Risk Management Framework (RMF) Discussion
November 15, 2016

Defense Security Service
Industrial Security Field Operations

Karl Hellmann
Authorizing Official, NISP Authorization Office (NAO)

Topics

- RMF Phased Implementation Schedule
- NAO Metrics
- DSS RMF Training Resources
- Job Aids, Templates & Artifacts
- Automated Tools

RMF Transition Schedule

Date	Milestones
April-June 2016	Pilot Program with Industry
Jul/Sept 2016	Release RMF Supporting artifacts, tools and job aids. Introduced RMF Resource Page (www.dss.mil/rmf)
August 2016	Release DSS Assessment and Authorization Manual (DAAPM)
October 2016	Start Phased Implementation (Stand-Alone Systems)
January 2017	Review of implementation and metrics for tentative planning of next phase (NISPPAC IA WG)

Metrics

- Zero plans submitted using NIST RMF requirements in October
- 344 currently accredited stand-alone systems due to expire through Feb 28, 2017
- Substantial increase in C&A submissions in September prior to transition start date
- DSS Targeted Time to Authorization Decision – 30 days
  - Estimated time for Industry SSP completion – 15 to 60 days
  - DAAPM recommended submission time – 60 days prior to expiration or need.
  - Proposal systems (Limited ATO/IATO with on-site waived by AO)

DSS RMF Training Resources

- Center for Development of Security Excellence (www.cdse.edu)
- NIST (www.nist.gov)
- NISP Risk Management Framework Resource Center (www.dss.mil/rmf)
- DAAPM
- Getting started with Risk Management Framework

RMF Templates & Job Aids

- NISP Risk Management Framework Resource Center (www.dss.mil/rmf)

- Templates:
  - System Security Plan (SSP)
  - SSP Appendices
  - Plan of Action & Milestones (POA&M)
  - Risk Assessment Report (RAR)
  - ISSM/ISSO Appointment Letter

- Technical Assessment Guides and Job Aids:
  - Windows 7
  - Windows 10
  - Red Hat Enterprise Linux 6
  - Windows Server 2012
  - RMF Overlay for DSS Baseline Categorization (M-L-L)
  - POA&M Job Aid

Automated Tools

- Security Content Automated Protocol (SCAP) Compliance Checker
  - Tool for scanning and analyzing security configurations
- Security Technical Implementation Guidelines (STIG) Viewer
  - A DISA application to view the result of vulnerability scans
- Getting started with the SCAP Compliance Checker and STIG Viewer
  - This document describes how to access and use the tools
- *Future* NAO Secure Baseline Configuration Toolkit
  - This tool will automatically set the technical configurations of the system using Group Policy Object (GPO) within the operating system

Discussion