ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Session Number G13 – Risk Management and NIST Reference Materials

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

- OBJECTIVE OF THIS BRIEFING – INFORMATION
  - A quick and short look at how NIST approaches Information Risk Management
  - Provide an opportunity to ask questions
  - Exploit an opportunity to hear for external stakeholders

What is NIST?

- The National Institute of Standards and Technology
  - Operational Unit of the Department of Commerce
  - Former National Bureau of Standards est. 1901
  - Nations First Physical Science Research Lab

NIST's mission:
To promote U.S. innovation and industrial competitiveness by advancing measurement science,
standards, and technology in ways that enhance economic security and improve our quality of life.

Why Does NIST Do IT Security?

- NIST ACT
- Cybersecurity R&D ACT
- Federal Information Security Management Act
- HSPD 7
- HSPD 12

ITL/CSD Other Core Areas

- Cryptography
- Identity
- Security Automation
- Access Control
- Cloud Computing Security
- Cybersecurity Research
- Risk Management – Our Talk Today

Mission Need for IT – Mission Exposure of IT

- 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 Threats We Face

- *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.

How Do We Think About Security?

- **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***

How Do We Think About Security?

- Cyber Economics
- Building Security In
- The Moving Target
- Trusted Tailored Spaces
- C-I-A Still the Triad?

NIST Work With Other Agencies

- *A Broad-Based Partnership —*
- National Institute of Standards and Technology
- Department of Defense
- Intelligence Community
  - **Office of the Director of National Intelligence**
  - **17 U.S. Intelligence Agencies**
- Committee on National Security Systems

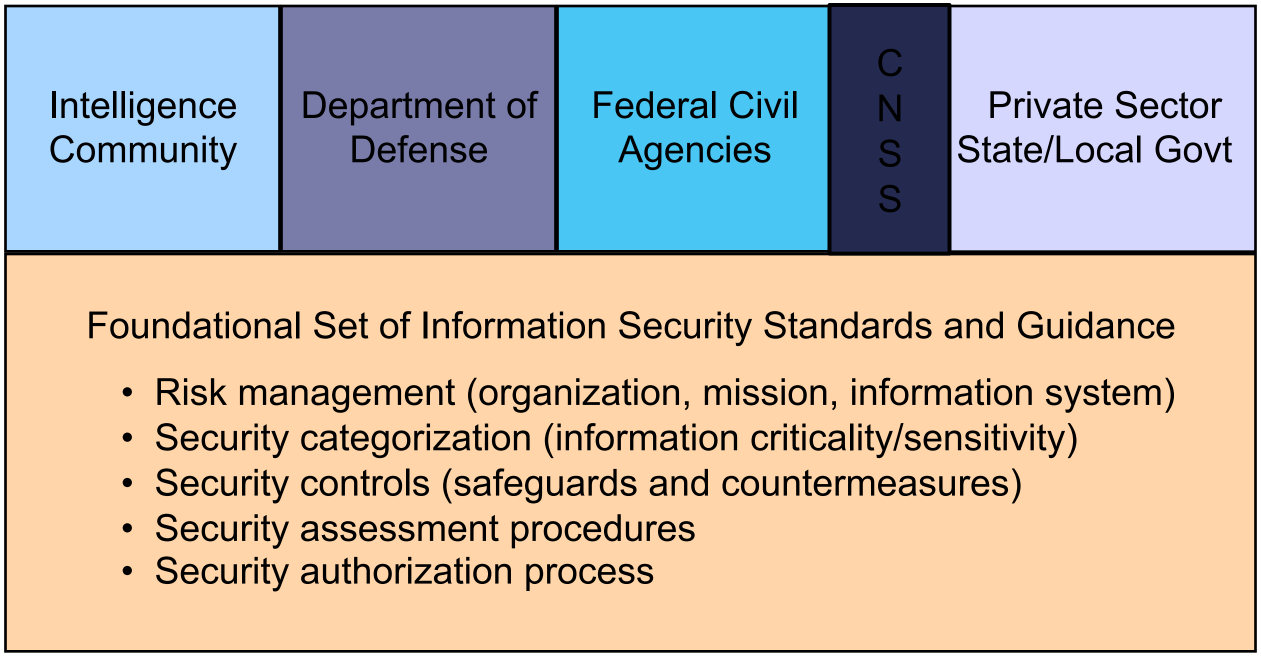
Unified Information Security Framework

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements



Intelligence Community

Department of Defense

Federal Civil Agencies

CNSS

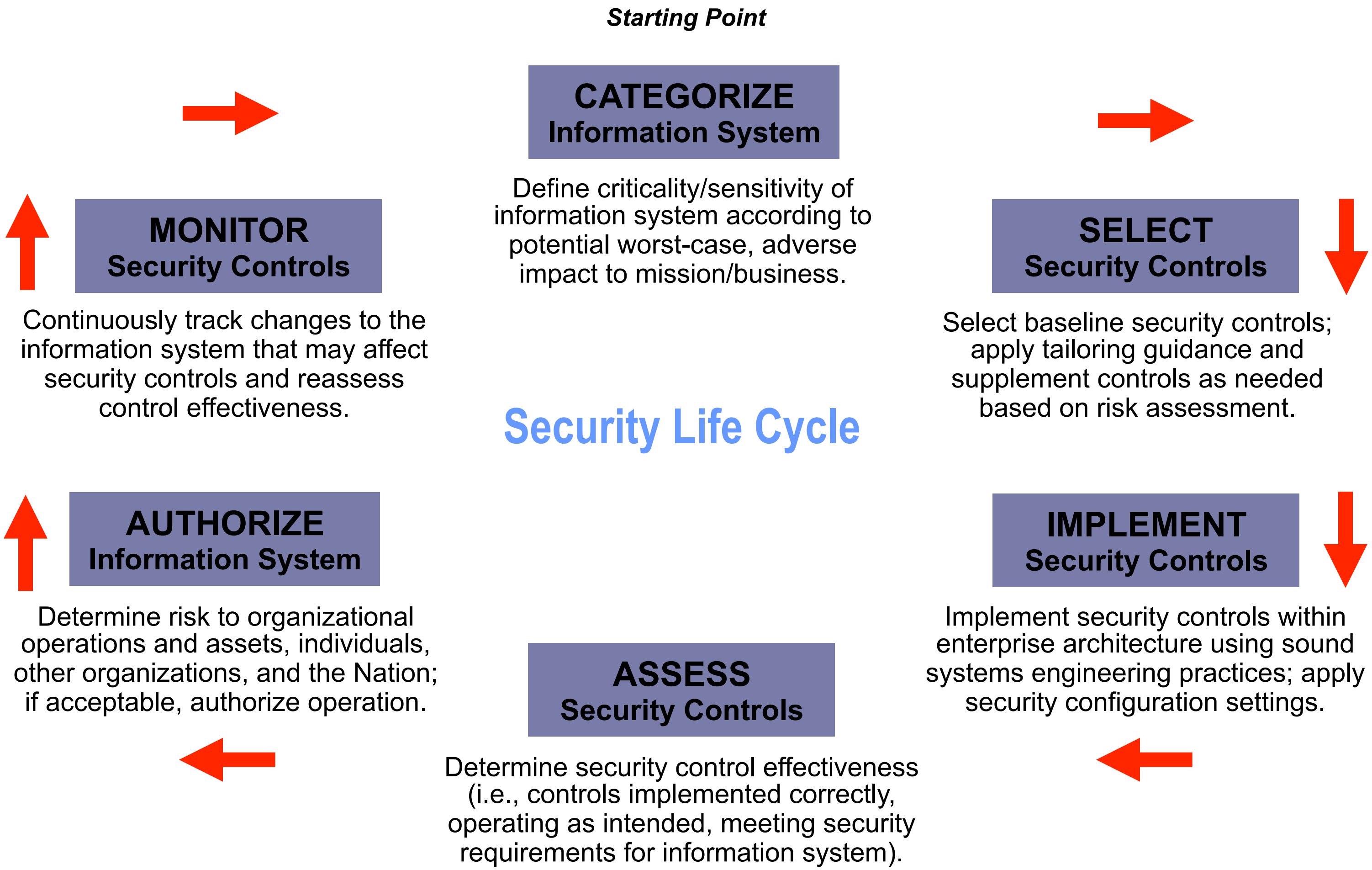
Private Sector State/Local Govt

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

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

NIST Work With Other Agencies

a few other examples

- NIST – DARPA – DOD ; Mobile Devices
- NIST – NSA- DHS ; Security Automation
- NIST – NASA – USAF; Software Testing
- NIST – Industry – SDOs; JTC1/IETF/IEEE/ISO
- NIST – DOE – Industry-FERC; Smart Grid
- DHS/ODNI/DoEd/OPM/NSF/SBA/Labor; NICE
- NIST/DOC/Industry - NSTIC

NIST Reference Materials

- SPs and FIPS
- Testing Conformance Programs
  - Crypto; PIV; IPv6
- The National Vulnerability Database
- Security Automation
- FDCC-USGCB

Preaching to the Choir

- Security vs Usability; Why must we fight?
- Relook at security in context of the Users
  - i.e. Alarm management
- Who do we reach out to? Have we got the right stakeholders?
- Default, easy and understandable

What is Next

- Next set of automation protocols and tools
- Next set of cryptography
- Clouds
- Next set of RMF guidelines
  - – Continuous Monitoring; Risk Assessments
- Next set of recommendations
  - – BIOS; Mobility; Supply Chain;
- Data; Data; Data; Analytics

How Do You Get All This Good Stuff?

- www.csrc.nist.gov

? QUESTIONS ?