Configuration Management and the RMF

*Information Security Transformation for the Federal Government*

**ISSA National Capital Chapter Meeting**

April 20, 2010

Kelley Dempsey

*Computer Security Division*

*Information Technology Laboratory*
The Threat Situation

Continuing serious cyber attacks on public and private sector information systems, large and small; targeting key operations and assets…

- 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 intentions of compromising federal information systems.
- Effective deployment of malicious software causing significant exfiltration of sensitive information (including intellectual property) and potential for disruption of critical information systems/services.
What is at Risk?

- Federal information systems supporting Defense, Civil, and Intelligence agencies within the federal government.

- Information systems supporting critical infrastructures within the United States (public and private sector) including:
  - 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

- Private sector information systems supporting U.S. industry and businesses (intellectual capital).
Federal Government Transformation For Information Security

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
- Standardized security authorization process

National security and non national security information systems
Key Risk Management Publications

- NIST Special Publication 800-53, Revision 3
  *Recommended Security Controls for Federal Information Systems and Organizations - August 2009*

- NIST Special Publication 800-37, Revision 1
  *Guide for Applying the Risk Management Framework to Federal Information Systems - February 2010*

- NIST Special Publication 800-53A, Revision 1
  *Guide for Assessing the Security Controls in Federal Information Systems and Organizations - Final Projected: June 2010 (FPD projected for April 2010)*

- NIST Special Publication 800-39

- NIST Special Publication 800-30, Revision 1

*see [http://csrc.nist.gov](http://csrc.nist.gov) for updated information on public drafts and final publications*
Risk Management Hierarchy

NIST SP 800-39

- Risk Executive Function (Oversight and Governance)
- Risk Assessment Methodologies
- Risk Mitigation Approaches
- Risk Tolerance
- Risk Monitoring Approaches
- Linkage to ISO/IEC 27001
Risk Management Hierarchy

TIER 1
Organization

- Mission / Business Processes
- Information Flows
- Information Categorization
- Information Protection Strategy
- Information Security Requirements
- Linkage to Enterprise Architecture

TIER 2
Mission / Business Process

TIER 3
Information System

NIST SP 800-39

Risk Management Strategy
Risk Management Hierarchy

TIER 1
Organization

TIER 2
Mission / Business Process
- Linkage to SDLC
- Information System Categorization
- Selection of Security Controls
- Security Control Allocation and Implementation
- Security Control Assessment
- Risk Acceptance
- Continuous Monitoring

TIER 3
Information System

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
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.

**SELECT Security Controls**
FIPS 200 / SP 800-53

**IMPLEMENT Security Controls**
SP 800-70

**ASSESS Security Controls**
SP 800-53A
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

**AUTHORIZE Information System**
SP 800-39
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

**MONITOR Security State**
SP 800-37 / SP 800-53A
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
Guide for Security Configuration Management of Information Systems

- NIST Special Publication (SP) 800-128
- Initial Public Draft released 18 March 2010
- Public comments accepted through 14 June 2010*
- Provides guidance for implementation of Configuration Management (CM) family controls from 800-53 Rev 3
- Implementation and continued operation of many non-CM controls are dependent on secure configurations and configuration change control

*Submit comments to sec-cert@nist.gov
SP 800-128 Phases

- Planning Phase
- Configuring to a Secure State Phase (implementing)
- Maintaining the Secure State Phase
- Monitoring
Planning Phase

- Establish/Develop Organizational and System level policies and procedures (CM-1)
- Develop Configuration Management Plan (CM-1/CM-9)
- Establish Change Control Board (CM-3)
- Develop IS Component Inventory (CM-8)
- Indentify Configuration Items (CM-3)
Configure to Secure State Phase

- Establish Secure Configurations (CM-6/CM-7)
- Implement & test Secure Configurations (CM-6/CM-7)
- Document the Secure Baseline Configuration (CM-2)
Maintaining Secure State Phase

- Implement Access Restrictions for Change (CM-5)
- Implement Configuration Change Control process for changes to the Baseline Configuration (CM-3)
- Conduct Security Impact Analyses for changes (CM-4)
- Document changes (new baseline) and archive previous baseline(s) (CM-2)
Monitor Phase

- Assess configurations on an ongoing basis using automated tools
  - Changes to Baselines (actual configuration settings, unauthorized software, etc.)
  - Changes in IS Component Inventory
- Analyze causes of unauthorized changes
- Report configuration status to senior management [Authorizing Official, RE(F), etc.]
- Monitor Phase activities support the generation of metrics
- Monitor Phase activities support all CM Family controls
800-128 Appendices

- The usual suspects
  - General references
  - Glossary
  - Acronyms
- Sample Templates
  - SCM Plan
  - Change Request
- Best Practices w/references to NIST SPs
- SCM Process Flowcharts
NIST SP 800-128 and SCAP (#1)

- SCAP = Security Content Automation Protocol
- The primary purpose of SCAP is to improve the automated application, verification, and reporting of commercial information technology product-specific security configuration settings.
- SCAP consists of six specifications (nomenclatures/metrics/languages)
- SCAP-expressed checklists can map to secure configuration settings
- If SCAP-enabled tools are not available, plan ahead by implementing SCAP-expressed checklists for secure configurations
- Encourage security software vendors to incorporate support for SCAP specifications (CCE, CPE, CVE, XCCDF)
NIST SP 800-128 and SCAP

(#2)

SCAP Specifications:

- Common Configuration Enumeration (CCE) - Nomenclature and dictionary of system security issues
- Common Platform Enumeration (CPE) - Nomenclature and dictionary of product names and versions
- Common Vulnerabilities and Exposures (CVE) - Nomenclature and dictionary of security-related software flaws
- Common Vulnerability Scoring System (CVSS) - Metric for measuring the severity of software vulnerabilities
- Extensible Configuration Checklist Description Format (XCCDF) - Language for specifying checklists and reporting checklist results
- Open Vulnerability and Assessment Language (OVAL) - Language for specifying low-level testing procedures used by checklists

For more information on SCAP, please see http://scap.nist.gov/ and/or NIST SP 800-117 and NIST SP 800-126 at http://csrc.nist.gov
NIST SP 800-128 and the RMF (#1)

- **RMF - Categorize Step**
  - Planning Phase of SCM
  - System information types and overall system impact level, along with organization- and system-level assessment of risk, determine the 800-53 baseline to be applied and level of effort for SCM implementation

- **RMF - Select Step**
  - Planning Phase of SCM
  - Tailor and supplement CM family of controls

- **RMF - Implement Step**
  - Configure to Secure State Phase of SCM
  - Establish, implement, test for functionality, and document Secure Configurations/Baselines
NIST SP 800-128 and the RMF (#2)

- **RMF - Assess Step**
  - Configure to Secure State Phase of SCM
  - Test secure configuration implementations for effectiveness (i.e., is the secure configuration operating as intended with respect to protecting the system)

- **RMF - Authorize Step**
  - Configure to Secure State Phase of SCM
  - Authorizing Official may require changes to the secure configuration and/or implementation of additional controls

- **RMF - Monitor Step**
  - Maintain the Secure State Phase of SCM
  - Monitor Phase of SCM
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

Kelley Dempsey  
(301) 975-2827  
kelly.dempsey@nist.gov

Pat Toth  
(301) 975-5140  
patricia.toth@nist.gov

Arnold Johnson  
(301) 975-3247  
arold.johnson@nist.gov

Web: [csrc.nist.gov/sec-cert](http://csrc.nist.gov/sec-cert)
Comments: sec-cert@nist.gov