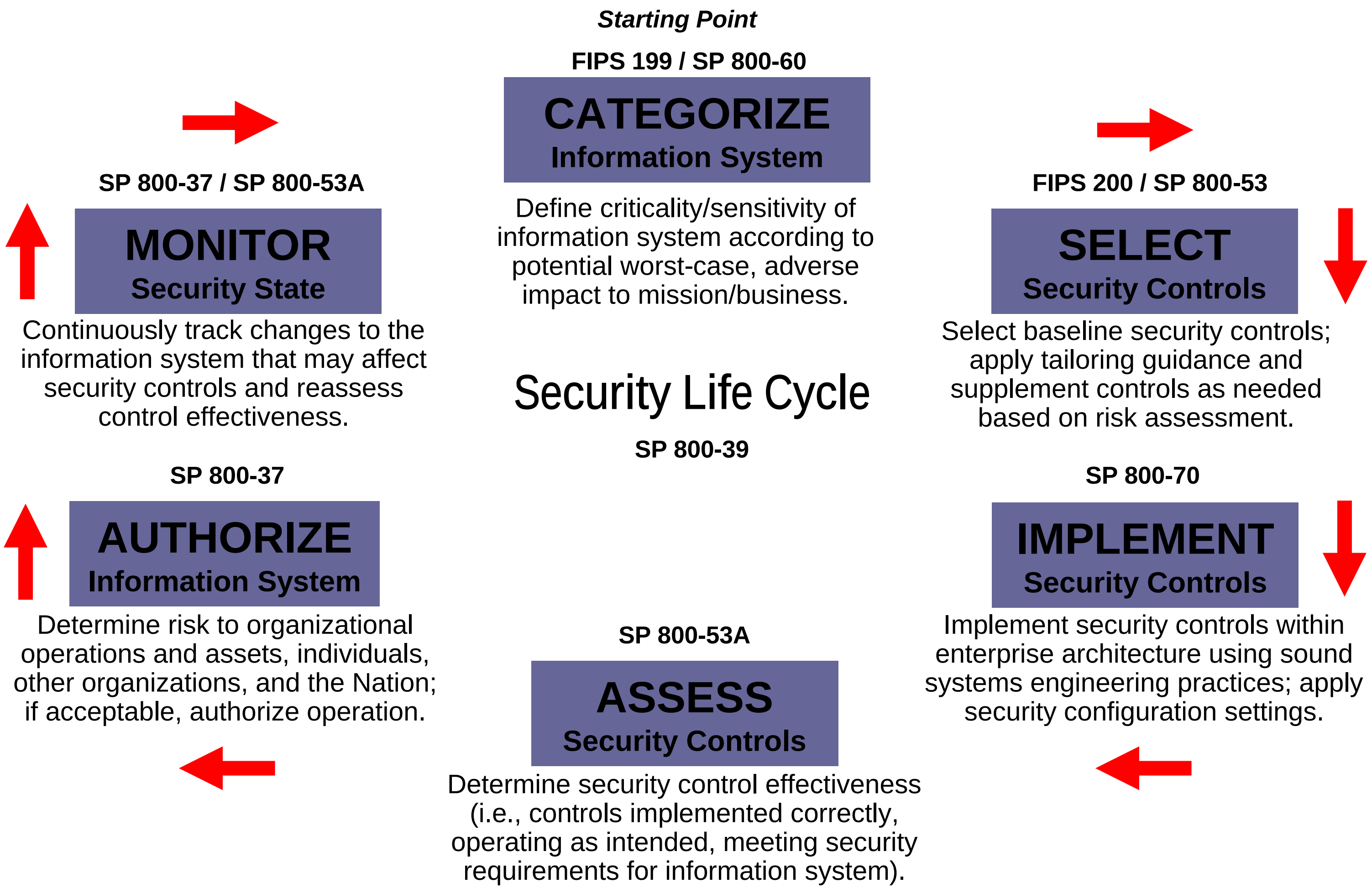
Department of Defense

Federal Civil Agencies

Private Sector State Local Govt

National security and non national security information systems

Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

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

FIPS 200 / SP 800-53

SELECT
Security Controls

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

SP 800-70

IMPLEMENT
Security Controls

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

SP 800-53A

ASSESS
Security Controls

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

SP 800-37

AUTHORIZE
Information System

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

SP 800-37 / SP 800-53A

MONITOR
Security State

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

Security Life Cycle

SP 800-39

Some of What We Face (example listing)

Threats

- Social engineering and phishing
- Web browsing attacks (compromised commercial websites)
- SQL injection methods against vulnerable websites
- Increasingly sophisticated BotNets
- Stolen credentials and certificates
- Pharming (website redirection)
- DNS Attacks
- Distributed Denial of Service (DDoS)
- Supply chain insertion
- Man in the Middle Attacks
- BIOS Root kits

Motivations

- Data Theft
- Blackmail
- Denial of Service
- Command and Control Disruption
- Espionage
- Fraud
- Terrorism
- Revenge
- Accidental
- Nature Events

What is your weakest link?

Constant Tension of Threat and Defend

“for every action there is an opposite reaction”

The Threat Actors are:

Volatile, Uncertain, Complex, Ambiguous

The Threats are:

Sophisticated, Agile, Tenacious, Impactful

Needs for Continuous Risk Management,

Agile Defenses,

Operations Under Compromise,

Rapid Response and Restore Capability,

Outreach to Federal Agencies

- Federal Computer Security Managers Forum
- Federal Information Security Educators Association
- Federal Agency Security Practices
- Information Security and Privacy Advisory Board
- Multiple Workshops, Conferences, Events
- Multiple Individual Agency Assistance

Standards and Guidelines Adoption by States

- State of Maryland
- State of California
- State of Missouri
- State of Georgia
- State of Florida
- State of Texas
- State of Alabama
- State of Arizona

“The Georgia Technology Authority (GTA) wishes to acknowledge the National Institute for Standards and Technology (NIST) publication, NISTIR 7359, and the NIST website as the source for much of the information contained in this document. GTA choose to model Georgia’s information risk management program after the federal program developed by NIST and overseen by the President’s Office of Management and Budget. As you read this document, you will gain an understanding of the benefits provided by this model.”

Outreach to the Private Sector

- Small-Medium Business Security Outreach
  - Joint Program with FBI/SBA
- Work with Major COTS Vendors
- Open Workshops/Public Participation
- Standards Development Organizations
  - IEEE, ANSI, ISO, IETF, CNSS

NIST

Matthew Scholl
Computer Security Division
Information Technology Laboratory
mscholl@nist.gov
301-975-2941

National Institute of Standards and Technology