DATA ITEM DESCRIPTION

Title: VULNERABILITY ASSESSMENT REPORT

Number: DI-IPSC-82252
AMSC Number: 10001
DTIC Applicable: No
Preparing Activity: MDA
Applicable Forms: None

Approval Date: 20190124
Limitation: N/A
GIDEP Applicable: No
Project Number: IPSC-2019-004

Use/Relationship: The Vulnerability Assessment Report documents the results of the vulnerability analysis and subsequent testing/evaluation of the as-built system, component, or service.

This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific task requirement included in the contract.

Requirements:

1. **Format.**

    a. The report shall be in contractor format unless otherwise specified on the Contract Data Requirements List (CDRL) (DD 1423).

    b. Security classification and distribution markings shall conform to the requirements of the contract, purchase description, and security requirements checklist, as applicable.

2. **Content.**

The Vulnerability Assessment Report shall:

    a. Document or reference the process used to perform the vulnerability assessment.

    b. Document the results of the vulnerability assessment.

        i. Identify sources of information used to support the software vulnerability assessment (e.g. vulnerability scanning, penetration, and fuzz testing tools and techniques).

        ii. Document all security-relevant information associated with identified software vulnerabilities to include detailed tool output when available.

        iii. Identify software vulnerabilities and attack patterns by Common Vulnerabilities and Exposures (CVE) identifier and Common Attack Pattern Enumeration and Classification (CAPEC) identifier where applicable.

Source: https://assist.dla.mil -- Downloaded: 2026-11-18T20:58Z
Check the source to verify that this is the current version before use.

iv. Provide recommendations for mitigating identified vulnerabilities.

END OF DI-IPSC-82252

Source: https://assist.dla.mil -- Downloaded: 2026-11-18T20:58Z
Check the source to verify that this is the current version before use.