NAO Roundtable
May 17, 2016

Defense Security Service
Industrial Security Field Operations

Karl Hellmann
Assistant Deputy Director, NISP Authorization Office (NAO)

NAO Topics

- NAO Operational Priorities
- RMF Timeline, Artifacts and Training
- Developing an Organizational Risk Assessment
- OBMS
- Command Cyber Readiness Inspections (CCRI)

NAO Operational Priorities

- Transition to Risk Management Framework (RMF)
- Development and Implementation of Quality Assurance Program
- Automated Tools for configuration assessments (SCAP/STIG Viewer)
- Integrate new CNSSI 7003 standards (PDS) into ISSP workload
- Coordinate agreements with government partners for RMF

RMF Transition Schedule

Date	Milestones
April-June 2016	Pilot Program with Industry
May/July 2016	Training for DSS Field Elements
June 2016	Release all RMF Supporting Artifacts, tools and job aids (Industry Training)
July 2016	Release Assessment and Authorization Manual
August 2016	Phased Implementation begins

What is Phased Implementation?

- The reason for phased implementation is to ensure that both Industry and DSS are successful in the transition to RMF
- Success will be measured by the ability of Industry to submit acceptable SSP's and DSS to complete authorization decisions within the current 30 day after submission timeline
- The first phase of the transition will be to submit only SSP's for stand-alone systems (the simplest systems we authorize) using the RMF process
- Once we have ensured that Industry and DSS can successfully accomplish the RMF process we will plan to transition more complex systems (LAN's/WAN's/SIPR) to the RMF process
- The goal is to be completely transitioned to the RMF process by February 1, 2018

RMF Artifacts

- Template SSP's
- NIST Overlays for tailoring controls
- DSS Assessment and Authorization Manual (DAAPM)
- Control Mapping NISPOM to NIST Guide
- Technical Assessment Guides

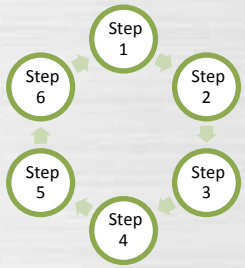
RMF Training Provided by CDSE

Introduction to RMF (CS124.16)

Continuous Monitoring (CS200.16)

Categorization of the System (CS102.16)

Monitoring Security Controls (CS107.16)



Selecting Security Controls (CS103.16)

Authorizing Systems (CS106.16)

Implementing Security Controls (CS104.16)

Assessing Security Controls (CS105.16)

Risk Assessment

- Coordinate with your government customer
  - Classification of program
  - Government threat assessment
  - Categorization of like government systems
- Local conditions for the facility
  - Facility location
  - System protections
  - Physical protections
  - Personnel at facility
- Corporate policies and procedures
  - Incident Response Plan
  - Disaster Recovery
  - Continuity of Operations
- DSS coordination
  - DSS CI threat assessment
  - Approval of physical security

OBMS

- Release 2.3.3 is current release. Release 3.1 is tentatively scheduled for the July/August timeframe
- Support for OBMS is transitioning within DSS
  - Knowledge Center replacing Call Center
  - Back end support from developer to DSS OCIO
- NCAISS will remain as the entry point to DSS systems
- National Industrial Security System (NISS) will modernize current DSS applications (ISFD; OBMS; e-FCL)

CCRI

- DSS will continue to conduct a portion of the CCRI's for industry on behalf of USCYBERCOM/DISA
- Imperative for Industry to work with the SIPR circuit sponsor
- Industry is responsible for maintaining the security of the SIPR circuit according to DISA regulations
- DISA has begun conducting No-notice CCRI's

Discussion