DSS Monthly Newsletter
July 2016 (Special Edition)

(Sent on behalf of your ISR.)

Dear FSO,

This is a special release in addition to the monthly VOI newsletter. This message contains information, and/or policy guidance of a time-sensitive nature. If you have any questions or recommendations for information to be included, please feel free to let us know.

RMF TRANSITION DATE EXTENDED TO OCTOBER 3, 2016

The DSS transition to Risk Management Framework (RMF)[1] was scheduled to begin on August 1, 2016. After assessing workload data obtained from the RMF Industry Pilot and reviewing concerns from Industry, DSS has decided to adjust the transition start date to October 3, 2016 for stand-alone systems.

The transition date change was briefed by the NISP Authorization Office (NAO), to the NISPPAC Certification and Accreditation (C&A) Working Group on Thursday, July 7, 2016. These two extra months provide our industry partners additional time to ensure their Information Systems security personnel are better trained and prepared to implement RMF.

The DSS NISP RMF methodology facilitates reciprocity within the DoD community and partner organizations in the NISP. This methodology aligns cleared industry's unique security environment with Federal government and DoD NIST system security standards. The DSS RMF will be promulgated in the DSS Assessments and Authorization Process Manual (DAAPM). The DAAPM will tentatively be available August 1, 2016.

The DAAPM provides guidance, templates, security controls, System Security Plan (SSP) Templates and other artifacts necessary for the RMF transition and necessary to meeting mandated implementation timelines. The DSS RMF Resource Center located at www.dss.mil/rmf, provides standardized information assurance-related implementation guidance for policy and procedures for management of all facilities, networks, and systems under the DSS cognizant Authorizing Official (AO) (previously referred to as the Designated Approving Authority).

[1] RMF is the unified information security framework for the federal government that is replacing the legacy Certification and Accreditation (C&A) processes within federal government departments/agencies, DoD, and the IC.

Current authorizations are grandfathered and systems can continue to process under existing authorizations until expiration. See transition timeline below:

System Accreditation Status	**Transition Timeline / Instructions**
System Security Plan /Master System Security Plan (MSSP) submitted prior to October 3, 2016.	Continue using current C&A process with the latest version of the ODAA Process Manual. The ATO will last no greater than 18 months starting October 3, 2016. Within six months of authorization, develop a Plan of Action and Milestones (POA&M) for transition to RMF.
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. **Phase 2:** Execute RMF Assessment and Authorization process through the DAAPM. *(Timeline TBD.)*

As we work through the overhaul of the legacy NISP C&A process, we recognize the challenge inherent in the transition. We ask for both your flexibility and cooperation as we collectively work to manage this change while maintaining the enhanced security procedures essential to the NISP.

Questions should be addressed through your DSS Field Office communications channels to the appropriate regional Authorizing Official.

Thanks,
ISR
Defense Security Service