DATA ITEM DESCRIPTION
Title: NAVAL AVIATION SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROCESS

Number: DI-MGMT-82147A
AMSC Number: N10062
DTIC Applicable: No
Preparing Activity: AS
Applicable Forms: N/A

Approval Date: 20190807
Limitation: N/A
GIDEP Applicable: Yes
Project Number: MGMT 2019-020

Use/Relationship: This Data Delivery Item contains the format, content and intended use information for the Naval Aviation Supply Chain Risk Management (SCRM) process report resulting from the work task described in the contract.

This DID contains the format, content, and intended use information for the data product resulting from the work task.

This DID supersedes DI-MGMT-82147.

Requirements:

1. Referenced Documents: The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as specified in the contract.

1.1. Individual program office program protection plan.

1.2. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161, Supply Chain Risk Management (SCRM) Practices for Federal Information Systems and Organizations, April 2015. Copies of this document can be found at https://csrc.nist.gov/publications/detail/sp/800-161/final

1.3. DoDI 5200.44 (20121105) Incorporating Change 3 (20181015), Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN). Copies of this document can be found at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf

2. Format: Contractor format is acceptable.

3. Content: The report shall contain the following:

3.1. Identify the SCRM lead

3.2. Identify SCRM countermeasures for Critical Program Information and Critical Components

3.3. Explain the Criticality Analysis Process

3.4. Provide a list of Critical Components

3.5. Provide supplier information for all critical components

3.6. Provide assessment for any threats to critical components from suppliers and indicate countermeasures taken to mitigate the threat(s)

3.7. Provide a counterfeit prevention plan for protection of critical components

3.8. Specify assurance measures to ensure no malicious intent is designed into critical components

3.9. Describe SCRM security controls implementation per NIST SP 800-161

4. Objective Quality Evidence (OQE) is any statement of fact, either quantitative or qualitative, pertaining to the quality of a product or service based on observations, measurements, or tests, which can be verified and is required in sufficient detail to describe the data elements in the Statement of Work.

5. Distribution Statement, as appropriate, in accordance with Department of Defense Instruction (DoDI) 5230.24, Distribution Statements on Technical Documents (Copies of this document can be obtained at: https://www.esd.whs.mil/.) Classification markings, as necessary, in accordance with DoD Manual (DoDM) 5200.01, Volume 2, DoD Information Security Program: Marking of Information. (Copies of this document can be obtained at: https://www.esd.whs.mil/.)"

End of DI-MGMT-82147A