

# Introduction to NIST's Risk Management Framework (RMF) and related standards and guidelines, and their application to industrial control systems (ICS)

Stuart Katzke and Keith Stouffer  
National Institute of Standards and Technology

**NOTE: Red Font indicates areas related to software assurance (SA)**

# Relationship Between SA & IT Security

## Simple Example

- SA → Security
  - Incorrect buggy SW can lead to losses of information & information system confidentiality, integrity, and availability
    - Introduces SW vulnerabilities that can be exploited or have other security impacts (e.g., denial of service/availability)
    - SW security controls not implemented correctly (i.e., not providing intended protection)
- Security → SA
  - Loss of SW integrity (i.e., inability to protect against unauthorized changes to SW) can undue SA measures (e.g., well designed, structured code)

# Federal Information Security Management Act of 2002 (FISMA)

Resulted in

NIST's FISMA Implementation  
Project:

Phase I (2003 – 2008)

Phase II (2007 – 2010)

# NIST's FISMA Implementation Project Strategic Vision

- Promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act (FISMA)
- Build a solid foundation of information security across one of the largest information technology infrastructures in the world based on comprehensive security standards and technical guidance.
- Institutionalize a comprehensive Risk Management Framework that promotes flexible, cost-effective information security programs for federal agencies.
- Establish a fundamental level of "security due diligence" for federal agencies and their contractors based on minimum security requirements and security controls.
- NIST standards and guidelines are voluntarily used by the private sector

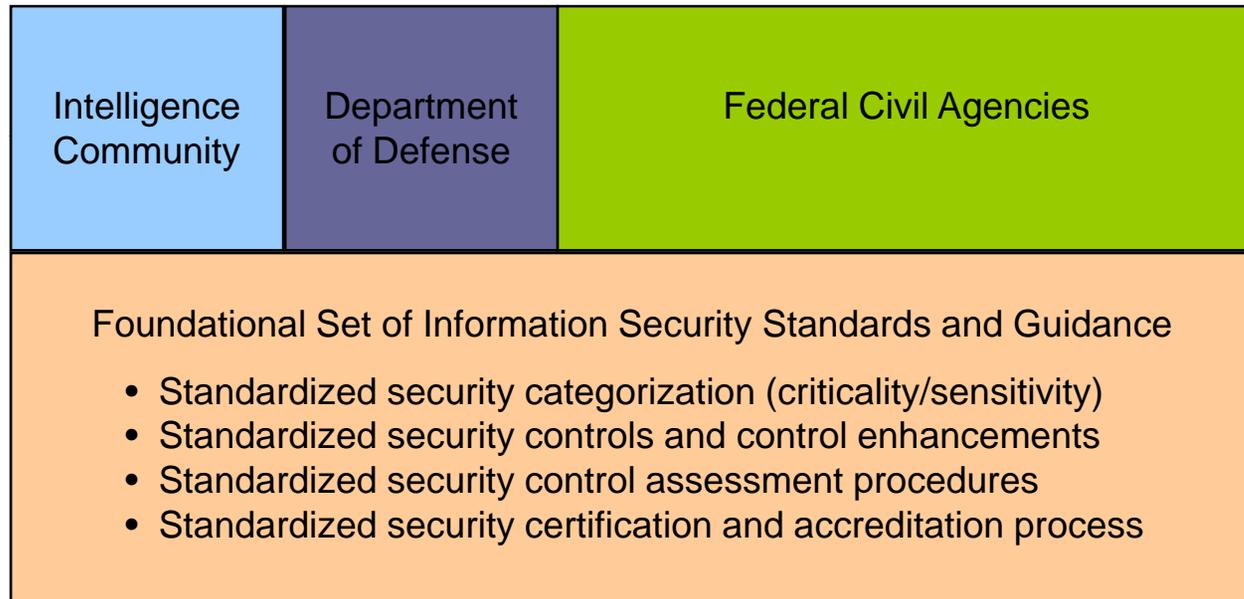
# A Unified Framework

*Civil, Defense, Intelligence Community Collaboration*

## The Generalized Model

**Unique  
Information  
Security  
Requirements**

*The "Delta"*



**Common  
Information  
Security  
Requirements**

National security and non national security information systems

# Phase I

- Mission: Develop and propagate core set of security standards and guidelines for federal agencies and support contractors.
- Timeline: 2003-2008
- Status: On track to complete final publications in FY08.

# Phase I Publications

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment) \*
- NIST Special Publication 800-39 (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) \*

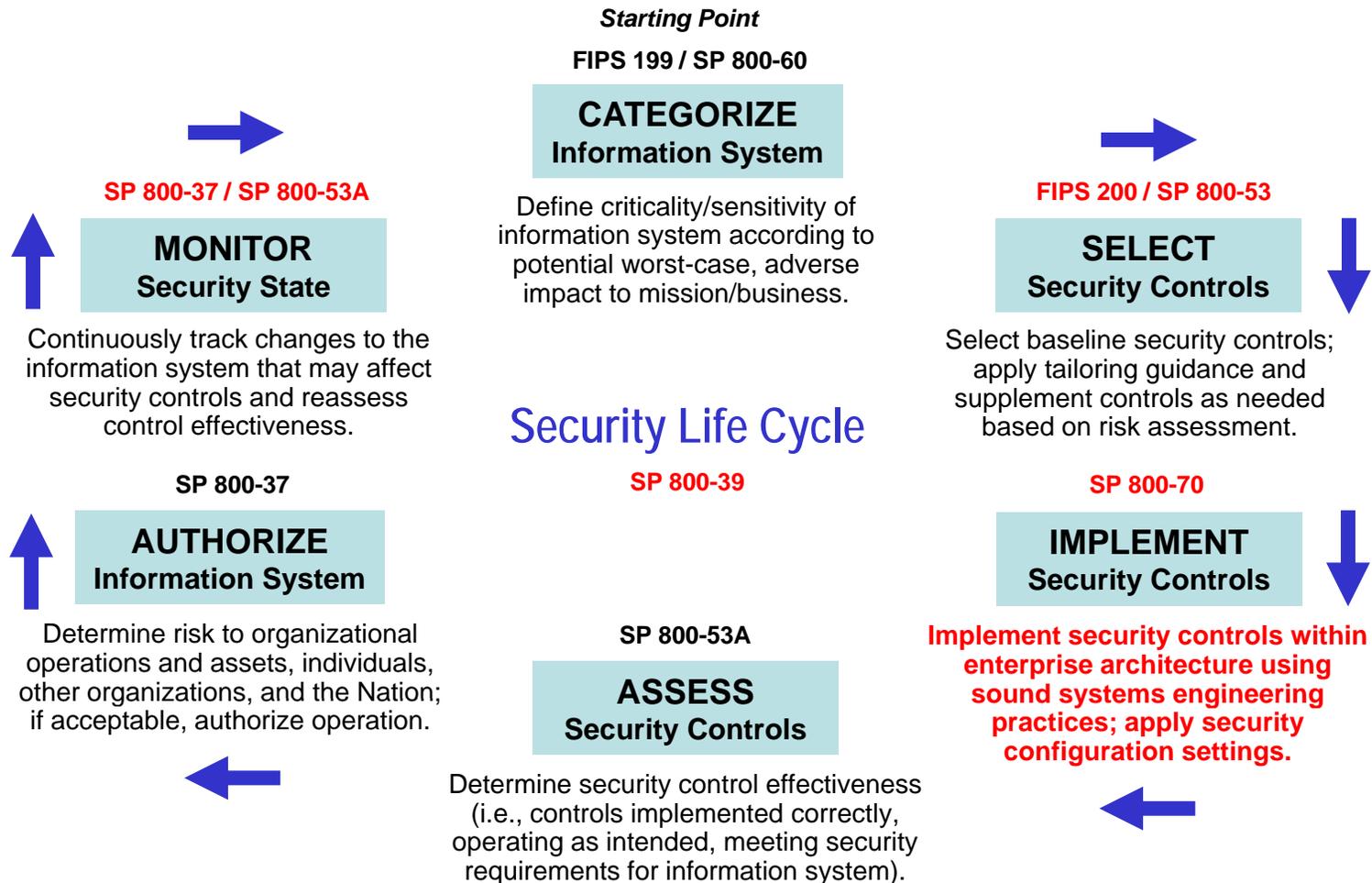
\* Publications currently under revision.

\*\* Publications currently under development.

# Phase II

- Mission: Develop and implement a standards-based organizational credentialing program for public and private sector entities to demonstrate core competencies for offering security services to federal agencies.
- Timeline: 2007-2010
- Status: Projected initiated; Draft NISTIR 7328.

# Risk Management Framework



# SP 800-53 Security Control Classes, Families, and Identifiers

<u>IDENTIFIER</u>	<u>FAMILY</u>	<u>CLASS</u>
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
<b>CM</b>	<b>Configuration Management</b>	<b>Operational</b>
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
<b>MA</b>	<b>Maintenance</b>	<b>Operational</b>
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
<b>SA</b>	<b>System and Services Acquisition</b>	<b>Management</b>
SC	System and Communications Protection	Technical
<b>SI</b>	<b>System and Information Integrity</b>	<b>Operational</b>

# Special Publication 800-39

## *Managing Risk from Information Systems An Enterprise Perspective*

- Extending the Risk Management Framework to enterprises.
- Risk-based mission protection.
- Common controls.
- **Trustworthiness of information systems.**
- Establishing trust relationships among enterprises.
- Risk executive function.
- Strategic planning considerations (defense-in-breadth).

# NIST's Industrial Control Systems (ICS) Project

# Industrial Control Systems - ICS

- What are ICS?
  - Supervisory Control and Data Acquisition (SCADA) Systems
  - Distributed Control Systems (DCS)
  - Programmable Logic Controllers (PLC)
  - Intelligent Field devices
- Used in all process control and manufacturing processes including electric, water, oil/gas, chemicals, auto manufacturing, etc

# CSD/ITL-ISD/MEL ICS Project (1 of 3)

- Cooperative relationship between the Computer Security Division (CSD) & Intelligent Systems Division (ISD) goes back about 7 years with start of the Process Control Security Requirements Forum.
  - CSD: IT security expertise & IT security community recognition
  - ISD: ICS expertise & ICS community recognition
- Federal agencies required to apply the RMF, including SP 800-53, to their ICSs
- Tailor the Risk Management Framework to provide workable, practical solutions for ICS *without causing more harm than the incidents we are working to prevent*

ITL: Information Technology Laboratory

MEL: Manufacturing Engineering Laboratory

National Institute of Standards and Technology

# CSD/ITL-ISD/MEL ICS Project (2 of 3)

- Immediate (short term) focus on improving the security of ICSs that are part of the USG's critical infrastructure (CI).
- Longer term focus on fostering *convergence* of approaches/standards in all government & private sectors that use/depend on all ICSs.
- Assist/support FERC, DHS, and DOE/National Labs in their missions/roles to protect the government's energy/power critical infrastructure from intentional (e.g., cyber attacks) and unintentional events (e.g., natural disasters).

# CSD/ITL-ISD/MEL ICS Project (3 of 3)

- “ICS” augmentation to SP 800-53, Revision 1
  - Hold workshops (3) to
    - Explore the applicability of FIPS 199, FIPS 200, and NIST SP 800-53 to federally owned/operated ICSs.
    - Get U.S. Government (USG) stake holder's inputs/experience
    - Develop the ICS version in cooperation with USG stakeholders
    - Validate the “ICS” version through implementation by USG stake holders and case studies (e.g., Bellingham Cyber Incident)
- NIST SP 800-82: A guidance document on how to secure ICSs

# NIST SP 800-53, Rev 2

- Original NIST SP 800-53, Rev 1 controls were not changed
- Additional guidance was added to Appendix I to address ICS
  - ICS Supplemental Guidance
  - ICS Control Enhancement
  - ICS Control Enhancement Supplemental Guidance
- Additional guidance provides information on how the control applies in ICS environments, or provides information as to why the control may not be applicable in ICS environments.
- Additional guidance was added to 68 of 171 controls
  - ICS Supplemental Guidance added to 59 controls
  - ICS Control Enhancements added to 2 controls
  - ICS Enhancement Supplemental Guidance added to 22 controls

# NIST SP 800-82

- Guide to Industrial Control Systems (ICS) Security
  - Provide guidance for establishing secure SCADA and ICS, including the security of legacy systems
- Content
  - Overview of ICS
  - ICS Characteristics, Threats and Vulnerabilities
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS Security Controls
  - Appendixes
    - Current Activities in Industrial Control System Security
    - Emerging Security Capabilities
    - ICS in the Federal Information Security Management Act (FISMA) Paradigm
- Second public draft released September 2007
- <http://csrc.nist.gov/publications/drafts.html>

# NIST ICS Security Project Contact Information

## *Project Leaders*

Keith Stouffer  
(301) 975-3877  
[keith.stouffer@nist.gov](mailto:keith.stouffer@nist.gov)

Dr. Stu Katzke  
(301) 975-4768  
[skatzke@nist.gov](mailto:skatzke@nist.gov)

[sec-ics@nist.gov](mailto:sec-ics@nist.gov)

## *Web Pages*

Federal Information Security Management Act (FISMA) Implementation Project

<http://csrc.nist.gov/sec-cert>

NIST ICS Security Project

<http://csrc.nist.gov/sec-cert/ics>

# Questions

