DATA ITEM DESCRIPTION

Title: SOFTWARE VULNERABILITY ASSESSMENT REPORT (SVAR)

Number: DI-IPSC-82252A
AMSC Number: 10220
DTIC Applicable: No
Preparing Activity: MDA
Applicable Forms: None

Approval Date: 20210211
Limitation: N/A
GIDEP Applicable: No
Project Number: IPSC-2021-004

Use/Relationship: The Software Vulnerability Assessment Report (SVAR) documents the results of software assurance activities from: threat assessment; attack surface analysis; static, dynamic, manual testing; supply chain risk management; vulnerability and risk assessment; and concludes with plans of action and milestones to mitigate risks to an acceptable level.

This DID contains the format, content, and intended use information for the data deliverable resulting from the work task described in the contract. This DID supersedes DI-IPSC-82252.

Requirements:

1. Reference 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.

a. "DoD Developer's Guidebook for Software Assurance," Carnegie Mellon University, Software Engineering Institute (SEI), federally funded research and development center (FFRDC). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=539177

b. "Program Manager's Guidebook for Software Assurance," Carnegie Mellon University, Software Engineering Institute (SEI), federally funded research and development center (FFRDC). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538771

c. "Software Assurance Evaluation Report (SAER)," DID Number DI-IPSC-82249, https://assist.dla.mil

d. "DoD Risk Management Framework (RMF) Knowledge Service," https://rmfks.osd.mil/rmf/Pages/default.aspx

2. Format.

The report shall be in contractor format unless tailored out in the Contract Data Requirements List (CDRL) (DD 1423).

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

3. Content.

This section shall be divided into paragraphs, as needed, to establish the context for the content described in later sections. "The term 'document' in this DID shall mean a collection of data regardless of its medium. The terms "section" and "paragraph" in this DID shall mean their equivalents in a digital format that fulfill the section or paragraph's requirements."

3.1 Reference Documents

This section shall list the number, title, revision, and date of all documents referenced in the report. This section shall also identify the source for all documents not available through normal Government stocking activities.

3.2 Document Management and Configuration Control

This section shall identify the version, release date, and other relevant management and configuration control information associated with the current version of the document. A change history highlighting significant changes from version to version, shall be included.

3.3 Table of Contents

This section shall index all sections, major paragraphs, subparagraphs and appendices with page numbers.

3.4 Document Scope

This section shall be divided into paragraphs covering system and software or Computer Software Configuration Item (CSCI) identification, system overview and document overview.

3.4.1 System and Software or Computer Software Configuration Item (CSCI) Identification

This section shall contain a full identification of the system and the software or Computer Software Configuration Item (CSCI), to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).

3.4.2 System Overview.

This section shall briefly state the purpose of the system to which the report applies. It shall describe the general nature of the system and software or CSCI; summarize the history of system development, operation, and maintenance; identify the project sponsor, acquirer, user, developer, and support agencies; identify current and planned operating sites; and list other relevant documents.

3.4.3 Document Overview

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

This section shall summarize the purpose and contents of the report and shall describe any security or privacy considerations associated with its use.

3.5 Software Overview

This section shall provide an overview description of the software or Computer Software Configuration Item (CSCI) pertaining to the vulnerability analysis.

3.6 Risk Management Framework (RMF)

This section shall document the RMF categorization, data types, and include a RMF control matrix showing compliance status for each RMF control, Reference d.

3.7 Software Operational Environment

This section shall identify the software operational environment (e.g., Defense System component, Research, Test, Development, Maintenance, Training & Planning, or Enterprise Business).

3.8 Software Architecture

This section shall provide an overview the software architecture including system, software, or Computer Software Configuration Item (CSCI) boundaries and interfaces.

3.9 Cybersecurity Functional Properties

This section shall provide a description of the cybersecurity functional properties of the software or firmware to be employed (e.g., identification, authorization, access controls, encryption, logging, data marking, fail-over and recovery, etc.).

3.10 Non Developmental Item (NDI) Software

This section shall identify all NDI software, including Bill-of-Materials of the 3rd party Commercial-off-the-Shelf(COTS), Government-off-the-Shelf (GOTS), and Open Source Software (OSS) used within the software.

3.11 Methods and Process

This section shall be divided into paragraphs, as needed, to establish the engineering methods, development processes, testing and evaluation techniques, quality control process, and program roadmap described in later sections.

3.11.1 Software Security Engineering Methods

This section shall provide a brief description of the software security engineering methods associated with the system software under vulnerability assessment.

3.11.2 Software Development Process

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

This section shall provide a brief description of the software development process for the developed software under vulnerability assessment.

3.11.3 Testing and Evaluation Techniques

This section shall provide a brief description of the software or Computer Software Configuration Item (CSCI) test, evaluation and validation techniques associated with the system software under vulnerability assessment.

3.11.4 Quality Control Processes

This section shall provide a brief description of the quality control processes associated with the system software under vulnerability assessment.

3.11.5 Program Roadmap

This section shall provide a brief description of the program roadmap associated with the vulnerability assessment of the system software.

3.12 Software Assurance Residual Risk Assessment

This section shall be divided into paragraphs, as needed, to establish the software assurance residual risk assessment described in later sections.

3.12.1 SAERs for Developed Software

This section shall provide a consolidated summary of Software Assurance Evaluation Reports (SAER) associated with results of static, dynamic, and manual software analyses of all developed software.

3.12.2 SAERs for NDI Software

This section shall provide a consolidation summary of NDI software SAERs on all applicable 3rd party COTS, GOTS, and OSS SAERs.

3.12.3 SAER and RMF

This section shall provide a system level residual risk assessment from all SAER, Reference c, results into an RMF Control Matrix, Reference d showing compliance status for each RMF control.

3.12.4 Plan of Actions and Milestones (POAM)

This section shall include in an appendix to the report a POAM addressing all non-compliant RMF Controls. Each item in the POAM shall have a description of the residual risk, the mitigation, the resources needed and timeline to be completion.

3.13 Notes.

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

This section shall contain any general information that aids in understanding the report (e.g., background information, glossary, rationale). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in the report and a list of any terms and definitions needed to understand the report.

3.14 Appendices

Appendices shall provide information published separately for convenience in document maintenance (e.g., charts, classified data, etc.), as necessary. As applicable, each appendix shall be referenced in the main body of the report where the data would normally have been provided. Appendices shall be lettered alphabetically (A, B, etc.).

3.14.1 Requirements Conflicts

Document any contractor proprietary components that were excluded from this report in an appendix, including proposed resolution thereof.

END OF DI-IPSC-82252A

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