DATA ITEM DESCRIPTION

Title: DOD Risk Management Framework (RMF) Package Deliverables

Number: DI-MGMT-82001
AMSC Number: 9595
DTIC Applicable: No
Preparing Activity: AS
Applicable Forms:

Approval Date: 20151027
Limitation:
GIDEP Applicable: No
Project Number: MGMT-2015-020

Use/relationship: The RMF Package Deliverable data will be used to satisfy the requirements of the RMF.

This Data Item Description (DID) contains the format, content, and intended use information for the data product resulting from the work task described by the contract.

Requirements:

1. Format. The RMF package artifacts shall be delivered in a format approved by the Government's Designated Accrediting Authority (DAA), Navy Authorizing Official (NAO) Authorizing Official (AO), or Information Systems Security Manager (ISSM).

2. Content. The content of the RMF package artifacts shall contain the necessary artifacts required by the DAA, NAO, AO, or ISSM to successfully achieve Platform IT (PIT) Designation, Platform IT Risk Approval (PRA), Interim Authority to Test (IATT), or Authority to Operate (ATO).

2.1 Introduction. This section shall contain a narrative of the RMF package deliverable content.

2.1.1 IATT Request. The IATT Request shall use the approved DAA, NAO, AO, or ISSM format. The IATT Request shall use the approved Test Plan document to identify the 'who', 'what', 'why', 'where', 'when', and 'how' of the requested Test event. The IATT Request may require IA Test Plan artifacts such as vulnerability scans and STIG checklists. The IATT Request shall be delivered not less than 30 days prior to the start of the Test Event to the Program Office.

2.1.2 Security Plan (SP). The SP shall use the approved DAA, NAO, AO, or ISSM format. The SP shall contain at a minimum, System Information, Mission Description, Concept of Operations (CONOPS), Environment, Operating and Computing Environment, Physical Security Measures, Facilities Descriptions, Threat Analysis, System Architecture Description, Components, Configurations, Accreditation Boundaries, Connection Process Guide (CPG) Compliant Network Diagrams, External Interfaces and Data Flow, Internal Data Flow, Contingency Plan, Incident Response Plan, User Descriptions and Clearances, Security Roles, Hardware Lists, Software Lists, Ports, Protocols, and Services (PPS), Configuration Management Plan, Information Assurance Vulnerability Management (IAVM) Plan, and A&ATasks and Milestones. The SP shall be approved and signed by the ISSM, User Rep, Program Manager (PM), and DAA, NAO, or AO.

2.1.3 Assessment and Authorization (A&A) Project Plan. The A&A Project Plan shall use the approved DAA, AO, or ISSM format. The A&A Project Plan is used to establish an executable RMF project plan. The A&A Project Plan shall be approved and signed by the ISSM, Echelon II

Representative, and PM. The A&A Project Plan shall define the various A&A Tasks and Milestones needed to achieve PRA, IATT, or ATO.

2.1.4 Collaboration Brief. The Collaboration Brief is a summary of the System Overview, RMF Package, and Residual Risk that is presented to the DAA, NAO, AO, Certification Authority (CA), or Security Control Assessor (SCA) during Collaboration. The Collaboration Brief shall use the approved DAA, NAO, AO, or ISSM format. The Collaboration Brief is submitted with the RMF package and is used to describe the System and Residual System Risk during the Collaboration meeting.

2.1.5 RMF Implementation Plan. The RMF Implementatn shall use the approved DAA, NAO, AO, or ISSM format. The DIP shall be used during the DIP Concurrence meeting with the Echelon II, Navy CA, and ODAA. The DIP shall define which IA Controls (IACs) will be 'Implemented', 'Inherited', 'Non-Compliant', or 'Not Applicable'. The DIP shall be approved by the DAA, AO, and ISSM prior to execution of the IA Test Plan. The DIP must be approved before moving forward with IA Control Implementation.

2.1.6 PIT Implementation Plan (PIP). The PIP shall use the approved DAA, NAO, AO, or ISSM format. The PIP shall be used during the PIT Concurrence meeting with the Echelon II, Navy CA, and ODAA. The PIP shall define which IACs will be 'Implemented', 'Inherited', 'Non-Compliant', or 'Not Applicable'. The PIP shall be approved by the DAA, AO, and ISSM prior to execution of the IA Test Plan. The PIP must be approved by the DAA, NAO, AO, CA, or SCA before moving forward with IA Control Implementation.

2.1.7 IA Test Plan. The IA Test Plan shall use the approved DAA, NAO, AO, or ISSM format. The IA Test Plan shall define all required Vulnerability Scans, Security Technical Implementation Guides (STIGs), Security Readiness Guides (SRGs), Secure Content Automation Protocol (SCAP) benchmarks, and other IA Controls or Security Overlays to be applied to the System. The IA Test Plan shall be approved by the DAA, NAO, AO, and ISSM during the DIP or PIP Concurrence Meeting. The IA Test Plan must be approved by the DAA, NAO, AO, CA, or SCA prior to moving forward with IA Control Implementation.

2.1.8 PIT Designation Request. The PIT Designation Request shall use the approved DAA, NAO, AO, or ISSM format. The PIT Designation Request is the formal request to the DAA, NAO, or AO that the System meets the requirements of PIT and shall be designated as Platform IT (versus an Information System (IS)). The PIT Designation Request shall be approved and a PIT Designation Letter shall be signed by the DAA or AO prior to the execution of the IA Test Plan and implementation of IA Controls.

2.1.9 PIT Determination Brief. The PIT Determination Brief shall use the approved DAA, NAO, AO, or ISSM format. The PIT Determination Brief shall be used in conjunction with the PIT Designation Request to formally request the System be designated Platform IT (versus and Information System).

2.1.10 Plan of Action and Milestones (POA&M). The POA&M shall use the approved DAA, NAO, AO, or ISSM format. The POA&M shall be considered a 'living' document and shall regularly be updated throughout the entire lifecycle of the System through Decommission. The POA&M shall contain all Not Applicable (N/A) IA Controls, All Non-Compliant IA Controls, and all Non-

Compliant Vulnerability Findings as identified in the Vulnerability Scans, STIGs, SRGs, and SCAP Benchmarks. At a minimum, the POA&M shall be updated monthly.

2.1.11 Privacy Impact Assessment (PIA). The PIA shall use the approved DAA, AO, or ISSM format. The PIA shall be approved and signed by the ISSM, PM, and the Command PIA Officer.

2.1.12 Vulnerability Scans. In accordance with the approved IA Test Plan, the System shall be scanned using the approved vulnerability scanning tools as identified by the DAA, AO, or ISSM. The vulnerability scanner shall be updated with the latest signatures and scanning engines prior to the execution of each vulnerability scan. At a minimum, vulnerability scans shall be conducted monthly against the System. Non-compliant findings shall be documented in the System POA&M on a minimum monthly basis. At a minimum, vulnerability scans shall be submitted electronically to the ISSM or uploaded into the RMF package (eMASS) or the Vulnerability Remediation Asset Manager (VRAM). Vulnerability scans shall be handled and transmitted in accordance with the System's classification level. Vulnerability reports shall be in a format approved by the DAA, NAO, AO, or ISSM. Vulnerability scans shall be protected in accordance with the System's classification.

2.1.13 Security Technical Implementation Guides (STIGs), Security Readiness Guides (SRGs), Secure Content Automation Protocol (SCAP) Benchmarks. In accordance with the approved IA Test Plan, the System shall be hardened using the required and approved STIGs, SRGs, SCAP Benchmarks, and other approved hardening tools. Non-compliant STIG, SRG, SCAP Benchmark, and other findings shall be documented in the System POA&M on a minimum monthly basis. Updates to the STIGs, SRGs, and SCAP Benchmarks are released on a monthly, quarterly, and yearly basis. Updates to the STIGs, SRGs, and SCAP Benchmarks shall be implemented into the System as they are released. Non-compliant STIG, SRG, and SCAP Benchmark findings shall be documented in the System POA&M on a minimum monthly basis. STIG, SRG, and SCAP Benchmark artifacts shall be provided in a format approved by the DAA, NAO, AO, or ISSM. STIG, SRG, and SCAP Benchmark artifacts shall be handled in accordance with the System's classification level. At a minimum, STIG, SRG, and SCAP Benchmarks shall be submitted electronically to the ISSM or uploaded into the RMF/RMF Package on a minimum monthly basis. STIG, SRG, and SCAP Benchmark results shall be protected in accordance with the System's classification.

2.1.13 Scorecard. The Scorecard shall use the approved DAA, NAO, AO, or ISSM format. The Scorecard shall be maintained and updated on a minimum monthly basis.

2.1.14 Contingency Plan. The Contingency Plan shall use the approved DAA, NAO, AO, or ISSM format. The Contingency Plan shall be submitted in conjunction with the System's SP. The Contingency Plan shall be approved and signed by the PM, ISSM, and DAA, NAO, or AO.

2.1.15 Information Assurance Vulnerability Management (IAVM) Plan. The IAVM Plan will define how the Developer and Program Office will track, notify, and implement security vulnerabilities as they are identified. The IAVM Plan shall use the approved DAA, NAO, AO, or ISSM format. The IAVM Plan shall be submitted in conjunction with the System's SP. The IAVM Plan shall be approved and signed by the PM, ISSM, and DAA, NAO, or AO.

2.1.16 Cyber Security Waiver Requests. Cyber Security Waiver Requests are an acknowledgement by the PM that compliance will not or can not be made during the life of the System due to technology or Programmatic constraints. Cyber Security Waivers shall use the approved DAA,

NAO, or AO format. All Cyber Security Waivers shall be approved and signed by the ISSM, PM, and First Flag or Equivalent prior to submission to the DAA or AO.

2.1.17 Cyber Security Waiver Extension Request. Cyber Security Waiver Extension Requests are an acknowledgment by the PM that compliance will be met beyond the stated compliance date. Cyber Security Waiver Extensions shall use the approved DAA, NAO, or AO format. All Cyber Security Waiver Extensions shall be approved and signed by the ISSM, PM, and First Flag or Equivalent prior to submission to the DAA or AO.

End of DI-MGMT-82001