Raytheon

Risk Management Framework Information Updates and Resources

Chris Biggs, CISSP, CAP

ISSM, FSO, Raytheon Company

October 12th, 2016

DSS Risk Management Framework Transition Plan

Standalone (MUSA/SUSA)
SSPs/MSSPs after October 3, 2016.

Execute RMF Assessment and Authorization through the DAAPM.

Standalones are no longer allowed to be self-certified under the C&A process.

Local Area Network (LAN), Wide Area Network (WAN) or Interconnected System after October 3, 2016.

Phase 1: Cleared contractors continue using the current C&A process with the latest version of the ODAA Process Manual. ATO will last no greater than 18 months starting October 3, 2016. Within six months of authorization, develop a POA&M for transition to RMF. LANs/WANs may continue to be self-certified as authorized under the C & A process.

Phase 2: Execute RMF Assessment and Authorization process through the DAAPM. *(Timeline TBD.)*

http://www.dss.mil/rmf/

Getting Started: Training

- CDSE: Introduction to the Risk Management Framework – high level overview of the RMF process and steps.
- DSS RMF Webinar Training Slides – Still high level but starting to look at the DSS implementation of RMF.
- Applying the RMF to Federal Information Systems – Not specific to DSS and industry implementation but more process.
- DISA RMF Training Presentation – geared toward DoD RMF implementation (overall RMF process)

Getting Started: Policy and Guidance

- NISPOM – no real IA related changes
- NIST 800-53 Security & Privacy Controls – the controls needed to be implemented. Moderate-Low-Low base.
- ODAA Process Manual – Very high level
- DSS Assessment and Authorization Manual (DAAPM) – more detailed, provides organizational requirements

Getting Started: Resources

- Getting Started with RMF – Pretty much this presentation
- NISPOM to NIST 800-53v4 Mapping – Where the guidance for each control is in the NISPOM. (Policy Document)
- System Security Plan Template
- System Security Plan Template Appendices - forms
- Plan of Action & Milestones (POA&M)
- Capital Region Excel SSP (Contact your ISSP/SCA)

SSP Changes

- Old SSP and IS Profile was a combined 80 pages with various boxes, in a locked PDF. Very straight forward.
- New SSP (and Appendices) is 223 pages in a Word file with each security control.
  - Some controls can be tailored out depending on the environment
  - Some can be partially mitigated
  - You could implement a compensating control
  - If you don’t have a process in place today, you can also POA&M them until you have a process.

RMF Changes – Just a few highlighted changes

- Establishment of a Configuration Control Board (CCB), must approve in writing all hardware changes: CM-3
- New DSS Authorized Warning Banner
- Auto-Disable after 90 days of inactivity: AC-2
- Data Transfer Agent – 2 separate accounts, transferring ANY data, including logging: AC-6(2)
- Two Person Integrity for all file transfers: AC-3(2)
- Separation of Duties: AC-5
- Need to monitor for wireless access points quarterly: AC-18
- All portable media will be encrypted: MP-2
- Media must be sanitized before 1st use: MP-6(3)

Getting Started: SCAP Tool and Technical Implementation

Training: Getting Started with the SCAP compliance checker and STIG Viewer

Resources:

- Technical Assessment Guide for Windows 7, Windows 10, Server 2012, RHEL 6
- SCAP Compliance Checker & DISA STIG Viewer