Downloaded from http://www.everyspec.com

DATA ITEM DESCRIPTION

Title: Naval Aviation Government Furnished Equipment (GFE) and Government Furnished Information (GFI) Cyber Vulnerability Report

Number: DI-MGMT-82146
AMSC Number: N9845
DTIC Applicable: N/A
Preparing Activity: AS
Applicable Forms: N/A

Approval Date: 20170726
Limitation: N/A
GIDEP Applicable: N/A
Project Number: MGMT-2017-045

Use/relationship: This Data Delivery Item contains the format and content for the contractor to report new cybersecurity vulnerabilities identified in GFE/GFI during execution of the contract. This report also contains a section for contractors to provide recommend hardware/software. Firmware changes or methods to remediate found vulnerabilities

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

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.

2. Format: Contractor format acceptable.

3. Content: The report shall contain the following information:

3.1. Government Furnished Equipment

3.1.1. Provide a description of the GFE item and the functions/tasks the item will perform with in the system.

3.1.2. Provide a detailed description of the vulnerability(ies) and the operating conditions that drive the vulnerability(ies). Include in the analysis potential cyber risks to the system

3.1.2.1. Provide a top level description of recommended solution to resolve vulnerability. Include estimated cyber risk after implementation of the proposed solution.

3.1.2.2. Include the pros/cons of the recommendation.

3.1.2.3. Include other options considered but not chosen and reason for exclusion.

3.1.2.4. Include a high/medium/low estimate of time and schedule to implement recommended solution

Downloaded from http://www.everyspec.com

3.2. Government Furnished Information

3.2.1. Provide a description of the GFI item and the systems/functions impacted.

3.2.2. Provide a detailed description of the vulnerability(ies) and the operating conditions that drive the vulnerability(ies). Include in the analysis potential cyber risks to the system

3.2.2.1. Provide a top level description of recommended solution to resolve vulnerability. Include estimated cyber risk after implementation of the proposed solution.

3.2.2.2. Include the pros/cons of the recommendation.

3.2.2.3. Include other options considered but not chosen and reason for exclusion.

3.2.2.4. Include a high/medium/low estimate of time and schedule to implement recommended solution

End of DI-MGMT-82146