DATA ITEM DESCRIPTION

1. DID NUMBER: DID-CM-DATA-CSAR-V5.3

2. TITLE: CONFIGURATION STATUS ACCOUNTING REPORT

3. DESCRIPTION AND INTENDED USE

3.1 The Configuration Status Accounting (CSA) system enables the efficient and effective execution of Configuration Management (CM) functions (ie, CM planning, configuration identification, control of configuration changes and configuration verification and audit). The CSA Report (CSAR), produced from the Contractor's CSA system, provides detailed information to describe the functional requirements and physical characteristics of Configuration Items (CIs), the status of changes to CIs, their associated documentation, and the actual configuration of individual CIs.

3.2 The Contractor uses the CSAR to inform the Commonwealth of the current status of a product (ie, a complete system or CI) and its Product Configuration Information, associated Configuration Baselines, and changes to that product throughout the period of the Contract.

3.3 The Commonwealth uses CSAR information to:

a. understand the current configuration of a product, its Product Configuration Information, and relationship to Configuration Baselines (including system-level baselines), and

b. inform Commonwealth CM activities related to that product throughout its lifecycle.

4. INTER-RELATIONSHIPS

4.1 The CSAR is subordinate to the following data items, where these data items are required under the Contract:

a. Configuration Management Plan (CMP);

b. Systems Engineering Management Plan (SEMP); and

c. Support Services Management Plan (SSMP).

4.2 The CSAR inter-relates with the following data items, where these data items are required under the Contract:

a. all data items derived from the Master Technical Data Index (MTDI) (eg, Support System Technical Data List (SSTDL));

b. Engineering Change Proposal (ECP);

c. Application for a Deviation (AFD); and

d. all data items that form part of a Baseline.

4.3 The CSAR also inter-relates with the Technical Data and Software Rights (TDSR) Schedule.

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

ANSI/EIA-649-C	*National Consensus Standard for Configuration Management*

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The CSAR shall be provided in soft copy format as structured data (eg, one or more databases, spreadsheets or other structured data format) that enables CASR content to be accessed, queried, read, printed and used to generate soft copy tabulated text reports.

6.1.3 Except where the soft copy data file is compatible with a standard Software application defined elsewhere in the Contract, or otherwise agreed in advance and in writing by the Commonwealth Representative, the CSAR shall be accompanied by any software and Technical Data required to enable the functions identified in clause 6.1.2.

6.1.4 ANSI/EIA-649-C provides guidance in relation to Commonwealth expectations for CSA reporting.

6.2 Specific Content

6.2.1 General

6.2.1.1 The CSAR shall be tailored by the governing plan for CM (eg, the Approved CMP) to include the sub-reports and information applicable to the phase of the lifecycle, the scope of the program, the Contract, and the complexity / grade of CM for the Materiel System.

6.2.1.2 The CSAR shall provide accurate, current information, relevant to the end item / CI, derived from the CSA system that is used to store and manage the Product Configuration Information.

6.2.1.3 Where the Contractor has delivered more than one configuration of a CI, the CSAR shall identify all currently approved documentation and the identification numbers for each configuration.

6.2.2 Indentured Item List

6.2.2.1 For each CI, the CSAR shall include, or be able to generate, an Indentured Item List that illustrates the breakdown structure of subordinate CIs, parts, assemblies, sub-assemblies and Software, such that the relationships (eg, where used, next higher assembly) within the product breakdown structure can be clearly understood.

6.2.2.2 The Indentured Item List shall, for each item in the product breakdown structure, include:

a. the configuration identifier / product identifier / Unique Item Identifier (UII);

b. the nature of the CI (ie, system, hardware, software);

c. the manufacturer's Enterprise Identifier (EID) (eg, NATO Commercial and Government Entity (NCAGE/CAGE) code);

d. the manufacturer's reference number / part number for the item;

e. an Effectivity identifier, such as a version number, useable on code or other, used to designate that a CI is useable on one or more higher-level CIs or end items; and

f. the name of the CI, part, component, assembly or Software item, as applicable.

6.2.2.3 The product hierarchy in the Indentured Item List shall be described to a level of detail that provides the Commonwealth with sufficient understanding of the evolving solution and to meet life cycle support concepts, supportability and other goals under the Contract.

6.2.3 Baseline Definitions

6.2.3.1 For each CI, the CSAR shall list the Product Configuration Information associated with the specific baselines relevant to that CI (ie, Functional Baseline (FBL), Product Baseline (PBL), interim product baseline, and other baselines as may be required under the Contract).

6.2.3.2 The Baseline Reports shall include:

a. for each CI:

(i) configuration identifier / product identifier / UII, including version numbers and any special identifiers / usable on codes used to distinguish between parts, assemblies, and software used in the product; and

(ii) the respective Configuration Control Authorities (CCA) and their EID; and

b. for each related configuration document:

(i) document title;

(ii) document number / identifier;

(iii) issue or version number and issue date, as applicable; and

(iv) the document type and, if applicable, sub-type.

6.2.3.3 **Functional Baseline Report**. The CSAR shall include, or be able to generate, Functional Baseline Reports that list the configuration documentation used to define the FBL for each CI including:

a. requirements specifications (functional, interoperability and interface characteristics and design constraints);

b. external interface definition documentation; and

c. agreed Verification documentation required to demonstrate the CI's characteristics.

6.2.3.4 **Product Baseline Report**. The CSAR shall include, or be able to generate, Product Baseline Reports that list the configuration documentation or other information artefacts used to define the PBL for each CI, and which include the following types of documentation:

a. specifications for the system and subordinate CIs, including both hardware and software CIs;

b. interface control documents;

c. engineering and manufacturing drawings and associated lists (eg, bill of materials, wiring lists, assembly drawings, item quantities);

d. design documentation (including, as applicable, software and firmware source code, and system, hardware, software and firmware design documentation);

e. computer aided design, simulation and modelling files;

f. Verification and Validation plans, procedures and reports and Verification Cross Reference Matrices (VCRMs);

g. audit reports, certifications and associated action items;

h. ECPs / Engineering Change Orders (ECOs), and Requests for Variance (RFVs)[1];

i. related Contract Change Proposals (CCPs);

j. operation and maintenance manuals;

k. recommended spares and support and test equipment; and

l. associated Training materials.

6.2.3.5 Configuration documentation for the Product Baseline Report shall be identified to a level of detail commensurate with the expected Defence activities and support strategy for the product.

6.2.4 Master Document Index

6.2.4.1 The CSAR shall include a Master Document Index for each CI (including end items) delivered for Acceptance (as specific or user-selectable filters / views), which includes:

a. a list of all subordinate CIs, including:

(i) the configuration identifier / product identifier / UII;

(ii) their respective CCA and associated EID; and

(iii) their allocated grades of CM;

b. an index of technical documents, including:

(i) specifications, interface control documents, drawings and design documentation;

[1] Note that an Application for a Deviation under the Contract may result in one or more RFVs being required for CM purposes.

(ii) logistics support documents including technical manuals and handbooks; and

(iii) technical manuals and handbooks;

c. the ECP / ECO register;

d. the RFV register (including the 'return to standard' status and due date);

e. the Defect reports; and

f. a list of open action items from the relevant CI audits.

6.2.5 Documents Report

6.2.5.1 The CSAR shall include a Documents Report that, for each configuration document in the CSA system, includes:

a. document number or identifier;

b. document full title;

c. document revision status (eg, draft, final);

d. issue or version number and issue date;

e. document type (eg, specification, drawing, source code) and, as applicable, sub-type (eg, detail assembly drawing, specification control drawing, wiring list);

f. other specific attributes that are relevant to the type of artefact (eg, drawing sizes and number of sheets for a drawing);

g. document media (if held externally);

h. reference to the applicable CI;

i. CDRL reference, if applicable;

j. the Current Document Control Authority (ie, the organisation that is responsible for the document content and the only authority that can effect changes to the document), and associated EID;

k. author / source organisation;

l. a reference to the TDSR Schedule to define any limitation of rights for document distribution and use (eg, associated with Intellectual Property and International Traffic in Arms Regulations); and

m. identification of associated ECOs.

6.2.6 Build Standard Report

6.2.6.1 The CSAR shall include a Build Standard Report that documents the build standards for CIs, and includes:

a. equipment title / CI name;

b. manufacturer's EID and reference number;

c. NATO Stock Number (NSN) / UII, as applicable; and

d. where a modification is applicable to the CI:

(i) ECO number;

(ii) modification number;

(iii) modification title; and

(iv) modification instruction identifier.

6.2.7 Build State Report

6.2.7.1 The CSAR shall include a Build State Report that documents the status of individual CIs, as delivered, including details of engineering changes, Deviations / variances, and relevant maintenance actions, and that includes:

a. equipment title / CI name;

b. manufacturer's EID, reference number, and serial number for rotable items;

c. NSN and UII, as applicable;

d. where a modification has been applied to the CI:

  (i) the ECO number / RFV number / modification instruction identifier;

  (ii) date modification completed; and

  (iii) modification strike number / dash number; and

e. for any rotables that were replaced during maintenance, prior to delivery, the reference / part number and serial number of those items.

6.2.8 ECP / ECO and RFV Reports

6.2.8.1 The CSAR shall include the current list of ECPs / ECOs and RFVs (if applicable), from the applicable register presented in dedicated ECP / ECO and RFV views, which include:

a. ECP / ECO / RFV number;

b. ECP / ECO / RFV title / short description;

c. where applicable, any parent AFD;

d. configuration identifier / product identifier / UII for the applicable CI;

e. change classification (ie, major, minor, administrative or RFV);

f. implementation status (eg, preliminary, CCB approved, issued, current effectivity / partial installation status, or closed); and

g. status date.

6.2.9 Defects Report

6.2.9.1 The CSAR shall include a Defects Report, which references all Defect reports for each CI, and for each Defect includes:

a. the configuration identifier / product identifier / UII for the applicable CI;

b. CI name;

c. Defect number;

d. Defect categorisation (eg, critical, major, minor);

e. if applicable, the RFV number; and

f. if resolved by a configuration / engineering change, the ECP / ECO number.

6.2.10 Action Item Report

6.2.10.1 The CSAR shall include an Action Item Report that lists all action items resulting from configuration audits, CCBs or ICWGs, which for each action item includes:

a. the configuration identifier / product identifier / UII for the applicable CI;

b. CI name;

c. the audit type / CCB / ICWG details;

d. action item number;

e. action item description;

f. date the action item was established;

g. if applicable, the contractual or specification requirement that is affected;

h. action item owner;

i. status / closure details; and

j. date for completion / date closed.

6.2.11 CSA Metrics Report

6.2.11.1 The CSAR shall include a Metrics Report that reports on measures for the execution of the Contractor's CM process and functions (eg, number and status of ECP / RFVs, processing times, and rates of closure of change documentation).

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-CM-DATA-XDATA-V5.3

2. TITLE: CONTRACTOR-DEFENCE CM DATA EXCHANGE SCHEMA

3. DESCRIPTION AND INTENDED USE

Note to drafters: If included, this DID is to be developed to meet the specific needs of the project / program. The DID should be as complete as practicable for inclusion in the RFT. If the DID cannot be finalised before the RFT, drafters should include a 'Note to tenderers' to identify the information requirements that are to be completed with the preferred tenderer / Contractor.

The complexity of the Materiel System, maturity of Commonwealth and Contractor CSA Systems, and Commonwealth requirements to access CM data to inform contract activities, will determine the optimum method by which CSA data is transferred from Contractor to Commonwealth. Refer to CASG Handbook (E&T) 12-2-002, CM Guide, which shows possible transfer methods - this DID is applicable to 'Method C' only. Use of this DID requires inclusion of the corresponding 'optional' clause in the SOW for the exchange of CSA data and related details in the CDRL.

The following note refers to the roll-out of the Defence ERP System with applicable CM functionality as part of the Enterprise Asset Management (EAM) framework. The Defence ERP System will release CM functionality for different domains (Land, Sea, Air) at different times, which may occur before or after the ED of any resultant Contract, and thus require changes to this DID before or after ED. If the applicable ERP 'Interface Development Specification' for 'Contractor Information Exchange' is finalised (eg, for uXLoader and OpenText Object Importer), and this DID is updated before ED, then the note below may also be deleted. Drafters may need to amend the note below as additional information becomes available from the ERP program.

Note: The Defence Enterprise Resource Planning (ERP) System will replace existing Defence information systems, over a number of years. If a Defence ERP solution for CM / CSA is not released prior to the start of the Contract, the subsequent introduction of these functions may require changes to the deliverable data formats developed in accordance with this DID.

3.1 Data transfer between Contractor and Defence Configuration Management (CM) Information Systems is an integral part of the Defence-Contractor interaction. This CM Data Exchange Schema defines how the Contractor is to apply EIA836B to realise an effective Configuration Status Accounting (CSA) data transfer capability. CSA data, produced from the Contractor's CSA system, and transferred in accordance with this DID, provides detailed information to describe the functional requirements and physical characteristics of Configuration Items (CIs), the status of changes to CIs, their associated documentation, and the actual configuration of individual CIs.

3.2 The Contractor uses the transferred CSA data to inform the Commonwealth of the current status of a product (ie, a complete system or CI) and its Product Configuration Information, associated Configuration Baselines, and changes to that product throughout the duration of the Contract.

3.3 The Commonwealth uses the transferred CSA data to:

a. understand the current configuration of a product, its Product Configuration Information, and relationship to Configuration Baselines (including system-level baselines); and

b. inform Commonwealth CM activities related to that product throughout its lifecycle.

4. INTER-RELATIONSHIPS

4.1 The Contractor-Defence CM Data Exchange Schema is subordinate to the following data items, where these data items are required under the Contract:

a. Configuration Management Plan (CMP);

b. Systems Engineering Management Plan (SEMP); and

c. Contractor Engineering Management Plan (CEMP).

4.2 The Contractor-Defence CM Data Exchange Schema inter-relates with the CSA Report.

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

EIA836B	Configuration Management Data Exchange and Interoperability
DEF(AUST)10814	Land Materiel Data Exchange Standard
ANP4422-6001	Materiel Data Exchange Specification
EAMI 152 & 153	Defence ERP Program Interface Development Specification - Contractor Information Exchange

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’ in the Statement of Work.

6.2 Specific Content

6.2.1 Exchange of CSA data shall conform to:

Note to drafters: Insert the exchange standards to be specified here.

a. DEF(AUST) 10814, Land Materiel Data Exchange Standard;

b. ANP4422-6001, Materiel Data Exchange Specification;

c. EAMI 152 & 153, Defence ERP Program Interface Development Specification - Contractor Information Exchange, and

d. [...DRAFTER TO INSERT...].

Note to drafters: If applicable, this section may need to include any additional specific physical or electronic transfer arrangements for transfer of CSA data in accordance with the applicable standard.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-CM-MGT-CMP-V5.3

2. TITLE: CONFIGURATION MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Configuration Management (CM) Plan (CMP) is the overarching plan for the management and implementation of CM for the Contract. The CMP defines the Contractor's methodologies, systems and processes for meeting the CM requirements of the Contract. The CMP includes the definition of CM activities for all hardware, Software and data (including all data items) associated with the Contract.

3.2 The Contractor uses the CMP to:

a. define, manage and monitor the CM program for the Contract;

b. ensure that those parties (including Subcontractors) who are undertaking CM activities understand their respective responsibilities, the processes to be used, and the time-frames involved; and

c. define the Contractor's expectations for Commonwealth involvement in the provision of CM activities.

3.3 The Commonwealth uses the CMP to:

a. gain visibility into the Contractor's planning for meeting the CM requirements of the Contract;

b. gain assurance that the Contractor's CM activities will meet the requirements of the Contract;

c. provide a basis for monitoring and assessing the Contractor's performance in relation to the CM requirements of the Contract;

d. confirm and coordinate Commonwealth interfaces with the Contractor's CM program; and

e. provide input into the Commonwealth's planning.

4. INTER-RELATIONSHIPS

4.1 The CMP is subordinate to the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP); or

b. Support Services Management Plan (SSMP).

4.2 The CMP inter-relates with the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Software Management Plan (SWMP);

c. Integrated Support Plan (ISP);

d. System Review Plan (SRP);

e. Verification and Validation Plan (V&VP);

f. Quality Plan (QP); and

g. Mission System Technical Documentation Tree.

5. APPLICABLE DOCUMENTS

5.1 The following data items form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Configuration Management Organisation

6.2.1.1 The CMP shall describe the CM organisation for the Contract, including:

a. the functional structure of the Contractor's and Approved Subcontractors' CM organisation;

b. lines of authority within the CM organisation and between the CM and engineering and project management organisations;

c. details of the formal links between the Contractor's CM organisation and Subcontractors; and

d. the responsibilities and authority of participating groups, organisations and individuals involved in CM, including their role in Configuration Control Boards (CCBs) and Interface Control Working Groups (ICWGs).

6.2.2 Configuration Management Integration

6.2.2.1 The CMP shall:

a. identify and detail the integration of CM functions with other Contract activities;

b. detail the Commonwealth's involvement and responsibilities in the Contractor's CM process, including the Commonwealth's involvement in CCBs and ICWGs;

c. the integration of Approved Subcontractors' activities with the Contractor's activities to achieve the CM requirements of the Contract; and

d. describe the integration of CM functions with other Contract activities, such as System Reviews.

6.2.3 Configuration Management Phasing and Milestones

6.2.3.1 The CMP shall describe and graphically portray the sequence of events and milestones for implementation of CM in phase with major Milestones and events. Where possible, this shall be done by cross-referencing to the applicable document (eg, the SRP). Events should include:

a. the release and submission of Configuration Documentation in relation to Contract events (eg, System Reviews);

b. the establishment of internal developmental configuration and contractual baselines;

c. the implementation of internal and Commonwealth configuration control;

d. the establishment of CCBs and ICWGs;

e. the implementation of the Configuration Status Accounting (CSA) system; and

f. the conduct of configuration audits.

6.2.4 Data Management

6.2.4.1 Specification Tree and Configuration Item List

6.2.4.1.1 The CMP shall define the relationship between the specification tree, as captured in the Mission System Technical Documentation Tree, and the Configuration Item (CI) list, and define how these will be managed.

6.2.4.2 Document Management

6.2.4.2.1 The CMP shall define the process and procedures to be used for managing the documentation required for the conduct of the Contract, including both formal deliverables and internal Contractor and Subcontractor documentation.

6.2.4.3 Drawing Management

6.2.4.3.1 The CMP shall define the process and procedures to be used for managing the engineering drawings and shall include:

a. identification of the engineering drawing practices standard used both by the Contractor and Subcontractors;

b. a statement of any need for deviation from the content of this standard during the program; and

c. an overview of the drawing management system including:

(i) a description of any information system tools used (eg, drawing management database) to support the drawing management system; and

(ii) a definition of the drawing procedures to be used.

6.2.5 Configuration Identification

6.2.5.1 Selection of Configuration Items

6.2.5.1.1 The CMP shall define the procedures for the selection of CIs, and detail the criteria used for their selection. The CMP shall, by inclusion or reference, define the list of CIs and their respective specifications and other defining top-level documentation.

6.2.5.2 Configuration Identifiers

6.2.5.2.1 The CMP shall define the procedures for assignment and physical marking of configuration identifiers, including:

a. document numbers and revision markings to documentation;

b. nomenclature, serial numbers and part numbers to hardware; and

c. software identifiers to software and firmware.

6.2.5.3 Developmental Configuration

6.2.5.3.1 The CMP shall define the procedures for establishing and controlling the documentation and repositories containing the elements of the developmental configuration, including:

a. the procedures for reporting, processing, tracking, rectifying and recording problems identified in the documentation defining the developmental configuration; and

b. the procedures for the establishment and control of a documentation library, drawing library and software development library.

6.2.5.4 Configuration Baselines

6.2.5.4.1 The CMP shall define the requirements for establishing Configuration Baselines, and include:

a. the procedures for the establishment of, at least, the Functional, Allocated and Product Baselines; and

b. the documentation to be used to define each Configuration Baseline.

6.2.5.5 Engineering Release

6.2.5.5.1 The CMP shall define the procedures for issuing approved configuration documentation, and amendments to this documentation, to functional activities (eg, manufacturing, logistics, and acquisition) within the Contractor's organisation.

6.2.5.6 Configuration Control

6.2.5.6.1 The CMP shall define and detail the functions, membership, responsibilities and authority of the CCBs planned for the Contract.

6.2.5.6.2 The CMP shall define the procedures, including Commonwealth involvement, and associated documentation for processing the following:

a. classification of changes, and the level of authority for change approval / concurrence;

b. Contract Change Proposals (CCPs);

c. Major Changes;

d. Minor Changes;

e. Applications for a Deviation (and related requests for variance, if applicable);

f. Advance Change Study Notices; and

g. Specification Change Notices.

6.2.6 Configuration Status Accounting

6.2.6.1 The CMP shall define the procedures for CSA, including:

a. methods for collecting, recording, processing and maintaining the data required to provide the status of accounting information through reports and / or access to a CSA system;

b. a complete description of the CSA system with respect to the areas related to:

(i) the identification of the currently approved configuration documentation and configuration identifiers associated with each CI;

(ii) the status of proposed engineering changes from initiation to implementation;

(iii) the results of configuration audits, and the status and disposition of discrepancies;

(iv) the status of Applications for a Deviation;

(v) the ability to trace changes from the baseline documentation of each CI; and

(vi) the effectiveness and installation status of configuration changes to all CIs at all locations;

c. the relationships between the CSA system held by the Contractor and the CSA systems held by applicable Approved Subcontractors (which may be or may represent respective Original Equipment Manufacturers (OEMs)) for each of the CIs, including:

(i) identifying where the master CSA system for the Mission System, or the major elements thereof, will reside (ie, the system or systems that hold the master data);

(ii) if the master CSA system is not held by the Contractor, describing how the CSA systems will interact and interrelate, firstly, to satisfy the requirements of the Contract (eg, to ensure that the data held by the Contractor is always current) and, secondly, to undertake any future upgrades of the Mission System over its life; and

(iii) describing the scope boundaries between the CSA system held by the Contractor and the CSA systems held by the applicable Approved Subcontractors; and

d. identification and description of the reports available from the CSA system and their frequency of reporting and distribution.

6.2.7 Configuration Audits

6.2.7.1 If an SRP is not required under the Contract, the CMP shall:

a. describe the Contractor's methodology and processes to establish and conduct Functional Configuration Audits (FCAs) and Physical Configuration Audits (PCAs);

b. detail, for each audit, the proposed audit venue(s) and the details of the organisation(s) and individuals involved in the audits and their specific audit responsibilities;

c. define entry criteria, exit criteria and checklist items for each FCA and PCA, incorporating the associated SOW requirements (eg, as may be included in Mandated System Review checklists for FCA and PCA, respectively) and supplemented where required by the Contractor's internal processes;

d. describe the plans, procedures, documentation, and schedules for the audits; and

e. describe the format for reporting results of in-process audits.

6.2.7.2 If an SRP is required under the Contract, the CMP shall summarise the information contained in the SRP regarding FCA and PCA, and provide any additional information in the CMP necessary to address the information requirements defined under clause 6.2.7.1.

6.2.8 Subcontractor Control

6.2.8.1 The CMP shall define the methods used to ensure that Approved Subcontractors comply with the CM requirements of the Contract.

6.2.9 Master Record Indexes

6.2.9.1 If required under the Contract, the CMP shall define the production and management of Master Record Indexes, including schedule, organisational responsibilities, and maintenance.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-CM-MGT-ECP-V5.3

2. TITLE: ENGINEERING CHANGE PROPOSAL

3. DESCRIPTION AND INTENDED USE

3.1 An Engineering Change Proposal (ECP), including as a software-only change defined in a Software Change Proposal (SWCP), is required to enable the proposal, review and assessment of, and the engineering management and control of changes to the existing design configuration of hardware and/or software.

3.2 The Contractor and the Commonwealth use the ECP (including the SWCP) as the common basis for defining the requirements, significance, approvals and scope of changes to the existing Functional Baseline and/or Product Baseline of the Materiel System and, if applicable, proposed changes to interfacing systems.

4. INTER-RELATIONSHIPS

4.1 Each ECP inter-relates with the following data items, where these data items are required under the Contract:

a. Contractor Engineering Management Plan (CEMP);

b. Configuration Management Plan (CMP);

c. Software Management Plan (SWMP); and

d. Software Support Plan (SWSP).

5. APPLICABLE DOCUMENTS

Note to drafters: Amend the following lists for the ADF regulatory / assurance framework to be referenced from the ECP form(s) annexed to this DID.

5.1 The following documents form a part of this DID to the extent specified herein:

AAP 8000.011	Defence Aviation Safety Regulations (DASR)
ANP3411-0101	Navy Materiel Assurance Publication
LMSM	Land Materiel Safety Manual

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.2 Specific Content

6.2.1 Specific Requirements

Note to drafters: Insert additional references below as required (eg, Configuration Management manual or software standard, as appropriate), noting that the CEMP, CMP, SWMP and/or SWSP that are used to tailor the application of manuals / standards are already applied through clause 4 (above) and the inclusion of ‘Contract’ in the clause below. Attach the applicable ECP and SWCP forms as annexes to this DID.

6.2.1.1 All engineering design and configuration change proposals shall be documented using the ECP form at Annex A, and in accordance with the Contract and:

a. [...INSERT REFERENCE...]; and

b. [...INSERT REFERENCE...].

Note to drafters: If including a separate SWCP, then retain and amend the clause below; otherwise, it may be deleted (as should reference to Annex B below). Insert additional references below as required (eg, software standards, as appropriate), noting that the CEMP, CMP, SWMP and/or SWSP that tailor the application of manuals / standards are already applied through clause 4 (above) and the inclusion of 'Contract' in the clause below. Attach the applicable SWCP form as an annex to this DID.

6.2.1.2 All software-only design and configuration change proposals shall be documented using the SWCP form at Annex B, and in accordance with the Contract and:

a. [...INSERT REFERENCE...]; and

b. [...INSERT REFERENCE...].

6.3 Annexes

Note to drafters: Include applicable forms as Annexes.

A. Engineering Change Proposal form

B. Software Change Proposal form

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-AEOA-V5.2

2. TITLE: APPLICATION FOR ENGINEERING ORGANISATION APPROVAL

3. DESCRIPTION AND INTENDED USE

3.1 The Application for Engineering Organisation Approval (AEOA) is a formal submission by the Contractor, to the Commonwealth, to demonstrate that it has the means to perform engineering activities that comply with specified ADF regulatory / assurance framework requirements.

3.2 The Contractor uses the AEOA to seek formal recognition of its engineering organisation by submitting evidence that the Contractor:

a. can, and will, sustain an engineering organisation that complies with the specified ADF regulatory / assurance framework requirements, to the extent that they apply to the engineering activities required under the Contract; and

b. will undertake the required engineering activities to approved standards, using competent and authorised individuals, who are acting as members of the complying engineering organisation.

3.3 The Commonwealth uses the AEOA, to assess the Contractor's capability and readiness to apply the specified ADF regulatory / assurance framework requirements to the engineering activities required under the Contract.

4. INTER-RELATIONSHIPS

4.1 The AEOA inter-relates with the following data items, where these data items are required under the Contract:

a. Contractor Engineering Management Plan (CEMP);

b. Systems Engineering Management Plan (SEMP); and

c. Configuration Management Plan (CMP).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

AAP 8000.011	Defence Aviation Safety Regulations (DASR)
ANP3411-0101	Naval Materiel Assurance Publication
LMSM	Land Materiel Safety Manual

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 When the Contract has specified delivery of other data items that contains aspects of the required information, the AEOA shall summarise these aspects and refer to the other data items.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.1.4 All documents provided as part of the AEOA shall be controlled documents.

6.2 Specific Content

6.2.1 Aerospace - Application for Design / Production Organisation Approval

6.2.1.1 Where the Contractor is required to comply with the DASR, as applicable to the scope of work under the Contract, the AEOA shall include:

a. for design activities, a completed *DASR Form 80 - Application for Military Design Organisation Approval*, supported by a *Design Organisation Exposition* (DOE) addressing the requirements of DASR 21.A.243; and/or

b. for production activities, a completed *DASR Form 50 - Application for DASR 21 Production Organisation Approval*, supported by a *Production Organisation Exposition* (POE) addressing the requirements of DASR 21.A.143.

6.2.1.2 In meeting the requirements of clause 6.2.1.1 the AEOA shall, except where provided to the Commonwealth by other means, include the CEMP, SEMP and CMP, as applicable, and all other plans, procedures, and other documents referenced in the DOE and/or POE, as applicable.

6.2.2 Land - Application to demonstrate compliance with the LMSM

6.2.2.1 Where the Contractor is required to show compliance with the LMSM, as applicable to the scope of work under the Contract, the AEOA shall:

a. be released under the authority of the Contractor’s Senior Design Engineer for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the engineering management systems, competent people, processes, data and other resources required to provide engineering management and design services consistent with applicable LMSM requirements identified in the Contract;

c. except where provided to the Commonwealth by other means, include the CEMP, SEMP and CMP, as applicable, and all other plans, procedures and related documents containing the objective quality evidence required by clause 6.2.2.1b; and

d. include a compliance matrix, showing how the Contractor’s engineering management system complies with LMSM requirements applicable to the engineering activities under the Contract.

6.2.3 Maritime – Application to demonstrate compliance with the Naval Materiel Assurance Publication

6.2.3.1 Where the Contractor is required to comply with the *Naval Materiel Assurance Publication*, as applicable to the scope of work under the Contract, the AEOA shall:

a. be released under the authority of the Contractor’s Senior Design Engineer for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the engineering management systems, competent people, processes, data and other resources required to provide engineering management and design services in accordance with *Naval Materiel Assurance Publication* requirements (refer to ANP3411-0101 Chapter 6, paragraphs 6.24 and 6.28);

c. except where provided to the Commonwealth by other means, include the CEMP, SEMP and CMP, as applicable, and all other plans, procedures and related documents containing the objective quality evidence required by clause 6.2.3.1b; and

d. include a compliance matrix showing how the Contractor’s engineering management system complies with *Naval Materiel Assurance Publication* requirements applicable to the engineering activities under the Contract.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-DEF-SS-V5.3

2. TITLE: SYSTEM SPECIFICATION

3. DESCRIPTION AND INTENDED USE

3.1 The System Specification (SS) defines the validated requirements for the Mission System. Unless otherwise specified in the Contract, a separate SS is required for each Mission System defined in the Contract.

3.2 The Contractor and the Commonwealth use the SS as the basis for common understanding of the technical requirements for the Mission System.

4. INTER-RELATIONSHIPS

4.1 The SS inter-relates with the following data items, where these data items are required under the Contract:

a. Support System Specification (SSSPEC);

b. Requirements Traceability Matrix (RTM); and

c. Verification Cross Reference Matrix (VCRM).

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

DI-IPSC-81431A	System/Subsystem Specification (SSS)

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 The specific SS content shall be in accordance with DI-IPSC-81431A, section 4, *Content Requirements*.

6.2.2 If the Contract requires a VCRM, DI-IPSC-81431A *Qualification Provisions* should be provided by reference to the VCRM.

6.2.3 If the Contract requires a RTM, DI-IPSC-81431A *Requirements traceability* should be provided by reference to the RTM.

DATA ITEM DESCRIPTION

1. **DID NUMBER:** **DID-ENG-DES-HEPR-V5.3**

2. **TITLE:** **HUMAN ENGINEERING PROGRAM REPORT**

3. DESCRIPTION AND INTENDED USE

3.1 The Human Engineering Program Report (HEPR) describes the activities undertaken within the Contractor's Human Engineering (HE) Program, identifies its elements, and describes how the outcomes address the SOW requirements.

3.2 The Contractor uses the HEPR to present progress on the elements of the HE program up to Final Acceptance.

3.3 The Commonwealth uses the HEPR to monitor progress of the HE program and assess its ability to meet the SOW objectives up to Final Acceptance.

4. INTER-RELATIONSHIPS

4.1 The HEPR is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP); and

b. Integrated Support Plan (ISP).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

MIL-STD-1472G	*Human Engineering*
MIL-HDBK-46855A	*Human Engineering Program, Process and Procedures*

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 The HEPR shall describe the activities undertaken within the Contractor's HE Program, and describe how the outcomes address the Contract requirements. The activities described shall include:

a. Subcontractor activities,

b. systems analysis,

c. equipment design,

d. equipment procedure development,

e. Personnel and Training requirements, and

f. Verification and Validation.

6.2.2 The HEPR shall identify:

a. the agreed tailoring of MIL-HDBK-46855 or an equivalent standard Approved by the Commonwealth Representative; and

b. the agreed tailoring of MIL-STD-1472 or an equivalent standard Approved by the Commonwealth Representative.

6.2.3 Any agreed tailoring shall identify specific provisions by paragraph, rationale, for tailoring and effects of tailoring on the HE program. If no tailoring is applied beyond that specified in the SOW, then this shall be stated.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-HW-DWGS-V5.3

2. TITLE: ENGINEERING DRAWINGS

3. DESCRIPTION AND INTENDED USE

3.1 In this DID, '*Engineering Drawings*' refers to Engineering Design Data for hardware products of the Materiel System, including technical drawings and data sets (eg, three-dimensional modelling and computer-aided design data). Engineering Drawings include design and production drawings and/or data sets for the applicable item(s) / system(s), as identified in the Approved Drawing List.

3.2 The Contractor uses the Engineering Drawings as part of the definition of the Product Baseline(s) for the applicable item(s) / system(s).

3.3 The Commonwealth uses the Engineering Drawings to:

a. confirm the current state of the applicable item / system, including when the item / system is being offered for Acceptance;

b. accurately define the interfaces to external systems; and

c. enable the applicable system / item to be supported over its Life-of-Type.

4. INTER-RELATIONSHIPS

4.1 The Engineering Drawings are subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Integrated Support Plan (ISP);

c. Technical Data Plan (TDP); and

d. Configuration Management Plan (CMP).

4.2 The Engineering Drawings inter-relate with the following data items, where these data items are required under the Contract:

a. Drawing List;

b. Mission System Technical Documentation Tree (MSTDT);

c. publications (including interactive electronic technical publications) and Training Materials (including Computer Based Training (CBT)) that contain or refer to the Engineering Drawings; and

d. Support System Technical Data List (SSTDL).

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

DEF(AUST)CMTD-5085C	Engineering Design Data for Defence Materiel

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall not comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.2 Specific Content

6.2.1 Engineering Drawings

6.2.1.1 Unless otherwise specified by the SOW or in the Approved governing plan for Technical Data under the Contract (ie, the Approved TDP or Approved ISP), the Engineering

Drawings shall consist of Level 3 drawings as defined by DEF(AUST)CMTD-5085C (as applicable to the type of Engineering Drawing).

6.2.1.2 All Engineering Drawings, associated lists and other design records shall be prepared, amended and managed in accordance with the requirements of DEF(AUST)CMTD-5085C (or equivalent specification in the Approved governing plan for Technical Data under the Contract) and the Approved governing plan for Configuration Management under the Contract (eg, CMP or SEMP).

6.2.1.3 Unless otherwise specified in the SOW, all Engineering Drawings shall be delivered in the formats defined in the Approved governing plan for Technical Data under the Contract (ie, the Approved TDP or Approved ISP) or as otherwise defined in the Approved Drawings List.

6.2.1.4 Configuration Control details for Engineering Drawings (eg, amendment status) shall be in accordance with the Approved governing plan for Configuration Management under the Contract.

6.2.1.5 The Engineering Drawings to be delivered shall include all drawings identified in the Approved Drawing List for the applicable delivery (eg, for a Mandated System Review or System Acceptance Milestone).

6.2.2 Interpretation Document

6.2.2.1 An interpretation document shall be provided for each Contractor and Subcontractor drawing system in accordance with DEF(AUST)CMTD-5085C (or equivalent specification in the Approved governing plan for Technical Data under the Contract). Each interpretation document shall include:

a. information to facilitate interpretation of the drawing and part number structure including the standards used; and

b. an explanation of symbology pertaining to notes, revision markers and effectivity annotations.

6.2.3 Associated Lists

6.2.3.1 Associated lists shall be prepared in accordance with DEF(AUST)CMTD-5085C (or equivalent specification in the Approved governing plan for Technical Data under the Contract) and provided in electronic format.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-MGT-MSSMP-V5.3

2. TITLE: MATERIEL SYSTEM SECURITY MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Materiel System Security Management Plan (MSSMP) describes the Contractor’s strategy, methodology, processes and tools for achieving the system security requirements of the Contract, particularly the Security Outcomes, including in relation to each different type of Security Authorisation. System security addresses, as applicable, physical security, Emanation Security (EMSEC), Information and Communications Technology (ICT) security and cyber security as they apply to each Security System-of-Interest (SSoI) (eg, the Mission System). For ICT/cyber security, this includes the Digitally Enabled Systems and Equipment (DESE) within each SSoI.

3.2 The Contractor uses the MSSMP to:

a. define, manage and monitor the Contractor’s system security and related activities under the Contract;

b. describe how the objectives of, and requirements for, the system security program set out in the SOW will be achieved for each SSoI;

c. ensure that those parties (including the Commonwealth and Subcontractors) performing system security activities understand their respective responsibilities, the processes to be used, and the time-frames involved; and

d. ensure that risks to achieving the system security requirements are recognised and appropriately managed for all SSoIs.

3.3 The Commonwealth uses the MSSMP to:

a. understand and evaluate the security-related design and management processes used by the Contractor, including in relation to design trade-offs both within and between SSoIs;

b. assist with ensuring consistency and coherency across the system security program for the set of SSoIs;

c. gain assurance that the Contractor’s design activities will satisfy the objectives of the system security program set out in the SOW and deliver Supplies that meet the system security requirements and enable the required Security Authorisations to be achieved;

d. provide a basis to monitor the progress of the development of the security design for a SSoI against the planned schedule;

e. help to identify issues of concern that could prevent the achievement of the required performance in relation to system security for a SSoI, and which need to be raised with the Contractor; and

f. as an input into the Commonwealth’s own planning, particularly in relation to liaising with the applicable Security Authorisation authorities.

4. INTER-RELATIONSHIPS

4.1 The MSSMP is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Integrated Support Plan (ISP);

c. Configuration Management Plan (CMP); and

d. Quality Plan.

4.2 The MSSMP inter-relates with the following data items, where these data items are required under the Contract:

a. System Specification (SS) (for each different type of Mission System);

b. Support System Specification (SSSPEC);

c. System Architecture Description (SAD);

d. the security-related data items required under the Contract (other than those identified under clause 4.1);

e. the Software-related data items required under the Contract;

f. Mission System Technical Documentation Tree (MSTDT);

g. Support System Technical Data List (SSTDL);

h. ADF regulatory / assurance plans;

i. Certification Plan (CERTP);

j. Electromagnetic Environmental Effects Management Plan (E3MP);

k. System Safety Program Plan (SSPP);

l. Disposal Plan (DISP);

m. Verification and Validation Plan (V&VP); and

n. Verification Cross Reference Matrix (VCRM).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Note to drafters: Amend the list of Applicable Documents to suit the Contract. Do not include documents that are included within the 'Governing Security Documents'.

Governing Security Documents	(see the Glossary for the definition of this term)
ANP4605	Navy Cyberworthiness
AFSMAN	Air Force Security Manual, Volume 1
	National Institute of Standards and Technology (NIST), 'Cybersecurity Framework (CSF)', Version 2.0, February 26, 2024
AS/NZS ISO 31000:2018	Risk Management – Principles and Guidelines
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1, September 2012
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018
NIST SP 800-53A	Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5, January 2022
	ACSC Publication, 'Strategies to Mitigate Cyber Security Incidents', February 2017
	ACSC Publication, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', February 2017
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection – Information security management systems – Requirements
ISO/IEC 27032:2023	Cybersecurity – Guidelines for internet security

ISA/IEC 62443 series	Security for Industrial Automation and Control Systems
ISO/IEC 27005:2022	Information security, cybersecurity and privacy protection – Guidance on managing information security risks
Defence ICT/Cyber SCRM Framework	The Defence ICT/Cyber Procurement Supply Chain Risk Management Framework, October 2020
	CASG Risk Management Product Risk Matrix

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the MSSMP should summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Overview

6.2.1.1 The MSSMP shall provide an overview of the Contractor’s system security program for the Contract, including:

a. defining the scope and purpose of the MSSMP, including:

(i) summarising the system security requirements of the SOW, including setting out the objectives of the system security program and identifying the requirements for the different types of Security Authorisations; and

(ii) describing the relationships to higher-level plans (eg, the plans identified at clause 4.1) and to relevant plans at the same level (eg, management plans for interfacing domains);

b. identifying and describing the nature and significance of the security risks and threats that will be managed through the MSSMP; and

c. describing any constraints, assumptions and risks associated with the program.

6.2.1.2 The MSSMP shall provide a list of key stakeholders involved with the Contractor’s system security program, including:

a. System Owner;

b. security requirements authorities;

c. Security Authorisation authorities; and

d. for projects involving integration into, or installation onto, Defence systems and platforms, the in-service agencies responsible for managing and supporting those systems and platforms.

Note: In responding to the following clause, the Contractor’s attention is drawn to the definitions of ‘Security System of Interest’ and ‘Target of Security Assessment’ set out in the Glossary, including the relationships between them.

6.2.1.3 The MSSMP shall provide an overview of each SSoI, including:

a. identifying the Targets of Security Assessment (ToSAs) within each SSoI where applicable;

b. identifying where ICT security and/or cyber security are applicable to the SSoI; and

c. identifying and briefly describing any significant items of DESE from an ICT security or cyber security perspective.

Note: In responding to the following clause, the Contractor may propose a set of ICT/cyber security-related data items, which are mapped to the identified ToSAs. For the different SSoIs and the ToSAs within larger Mission Systems (eg, aircraft or ship), it may be more appropriate to develop and deliver the required ICT/cyber security documentation progressively as long as the overall requirement in the CDRL for each data item is achieved.

6.2.1.4 The MSSMP shall provide the Contractor's mapping of the security-related data items in the CDRL to the SSoIs and ToSAs, showing how the data item requirements in the CDRL will be met.

6.2.2 Requirements

6.2.2.1 The MSSMP shall provide an overview of the technical requirements that must be met in relation to system security for each SSoI/ToSA (eg, as set out in Legislation, the Governing Security Documents and the FPS and/or each Mission System SS and the SSSPEC) and any inter-relationships with relevant Defence and government policies.

6.2.3 Organisation and Communication

6.2.3.1 The MSSMP shall describe the system security organisation(s) within the Contractor's overall organisation, including:

a. details of the Contractor's security team that is dedicated to the Contract, including numbers and skills;

b. specifically in relation to ICT/cyber security, how the necessary skills will be identified, obtained and retained over the period of the Contract;

c. a description of the relationships to any other areas within the Contractor's organisation that are involved with or support the Contractor's system security program; and

d. whether or not Subcontractors will be incorporated into the program and, if so, the details of the Subcontractors, including the nature and scope of the work to be undertaken.

6.2.3.2 The MSSMP shall describe any Integrated Product Team (IPT) arrangements for the Contractor's system security program, including membership, leadership and terms of reference.

6.2.3.3 The MSSMP shall describe how the Contractor will work with Subcontractors to ensure that they provide goods that are suitable to meet the security requirements of the Contract.

6.2.4 Security Risk Management

6.2.4.1 The MSSMP shall describe the risk management processes to be applied to the Contractor's system security program, cross-referring to the risk-management elements of the Approved Project Management Plan (PMP) and the applicable elements of the Approved ADF regulatory / assurance plans as appropriate, including:

a. the processes to be used to identify system security risks, including:

(i) conducting a security threat and risk assessment, including in relation to any classified threats associated with the operation and support of the SSoIs;

(ii) if a SAD is required under the Contract, utilising the system architecture modelling processes and practices;

(iii) undertaking specific activities in relation to ICT/cyber security, such as performing threat modelling, penetration testing, and mapping the cyber attack and engagement surfaces; and

(iv) ensuring that the set of security-related risks remains current, particularly in relation to ICT/cyber security;

Note to drafters: The following clause refers to the CASG Risk Management Product Matrix, which is identified as an Applicable Document in clause 5. This enables a 5x5 matrix to be employed for the purposes of project or product risk management using the Predict! tool. The Security Authorisation process, however, requires the use of a 6x6 matrix in accordance with the DSPF. Drafters should amend the following clause and the Applicable Documents to suit their contract-management circumstances (ie, to select the risk matrix that will result in the least

work for the contract-management team, either translating into the DSPF 6x6 matrix if the CASG matrix is retained, or translating into Predict! if the following clause is amended to incorporate the DSPF matrix).

b. the processes to be used for analysing, assessing and evaluating system security risks, including the specific assessment criteria to be used, cross-referring to the CASG Risk Management Product Risk Matrix in relation to assessing risks to ‘Security & Cyber’;

c. the risk register(s) to be used for recording each system security risk (eg, SRMP), including its attributes, evaluation and treatment(s);

d. the processes to be used to determine the specific risk treatment strategies to be employed, particularly the application of risk controls (eg, as per the ISM and other applicable standards for ICT/cyber security); and

e. the mechanisms to be used to keep the Commonwealth apprised of system security risks.

6.2.5 System Security Design Processes

6.2.5.1 The MSSMP shall describe the Contractor’s design processes for achieving the security requirements of the Contract, including:

a. the strategy and methodology to meet the system security objectives defined in the SOW and satisfy the security requirements of the Contract, including as set out in the relevant specifications (eg, FPS/SS/SSSPEC) for each SSoI;

b. the outcomes to be achieved and the expected level of design maturity at each of the Mandated System Review (MSRs), where MSRs are applicable to a SSoI;

c. the documentation to be produced during each stage of development for each SSoI/ToSA and each security domain, cross-referring to the response to clause 6.2.1.4 and the MSTDT and/or SSTDL, as appropriate;

d. the approach, methods, and activities to synthesise security into the design solution for each SSoI/ToSA (for system architecture, Software and hardware), including:

(i) utilisation of system architecture modelling activities, including co-ordination with the Commonwealth through the SAD;

(ii) analysis of threats and vulnerabilities;

(iii) implementation of system security controls and response mechanisms;

(iv) the application of design criteria, including the selected security strategies governing the use of Commercial-Off-The-Shelf (COTS), developmental and non-developmental items (particularly DESE), open systems architecture and re-use technologies;

(v) for Software (including firmware), the utilisation of secure systems development processes and practices (eg, reducing attack surfaces, securing code, testing code for vulnerabilities, Cyber Supply Chain considerations, and application of the Contractor’s Quality Management System (QMS) to provide assurance);

(vi) the considerations to be taken into account to achieve end-to-end system security;

(vii) continuous review of threats and vulnerabilities; and

(viii) implementation of updates and control;

e. interfaces and interdependencies with other design activities for each SSoI/ToSA; and

f. for the Mission System only (including, where applicable, each ToSA within the Mission System), the identification and resolution of any whole-of-system system security-related risks, Issues and opportunities, including managing trade-offs between the various specialty engineering domain requirements.

Note: In relation to the NIST Special Publication references identified in clause 5.1, the MSSMP should be developed from the latest versions of these documents, except where otherwise agreed by the Commonwealth Representative.

6.2.5.2 The MSSMP shall identify all reference documents that will be used in the development of the security design for each SSoI/ToSA, including applicable security standards, policies, supporting technical documentation and guidance, including to the extent applicable, the documents identified at clause 5.1.

6.2.5.3 The MSSMP shall describe, in annexes to the MSSMP, the tailoring of the identified standards to meet the security requirements of the Contract, including:

a. the activities or processes from each standard to be undertaken, including the rationale for including and tailoring or excluding an activity or process;

b. the data required, including from related programs (eg, Systems Engineering program, Electromagnetic Environmental Effects (E3) program or system safety program), to perform the identified analysis activities / processes;

c. the expected outcomes associated with undertaking each activity or process;

d. how the outcomes relate to the requirements of the Contract and the Contractor's proposed solutions for each SSoI/ToSA;

e. how the outcomes will be documented;

f. the tools to be utilised to undertake each activity or process; and

g. the expected role of the Commonwealth in reviewing the outcomes.

6.2.6 System Security and Support

6.2.6.1 The MSSMP shall describe any unique aspects of the Contractor's system security program relating to the Support System that are not addressed through the other clauses in this DID, including (for example):

a. how security requirements will be incorporated into the Contractor's Cyber Supply Chains to address ICT/cyber security risks for DESE, cross-referring to any Cyber Supply Chain Risk Plan (CSCRP) required under the Contract and describing how the Cyber Supply Chain risk assessments will be kept current and the Commonwealth will be kept apprised of changed circumstances, as new items of DESE for the SSoIs are identified;

b. the security requirements for support-related equipment (eg, Support and Test Equipment (S&TE), Training Equipment, and Facilities equipment and ICT systems);

c. operational security requirements for all phases of the life of the Mission System up to and including disposal; and

d. considerations in relation to system security monitoring and Maintenance, including for ICT/cyber security:

(i) countermeasures against malicious code;

(ii) intrusion detection strategies and detection mechanisms;

(iii) audit and event log analysis and alerting;

(iv) system integrity checking (system characterisation);

(v) vulnerability monitoring, assessments and patching;

(vi) periodic revalidation of security controls;

(vii) user access management;

(viii) periodic audit of intrusion detection procedures;

(ix) systematic user Training and awareness programs; and

(x) maintaining the currency of authorised Training packages and Security Standard Operating Procedures (SSOPs).

6.2.7 Security Authorisations and Verification & Validation

6.2.7.1 The MSSMP shall explain the approach to achieving the required Security Authorisations for each SSoI/ToSA in accordance with the Contract, the Governing Security Documents, CERTP (if applicable), and other applicable documents identified at clause 5.1, including:

a. explaining the approach to be used for each of the different Security Authorisations required for physical security, EMSEC, ICT security and cyber security for each SSoI/ToSA, as applicable, including identifying the Objective Evidence to be provided to support the achievement of these authorisations;

b. describing how the Contractor will engage with the relevant Security Authorisation authorities, and the roles and responsibilities of the different stakeholders, including the stakeholder identified in accordance with clause 6.2.1.2; and

c. describing any circumstances where a particular Security Authorisation (eg, for ICT security) is a necessary precursor to the conduct of any aspect of AV&V.

6.2.7.2 The MSSMP shall explain the approach to conducting Verification and Validation (V&V) of the security requirements of the Contract for each SSoI/ToSA, cross-referring to the applicable V&V and/or assurance data items identified at clause 4.2 as appropriate, including:

a. evaluation of delivered systems and equipment, including in relation to:

(i) mapping of cyber attack and engagement surfaces;

(ii) the confidentiality, integrity and availability of systems and data; and

(iii) the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations, including the ability to detect, manage and recover from cyber security incidents;

b. how the proposed V&V supports the security assurance processes and requirements set out in the Contract and applicable data items, such as the CERTP;

c. how the effectiveness of security controls will be demonstrated, including the identification of any Certification and Accreditation requirements for software, security devices or other special security features; and

d. the evidence that will be collected and provided to the Commonwealth to provide confidence that the security requirements for each SSoI/ToSA will be met.

6.2.8 System Security Tools

6.2.8.1 The MSSMP shall describe any simulation and other tools, instruments, items of equipment, test facilities and any other major elements that will be required to define, design, develop, implement, Certify, Accredit, Verify and Validate the security requirements of the Contract, including in relation to each SSoI/ToSA.

6.2.9 System Security Schedule

6.2.9.1 The MSSMP shall contain a summary of the system security schedule, which identifies key activities, events and milestones for the system security program for the Contract, including for the different types of Security Authorisations for each SSoI/ToSA.

6.2.9.2 The full system security program schedule shall be included in the CMS.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-MGT-SIP-V5.3

2. TITLE: SITE INSTALLATION PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Site Installation Plan (SIP) describes the Contractor’s strategy, methodology and plans for undertaking site installation activities at all of the Commonwealth Premises, including facilities where installation of Mission System elements or Support System Components (or both) is required. The SIP includes the Contractor's plans for integrating its activities with those of the Commonwealth (or other party) at these installation sites.

3.2 The Contractor uses the SIP to:

a. define, manage and monitor its activities at the installation sites;

b. plan and co-ordinate its involvement with the Commonwealth’s (or other parties’) activities at these sites; and

c. ensure that those parties (including Subcontractors) working at the installation sites understand their respective responsibilities, the processes to be used, and the time frames involved.

3.3 The Commonwealth uses the SIP to:

a. understand and evaluate the Contractor’s requirements for installing Mission System elements or Support System Components (or both) at the installation sites;

b. identify and understand the Commonwealth’s involvement in the Contractor’s activities, including the monitoring of the Contractor’s activities; and

c. provide input to the Commonwealth’s own planning (eg, in relation to site preparation and co-ordination with other Commonwealth organisations).

4. INTER-RELATIONSHIPS

4.1 The SIP is subordinate to the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP);

b. System Engineering Management Plan (SEMP); and

c. Integrated Support Plan (ISP).

4.2 The SIP inter-relates with the following data items, where these data items are required under the Contract:

a. Contractor Transition Plan (CTXP);

b. Facilities Requirements Analysis Report (FRAR);

c. System Integration Plan (SINTP);

d. Verification and Validation Plan (V&VP); and

e. Contract Master Schedule (CMS).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the SIP shall summarise these aspects and refer to the other data item.

6.1.3 The SIP shall comprise a main body and a series of separate Site-specific annexes, where:

a. the main body shall describe all site installation activities that are required to be undertaken by the Contractor under the Contract and which are common/applicable at all Sites; and

b. a separate annex shall be used to describe the Site-specific installation activities, constraints and information applicable at each Site.

6.2 Specific Content – Main Body

6.2.1 General

6.2.1.1 The main body of the SIP shall describe the objectives, scope, constraints, and assumptions associated with the Contractor’s site installation activities at Commonwealth Premises (including facilities).

6.2.1.2 The main body of the SIP shall include all installation activities at Commonwealth Premises, including in relation to any:

a. new, modified or existing Contractor provided facilities; and

b. new, modified or existing Commonwealth provided facilities.

6.2.1.3 The main body of the SIP shall provide a summary of the key relationships between the Contractor’s activities and those of the Commonwealth (or other party), including any access requirements to Commonwealth Premises, required for the installation of any Mission System elements or Support System Components (or both).

6.2.2 Risk Management

6.2.2.1 All risks associated with site installation activities shall be documented in the Risk Register, in accordance with the Approved Project Management Plan (PMP).

6.2.2.2 The main body of the SIP shall describe the risk management strategies common to all site-installation activities.

6.2.3 Organisation and Management

6.2.3.1 The main body of the SIP shall include the Contractor's organisational arrangements (including Subcontractors) for its site installation activities, and the inter-relationships between the installation organisation and the other parts of the Contractor's organisation for the Contract.

6.2.3.2 The main body of the SIP shall identify the individual within the Contractor’s organisation who will have managerial responsibility and accountability for meeting the site installation requirements of the Contract.

6.2.3.3 The main body of the SIP shall identify the Contractor’s expectations of the Commonwealth with respect to site installation activities at Commonwealth-managed sites.

6.2.4 Site Installation Activities

6.2.4.1 The main body of the SIP shall describe the Contractor’s processes, procedures and common activities, and plans for co-ordinating the Contractor’s activities and the Commonwealth’s activities for all site-installation activities required under the Contract, including:

a. the major activities to be undertaken, when, and by whom;

b. an overview of the integration of Subcontractors into the Contractor's activities;

c. the relationship between access, installation and Verification and, if applicable, Validation activities;

d. processes, procedures and forms for co-ordination of interruptions to power, communications and other services;

e. implications for security and safety, including the Contractor's plan to manage work health and safety during site installation; and

f. any facilities approvals required.

6.2.4.2 The main body of the SIP shall include:

a. an outline of the general physical and electrical characteristics of the proposed installation(s); and

b. a description of any Verification and Validation (V&V) activities, including tests that may be conducted during and following installation to confirm that the installation has been successful.

6.2.4.3 Without limiting the requirements of the Contract, the main body of the SIP shall provide an overview of the actual and potential impact of site installation activities on:

a. existing systems or equipment, including outages to operational capability;

b. facilities, including:

(i) utility services, such as water, plumbing, drainage, gas, electricity and phone connections;

(ii) monitoring services, such alarm services, including fire alarms;

(iii) roads, paths, car parks, retaining walls, storage tanks, landscaping, and fencing;

(iv) electrical distribution, including power feeds, switchboards, UPS, sub-circuits arrangements; and

(v) heating, ventilation and air-conditioning (HVAC); and

c. the environment.

6.2.5 Site Installation Schedule

6.2.5.1 The main body of the SIP shall include a schedule of the site installation activities, showing the relationships between activities at each installation site and between different installation sites, as required under the Contract.

6.2.5.2 The full site installation schedule shall be provided as part of the CMS.

6.3 Annex Requirements – Site Specific

6.3.1 General

6.3.1.1 Each annex to the SIP shall provide site-specific details for the installation activities required under the Contract at any:

a. new, modified or existing Contractor provided facilities; and

b. new, modified or existing Commonwealth provided facilities.

6.3.1.2 Each annex to the SIP shall identify the site-specific relationships between the Contractor's activities and those of the Commonwealth (or other party), including any access requirements to Commonwealth Premises, required for the installation of any Mission System elements or Support System Components (or both) at the relevant Commonwealth Premises.

6.3.2 Risk Management

6.3.2.1 Each annex to the SIP shall describe the risk management strategies associated with the site-specific installation risks applicable at the relevant Commonwealth Premises.

6.3.3 Organisation Management

6.3.3.1 Each annex to the SIP shall identify the individual within the Contractor's organisation who will have managerial responsibility and accountability for meeting the site installation requirements at the relevant Commonwealth Premises.

6.3.4 Site Installation Activities

6.3.4.1 Each annex to the SIP shall describe the Contractor's plans for co-ordinating the Contractor's activities and the Commonwealth's activities at the relevant Commonwealth Premises, including:

a. the major activities to be undertaken (including during each phase of the system implementation process from removal of existing equipment (if applicable), construction work undertaken by the Commonwealth, and installation and V&V activities to be undertaken by the Contractor), when, and by whom;

b. the integration of Subcontractors into the Contractor's activities;

c. site-specific access requirements to various parts of the site, including timeframes associated with these access requirements;

d. the relationship between the Contractor's site-specific access requirements and specific Commonwealth constraints associated with operational, support or training activities, including any Commonwealth constraints associated with site preparation before access can be provided to the Contractor (eg, for removal of existing equipment);

e. site-specific co-ordination of interruptions to power, communications and other services;

f. site-specific implications for security and safety, including the Contractor's plan to manage:

(i) site-specific security considerations during site installation, including management of site-related Certifications and re-Certifications; and

(ii) work health and safety during site installation;

g. any site-specific facilities approvals required; and

h. activities to be undertaken to ensure the installation site is returned to a clean and functional condition upon completion of site installation activities, including such aspects as repairing any damage to road surfaces and removal of rubbish.

6.3.4.2 Each annex to the SIP shall include the following information applicable at the relevant Commonwealth Premises:

a. an outline of the physical and electrical characteristics of the proposed installation(s);

b. references to the relevant site installation drawings, which document at least the following:

(i) equipment housings;

(ii) equipment racks and contents;

(iii) interconnections between components;

(iv) fencing; and

(v) cable runs;

c. a description of any V&V activities, including tests, that may be conducted during and following site installation to confirm that the installation has been successful and the Site is ready for subsequent Contract activities (eg, further V&V activities or Site Acceptance).

6.3.4.3 Without limiting the requirements of the Contract, each annex to the SIP shall identify the site-specific impact of site installation activities on:

a. existing systems or equipment, including outages to operational capability;

b. facilities, including:

(i) utility services, such as water, plumbing, drainage, gas, electricity and phone connections;

(ii) monitoring services, such alarm services, including fire alarms;

(iii) roads, paths, car parks, retaining walls, storage tanks, landscaping, and fencing;

(iv) electrical distribution, including power feeds, switchboards, UPS, sub-circuits arrangements; and

(v) heating, ventilation and air-conditioning (HVAC); and

c. the environment, including in relation to:

(i) vehicle hygiene requirements;

(ii) sediment and erosion control;

(iii) road base and quarry material;

(iv) vegetation management;

(v) POL and vehicle refuelling;

(vi) waste management;

(vii) fauna protection;

(viii) heritage protection;

(ix) vehicle movement;

(x) fire control; and

(xi) others as required.

DATA ITEM DESCRIPTION

1. **DID NUMBER: DID-ENG-MGT-SSPP-V5.3**

2. **TITLE: SYSTEM SAFETY PROGRAM PLAN**

3. **DESCRIPTION AND INTENDED USE**

3.1 The purpose of the System Safety Program Plan (SSPP) is to describe the tasks and activities for system-safety management and system-safety engineering that are required to achieve Safety Outcomes. The Approved SSPP provides a formal basis of co-ordination, consultation and understanding between the Contractor and the Commonwealth on how the system-safety program will be executed to meet contractual and legislative requirements.

3.2 The Contractor uses the SSPP to describe how the system-safety program will be accomplished to meet their legislative obligations and the Materiel Safety requirements included in the Contract.

3.3 The Commonwealth uses the SSPP to plan and monitor the Contractor's system-safety program and to determine whether the program will achieve a level of Materiel Safety acceptable to the Commonwealth, and facilitate Commonwealth compliance with legislation, including the WHS Legislation.

4. **INTER-RELATIONSHIPS**

4.1 The SSPP is a subordinate plan to the following data items, where these data items are required under the Contract:

a. System Engineering Management Plan (SEMP); and

b. Integrated Support Plan (ISP).

4.2 The SSPP inter-relates with the following data items, where these data items are required under the Contract:

a. Software Management Plan (SWMP);

b. Contract Master Schedule (CMS);

c. Hazard Analysis Report (HAR);

d. Hazard Log (HL);

e. Safety Case Report (SCR);

f. Materiel Safety Assessment;

g. Safety Data Sheets (SDSs);

h. the security-related data items required under the Contract (ie, in relation to the relationships between security considerations and safety considerations);

i. Quality Plan (QP);

j. Verification and Validation Plan (V&VP);

k. Verification Cross-Reference Matrix (VCRM); and

l. Health and Safety Management Plan (HSMP).

5. **APPLICABLE DOCUMENTS**

5.1 The following documents form a part of this DID to the extent specified herein:

MIL-STD-882E	*System Safety*
	WHS Legislation

The system safety standards identified under the System Safety Program clause of the SOW

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the SSPP shall summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Program Scope and Objectives

6.2.1.1 The SSPP shall define a program to satisfy the system-safety requirements of the Contract by describing:

a. the scope of the system-safety program in terms of the system and the life-cycle phase;

b. the overall approach of the system-safety management, software safety management and engineering program to achieving Safety Outcomes, including through the hazard analyses required by clause 6.2.6 and related Contract requirements;

c. the integration of system-safety activities with the Systems Engineering and other functional elements of the Contract; and

d. the resource requirements needed to execute the SSPP.

6.2.1.2 The SSPP shall provide traceability for all contractually required system-safety tasks and responsibilities in a matrix that correlates the requirements of the Contract (including regulatory requirements and design constraints) to the location in the SSPP where each requirement is addressed by the system safety program.

6.2.2 System Safety Interfaces

6.2.2.1 The SSPP shall describe the interfaces between the system-safety program and:

a. all other applicable safety disciplines including nuclear safety, range safety, explosive and ordnance safety, chemical and biological safety and laser safety;

b. Systems Engineering, and all other related disciplines including reliability and maintainability, Quality Management, software development, human factors engineering and medical support (for health hazard assessments); and

c. all system integration and test disciplines.

6.2.3 System Safety Organisation

6.2.3.1 The SSPP shall:

a. describe the system-safety organisation or function within the Contractor’s organisation for the Contract, including the organisational and functional relationships and lines of communication;

b. identify the responsibility and authority of each person and organisational unit involved in executing each of the contractual system-safety requirements, including Key Persons, Subcontractors and system-safety groups;

c. describe the procedures that the Contractor will use to integrate system-safety and hazard management efforts for external system interfaces, including:

(i) the roles of Commonwealth agencies, Associated Parties and Subcontractors necessary to integrate safety requirements for the total system;

(ii) the interfaces between the Contractor and each Subcontractor and Associated Party (eg, for integrating hazard analyses);

(iii) integrated product teams, or working groups, with representatives from Subcontractors and Associated Parties (as applicable);

(iv) any system-safety integration roles and their specific responsibilities for managing interfaces with external systems;

(v) integrating hardware and software provided as GFE;

(vi) assigning requirements to organisational units and Subcontractors;

(vii) coordinating Subcontractor system-safety engineering efforts;

(viii) facilitating system-safety program reviews;

(ix) recommending mitigation measures including assessing feasibility, cost, and effectiveness of the measures, and allocating implementation responsibility to Subcontractors and Associated Parties;

(x) reporting on program safety status and measures; and

(xi) the approach to consulting, coordinating and cooperating on safety issues, including between the parties, Subcontractors and Associated Parties; and

d. the process through which Contractor management decisions will be made, including timely notification to the Commonwealth of unacceptable risks, necessary actions in the event of mishaps, incidents, or malfunctions, and for requesting exemptions to system-safety requirements, program deviations and Engineering Change Proposals, when applicable.

6.2.4 System Safety Program Milestones

6.2.4.1 The SSPP shall:

a. define a schedule of system-safety program milestones including required inputs and outputs, and start and completion dates;

b. relate the schedule of the system-safety program to system-level activities, Mandated System Reviews, and Milestones within the CMS;

c. identify the schedules for subsystem, component, and software safety activities applicable to the system-safety program but specified in other engineering studies and development efforts to preclude duplication; and

d. include a schedule of internal review meetings with Subcontractors and Associated Parties to cooperate, consult and coordinate the system-safety program effort.

6.2.5 General System Safety Requirements and Criteria

6.2.5.1 The SSPP shall:

a. list the safety standards, system specifications, specified design constraints, and the civil and military regulations containing safety requirements that shall be complied with by the Contractor, including the Applicable Documents at clause 5 and identifying titles, dates and, where applicable, paragraph numbers;

b. describe general engineering requirements and design criteria for achieving safety outcomes applicable to design and development activities, including the role of Software in safety for each of the relevant states and modes);

c. identify safety requirements for all appropriate phases of the life cycle up to, and including, disposal;

d. describe the method for ensuring flow-down of hazard identification, mitigation strategies and associated system-safety program requirements to Subcontractors; and

e. describe the structure of the Materiel Safety baseline documentation to be delivered to the Commonwealth (ie, the SCR or Materiel Safety Assessment, as applicable to the Contract).

6.2.6 Hazard Analysis

6.2.6.1 The SSPP shall describe:

a. the process for hazard identification, risk assessment, risk mitigation, communication of risks and support to risk acceptance including:

(i) for hazard identification, the systematic identification process that evaluates the system throughout its life-cycle, including system hardware and software, system interfaces (including human interfaces), the intended use or application and operational environment, and disposal;

(ii) for risk assessment, the description of severity categories, probability levels, and the process for assigning Hazard Risk Indices (HRIs);

(iii) for risk mitigation, how decisions will be made within the system-safety process, with an emphasis on achieving Safety Outcomes including, in the context of cost to eliminate and minimise risks, whether the cost of further mitigation would be grossly disproportionate to the risk; and

(iv) for risk acceptance, the procedures for communicating and coordinating Commonwealth residual risk acceptance, including procedures for engaging the relevant Commonwealth authority(ies);

b. the approach for applying system-safety processes to extant system interfaces, subsystems or components (eg, for off-the-shelf items or legacy software) including the approach for verification and ensuring that existing data is consistent with the configuration, role and environment for the Mission System(s) and other Supplies;

c. the process for determining whether a qualitative or quantitative risk assessment is appropriate for a given hazard;

d. the hazard analyses to be performed (eg, preliminary hazard analysis, subsystem hazard analysis), the techniques to be used (eg, fault tree analysis, FMECA) and the documentation of the results, including the hazard analyses to be reported in each Hazard Analysis Report that is required to be delivered by the Contractor;

e. the scope of each analysis activity, the integration of Associated Party and Subcontractor hazard analyses within the overall system hazard analyses, and the depth within the system to which each analytical technique will be used;

f. for system interfaces, how analysis of the integrated system design, operations, and the interfaces between the products from each Subcontractor and Associated Party and the Mission System, or other major Supplies, will be executed;

g. the efforts to identify and control hazards associated with Problematic Substances and Problematic Sources incorporated within the design, and those Problematic Substances and Problematic Sources used in operation and support during the system’s life-cycle;

h. the efforts to identify and control WHS hazards directly related to the design (eg, noise, vibration, working at heights, working in confined spaces, lifting requirements and other human interface and ergonomic factors); and

i. the systematic software safety approach to be followed, when applicable.

6.2.6.2 The SSPP shall provide traceability to the hazard analysis tasks from MIL-STD-882E, or an equivalent standard acceptable to the Commonwealth Representative, and identify any tailoring of the standard tasks for the system-safety program under the Contract.

6.2.7 System Safety Data

6.2.7.1 The SSPP shall:

a. describe the approach for collecting and processing pertinent hazard, mishap, and safety lessons learned data, including both historical data used to assist system safety analyses and current system data in the Hazard Log;

b. describe the management and use of the Hazard Log for recording each mishap risk and hazard, and the findings and results of the related analysis including hazard and safety-risk analyses, risk mitigation, and treatment;

c. identify all deliverable data items by title and number, and means of delivery (eg, hard copy, electronically); and

d. identify non-deliverable system-safety data and describe the procedures for accessibility by the Commonwealth and retention of data of historical value.

6.2.7.2 The SSPP shall, in accordance with clause 6.2.7.1, describe the scope of the SCR or Materiel Safety Assessment, as applicable to the Contract, and the supporting information to be delivered to the Commonwealth as evidence for the assessment of Materiel Safety.

6.2.8 Safety Verification

6.2.8.1 The SSPP shall describe:

a. the Verification, and reporting, of the effectiveness of mitigation measures in achieving Safety Outcomes through test, analysis, inspection, or other means;

b. the Verification, and reporting, that hardware, software, and procedures comply with identified hazard management requirements;

c. requirements for certification, independent review evaluations and special testing of safety features (eg, insensitive munitions tests and render safe / emergency disposal procedures);

d. the procedures in place to transmit safety-related Verification information to the Commonwealth; and

e. the procedures for ensuring the safe conduct of all Verification activities.

6.2.9 Audit Program

6.2.9.1 The SSPP shall describe the techniques and procedures to be employed by the Contractor to ensure that the objectives and related requirements of the system-safety program, including the achievement of Safety Outcomes, are being accomplished.

6.2.10 Training

6.2.10.1 The SSPP shall describe the safety training for personnel involved with the system-safety program.

6.2.11 Incident Reporting

6.2.11.1 The SSPP shall describe the incident alerting (including for mishaps and malfunctions), investigation and reporting processes, including notification of the Commonwealth.

6.2.12 System Safety Working Group

6.2.12.1 Where the SOW requires the Contractor to establish a System Safety Working Group (SSWG), the SSPP shall include a plan for the SSWG, including:

a. objectives and the terms of reference for the SSWG;

b. the membership and points of contact for the SSWG; and

c. arrangements for the conduct of SSWG meetings.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-CSCRP-V5.3

2. TITLE: CYBER SUPPLY CHAIN RISK PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Cyber Supply Chain Risk Plan (CSCRP) is used to identify and track Cyber Supply Chain threats for Digitally Enabled Systems and Equipment (DESE) and Software, the associated risk assessments, the risk treatment options, and the existing and proposed risk controls associated with the Cyber Supply Chains for the Security Systems-of-Interest (SSoIs), including during design, development, build, operation and support. The Approved governing plan (eg, Materiel System Security Management Plan (MSSMP) or In-Service Security Management Plan (ISSMP), as applicable) provides the plan and associated processes for managing security-related risks, while the CSCRP addresses the specific risk information relating to Cyber Supply Chain risks for the SSoIs (or relevant components thereof).

3.2 The Contractor uses the CSCRP:

a. to document the Cyber Supply Chain threats for the SSoIs/DESE/Software, including the associated risk assessments, and to review and update those threats and assessments as circumstances change during the acquisition phase and the in-service phase (as applicable);

b. to document the risk treatment options, the existing and proposed risk controls, and the residual risk exposure;

c. to advise the Commonwealth and, as applicable, the ICT and cyber Security Authorisation authorities and assessor(s) of the Cyber Supply Chain threats and risk assessments associated with the SSoIs; and

d. as one of the security artefacts to provide assurance to the Commonwealth that the Contractor's security activities will result in the cyber-security requirements for a SSoI being achieved and maintained.

3.3 The Commonwealth uses the CSCRP:

a. to gain assurance that the Contractor has a sound Cyber Supply Chain program in place that complies with applicable Government and Defence security requirements and policies;

b. to understand and evaluate the Contractor's approach to meeting the Cyber Supply Chain requirements of the Contract as part of the system security program for the acquisition phase and in-service phase (as applicable);

c. to identify and understand the Commonwealth's involvement in the Contractor's Cyber Supply Chain program, including the monitoring of the Contractor's program;

d. as an input to its own planning, including in relation to attaining and/or maintaining the required ICT/cyber Security Authorisations for a SSoI; and

e. as part of the Objective Evidence provided to the relevant Defence authorities as part of initially obtaining and subsequently maintaining the required ICT/cyber Security Authorisations for a SSoI.

4. INTER-RELATIONSHIPS

4.1 The CSCRP is subordinate to the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP);

b. Support Services Management Plan (SSMP);

c. Systems Engineering Management Plan (SEMP);

d. Contractor Engineering Management Plan (CEMP);

e. Materiel System Security Management Plan (MSSMP); and

f. In-Service Security Management Plan (ISSMP).

4.2 The CSCRP inter-relates with the following data items, where these data items are required under the Contract:

a. System Architecture Description (SAD), which identifies the product breakdown structure or system breakdown structure for the relevant SSoIs;

b. Software List (SWLIST);

c. Configuration Status Accounting Report (CSAR);

d. any provisioning lists required under the Contract (eg, the Recommended Spares Provisioning List (RSPL) or the Recommended Provisioning List (RPL)); and

e. the security-related data items required under the Contract (other than those identified under clause 4.1).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Governing Security Documents	(see the Glossary for the definition of this term)
CTIS	Australian Cyber Security Centre (ACSC) Cyber Threat Intelligence Sharing (CTIS) platform
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1, September 2012
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018
ISO/IEC 27005:2022	Information security, cybersecurity and privacy protection – Guidance on managing information security risks
ASIO 18-9938	Security Manager’s Guide: Supply Chain Security, 2018
	ACSC Publication, ‘Cyber Supply Chain Risk Management’, May 2023
	ACSC Publication, ‘Identifying Cyber Supply Chain Risks’, May 2023
	ACSC Publication, ‘Cloud Computing Security Considerations’, October 2021
Defence ICT/Cyber SCRM Framework	The Defence ICT/Cyber Procurement Supply Chain Risk Management Framework, October 2020

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

Note: This DID has been written on the basis that all SSoIs applicable to a Contract will be addressed within a single CSCRP. Where this is not the case, such as may occur for larger

Mission Systems (eg, aircraft or ship), the requirements of the DID should be interpreted in the context of the set of CSCRPs and associated SSoIs (or components thereof).

6.1.2 The CSCRP shall be consistent with and, where applicable, comply with the Governing Security Documents. The CSCRP shall accord with the risk management framework documented in the Approved governing plan (eg, PMP/SSMP, MSSMP or ISSMP), as applicable.

6.1.3 In relation to the delivery of each version of the CSCRP for a SSoI (eg, during the acquisition phase or as part of the development of a Major Change during the support phase), each version shall, at the time of delivery, be sufficiently complete to satisfy the purpose for which it is being provided (eg, to support the assessment of cyber Security Authorisation for a particular SSoI or element thereof).

6.1.4 When the Contract has specified delivery of another data item that contains aspects of the required information, the CSCRP should summarise these aspects and refer to the other data item.

6.1.5 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Summary

6.2.1.1 The CSCRP shall include a system-level summary of the CSCRP, including:

a. an overview of each SSoI being assessed, including identifying any standalone elements, such as an item of Training Equipment or a security system within a Facility;

b. a brief description of the risk-assessment process undertaken, cross-referring to the Approved governing plan, as appropriate;

c. a summary of the Cyber Supply Chain risk sources considered, including the severity of risk exposures associated with these risk sources; and

d. the significant conclusions of the CSCRP.

6.2.2 Scope

6.2.2.1 The CSCRP shall identify the product breakdown structure or system breakdown structure (as applicable) for each SSoI (or significant products within an SSoI), which decomposes the system and its related subsystems to a level, which enables the identification of all DESE and Software components and any associated ICT services (eg, cloud computing services) that:

a. form part of the SSoI that will be obtained through the Contractor's Cyber Supply Chain or acquired through other means, such as from open-sources; and

b. have the potential to include cyber vulnerabilities or introduce cyber vulnerabilities into an SSoI (or element thereof),

(hereinafter known as '**Vulnerable Components / Services**').

6.2.2.2 The CSCRP shall identify any assumptions and constraints associated with the assessment of the Cyber Supply Chains for an SSoI, including any factors relating to the CSCRP that are assumed but not confirmed and that have constrained the assessment of Cyber Supply Chain risks for the SSoI.

6.2.2.3 In responding to the specific requirements of this DID, the CSCRP shall describe how the Applicable Documents listed at clause 5 have been utilised to ensure that the CSCRP will achieve the objectives and purposes set out in clause 3.

6.2.2.4 The CSCRP shall describe the processes and timings for updating the CSCRP as new items of DESE and/or proposed new suppliers are identified, including how the Commonwealth will be kept apprised of the updated risk assessments and any judgements arising from those risk assessments associated with these new aspects.

6.2.3 Supply Chain Risk Assessment

6.2.3.1 The CSCRP shall identify and describe the Cyber Supply Chain risks applicable to the scope of the assessment identified through clause 6.2.2.

6.2.3.2 The CSCRP shall consider the following Cyber Supply Chain risk sources (as described in the ACSC Publication, 'Identifying Cyber Supply Chain Risks') as a minimum:

a. risks due to foreign control or interference;

b. risks due to poor security practices, including by lower-tier suppliers (which could include, for example, insertion of counterfeits, unauthorised production, compromised / infected system images, malicious insiders, tampering, insertion of malicious software and hardware, and poor patch-management practices);

c. risks due to lack of transparency;

d. risks due to access and privileges; and

e. risks due to poor business practices.

6.2.3.3 The CSCRP shall include the following information for each identified Vulnerable Component / Service:

a. the component/service title and unique identifier;

b. a component/service description;

c. the criticality (consequence) assessment conducted in accordance with the Defence ICT/Cyber SCRM Framework;

d. the vulnerability (likelihood) assessment conducted in accordance with the Defence ICT/Cyber SCRM Framework;

e. the existing controls (eg, as identified in Table Three of the Defence ICT/Cyber SCRM Framework or other source Approved by the Commonwealth Representative);

f. the resultant risk exposure;

Note: The October 2020 version of the Defence ICT/Cyber SCRM Framework identifies five treatment options: Avoid, Share, Exploit, Accept and Reduce. For consistency of risk management practices across all aspects of the Contract, these five options should be mapped into the standard treatment options and language identified in the Contract.

g. the treatment option(s) (ie, acceptance, reduction, transfer or avoidance);

h. the treatment recommendation(s);

i. the residual likelihood of occurrence after the identified treatment recommendations, which involve implementation actions, have been implemented;

j. the residual consequence of realisation after the identified treatment recommendations, which involve implementation actions, have been implemented; and

k. the residual risk exposure.

6.2.4 Risk Treatment Planning

Note: The risk-treatment plan for each Cyber Supply Chain risk may involve both initial activities as part of establishing the Cyber Supply Chain(s) as well as ongoing monitoring and surveillance activities, including (for example) the inclusion of specific provisions in Subcontracts and limiting the supply of particularly vulnerable components to only known and trusted suppliers (eg, from the Five Eyes (FVEY) countries). The Commonwealth expects that both sets of activities will be addressed in each risk-treatment plan (to the extent applicable), including how ongoing performance monitoring will be undertaken and how the Contractor will set up and/or manage its support arrangements to ensure that the risk-treatment plans will have ongoing validity.

6.2.4.1 The CSCRP shall set out the Contractor's risk-treatment plan for each risk for which the risk-treatment option is to either:

a. reduce the likelihood and/or reduce the consequence; or

b. avoid the risk by changing the design of the SSoI to enable such avoidance to occur,

with the aim of demonstrating that these risk-treatment plans, once implemented, will be sufficient to ensure that the SSoI will be ASARP.

6.2.4.2 Each risk-treatment plan shall include:

a. the position responsible within the Contractor's or supplier's organisation;

b. a brief description of the required scope of work;

c. the envisaged schedule for implementation, including the associated milestones;

d. the likely resources;

e. the envisaged cost; and

f. any other relevant information (eg, implementation risks and verification activities).

6.2.5 Residual Risk Exposure

6.2.5.1 The CSCRP shall record whether the residual risk exposure associated with each Cyber Supply Chain risk has been accepted by the Commonwealth in support of:

a. if applicable, ICT Security Authorisation for the SSoIs (or elements thereof); and

b. cyber Security Authorisation for the SSoIs (or elements thereof).

6.2.5.2 The record of risk acceptance required under clause 6.2.5.1 shall include:

a. the Contractor's risk acceptance authority by title and organisation, and date of acceptance;

b. the Commonwealth authority's concurrence or non-concurrence, as applicable, by title and organisation, and date of risk acceptance; and

c. identification details for the signed risk acceptance document(s).

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-CSCR-V5.3

2. TITLE: CYBER SECURITY CASE REPORT

3. DESCRIPTION AND INTENDED USE

3.1 The Cyber Security Case Report (CSCR) documents a comprehensive evaluation, at the time of the report, of the cyber threats and system vulnerabilities and their associated risks prior to test or operation of a Security System-of-Interest (SSoI), following system modification, or prior to the Acceptance of an SSoI (or element thereof). A CSCR may address multiple SSoIs if this is efficient and practicable.

3.2 The CSCR, including by reference to other security-related data items (which in totality form the 'Cyber Security Case'), identifies the cyber threats, associated risks, and measures to ensure that cyber threats have been either eliminated or their potential effects minimised so that the SSoI (or element thereof) is assessed to be As Secure As Reasonably Practicable (ASARP) – in summary, all of the evidence needed to demonstrate that the cyber-related Security Outcomes have been, or will be[1], met. The CSCR documents the consultation outcomes between the Commonwealth and Contractor and formal risk acceptance decisions made.

3.3 The Contractor uses the CSCR to present an argument, supported by a body of evidence, to demonstrate that, for an SSoI (or element thereof):

a. when used in relation to the Acceptance of Supplies, the SSoI (or element thereof) is ASARP and can be operated under a known threat environment with an acceptable level of risk of performance degradation due to cyber attack, as the cyber-related Security Outcomes have been, or will be, met;

b. the applicable Defence and Government cyber-security requirements, including in relation to relevant Security Authorisations, design rules, standards, and codes of practice, have been satisfied and the residual security risks are acceptable; and

c. the confidentiality, integrity and availability of the SSoI (including the data processed, stored and/or communicated electronically or by similar means by the SSoI) can be maintained during operations.

3.4 The Commonwealth uses the CSCR for an SSoI (or element thereof):

a. to determine that the cyber threats to Defence operations and system integrity have been identified and that the cyber-related Security Outcomes have been, or will be, met;

b. when applicable, as a basis for evaluating system security prior to the Acceptance of Supplies;

c. as the principle justification for assessing that risk of compromise from cyber attack has been mitigated to an 'acceptable level' based on the robustness of the arguments underpinning the CSCR; and

d. as the basis for assessing and managing cyber-security risks throughout the life-cycle of an SSoI.

4. INTER-RELATIONSHIPS

4.1 The CSCR is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Contractor Engineering Management Plan (CEMP);

[1] Reference to 'will be' acknowledges that some measures can only be established through Defence processes and training.

c. Materiel System Security Management Plan (MSSMP); and

d. In-Service Security Management Plan (ISSMP).

4.2 The CSCR inter-relates with the following data items, where these data items are required under the Contract:

a. Cyber Supply Chain Risk Plan (CSCRP);

b. the security-related data items required for physical security, Emanation Security (EMSEC), and Information and Communications Technology (ICT) security; and

c. Verification and Validation (V&V) data items, such as the V&V Plan (V&VP), Verification Cross Reference Matrix (VCRM), Acceptance Test Plans (ATPs), and Acceptance Test Reports (ATRs).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Governing Security Documents	(see the Glossary for the definition of this term)

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the CSCR shall summarise these aspects and refer to the other data item as part of the body of evidence.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The CSCR shall comprise a comprehensive and structured body of evidence that demonstrates, by reasoned argument, that an SSoI is suitable for Acceptance with respect to cyber security.

6.2.1.2 The CSCR shall include an executive summary.

6.2.1.3 Subject to clause 6.1.2, the CSCR shall provide a description of the SSoI(s) to which the Cyber Security Case relates, including:

a. the applicable configuration(s), roles, functions and environments, system boundaries, Targets of Security Assessment (ToSAs), major and security-critical Digitally Enabled Systems and Equipment (DESE) and Software, and areas of cyber-security risk that are worthy of particular attention; and

b. where relevant, any interfaces and interactions with other systems and personnel that may present cyber-security interface risks that cannot be managed by a single Contractor or Commonwealth entity.

6.2.2 System Security Program

6.2.2.1 The CSCR shall provide a description of the system security program employed by the Contractor to provide assurances as to the integrity of the process used to develop and update the Cyber Security Case, including the Contractor’s current assessment of cyber maturity against the Defence Cyberworthiness System (DCwS).

6.2.2.2 The description of the system security program shall summarise the analyses performed to achieve the cyber-related Security Outcomes, including:

a. a summary of the system security engineering and management processes employed to meet the cyber security-related requirements of the Contract, with explicit reference to the quality procedures employed;

b. a summary of the Cyber Security Assurance Basis, if one is required by the Contract;

c. the overarching approach and procedural requirements to ensure the authenticity of materiel through the Cyber Supply Chain (as part of both the acquisition phase and the in-service phase);

d. details of relevant Security Authorisations; and

e. the responsibilities and accountabilities of Key Persons involved in the system security program.

6.2.2.3 The CSCR shall summarise the requirements, criteria and methodology used to classify and rank cyber threats, including any assumptions on which the criteria or methodologies were based or derived including the definitions for the cyber threat risk indices and of acceptable risk. Where data for extant subsystems, components and interfaces were incorporated into the analysis, the CSCR shall summarise how that existing data was validated and, if necessary, adapted for the configuration(s), role and environment applicable to an SSoI (or element thereof).

6.2.3 SSoI Cyber-Security Assessment

6.2.3.1 The CSCR shall demonstrate, through assessment based on Objective Evidence, how an SSoI achieves the cyber-security requirements specified under the Contract, the requirements of relevant Australian legislation, codes of practice, civil and Defence regulatory requirements, and applicable design and safety standards.

6.2.3.2 The CSCR shall contain the Objective Evidence used to demonstrate that the cyber-related Security Outcomes for an SSoI have been, or will be, met, including:

a. a list of all cyber security-related risks with a residual (ie, post-treatment) risk level of medium or above, or as otherwise defined in the Approved MSSMP or the Approved ISSMP, as applicable;

b. subject to clause 6.1.2, the cyber threats against which the analyses and risk assessments were undertaken;

c. subject to clause 6.1.2, results of any cyber threat analyses conducted;

d. subject to clause 6.1.2, the details of any calculations, analyses, tests or examinations necessary to demonstrate that the cyber-related Security Outcomes have been, or will be, met, including the actions undertaken to:

(i) identify cyber threats that could give rise to risks to the confidentiality, classification, availability and/or integrity of information and data processed, stored and/or communicated electronically or by similar means by the SSoI;

(ii) identify cyber threats that could give rise to risks to operational effectiveness and/or achieving the Safety Outcome;

(iii) evaluate the actions taken to eliminate the cyber threats and associated risks to cyber security so that the SSoI is assessed as ASARP; and

(iv) validate the performance of cyber security controls;

e. subject to clause 6.1.2, recommendations applicable to cyber threats at, or caused by, the interface between the SSoI and other system(s), where applicable;

f. evidence that all applicable Security Authorisations and necessary security-related compliance assurance activities, as required by applicable security authorities, have been met;

g. a list of all pertinent reference materials including reports, standards and regulations, specifications and requirements documents, design documentation, and operating, maintenance and other manuals, including the Approved ISSMP and Approved SSOPs;

h. subject to clause 6.1.2, evidence to demonstrate that the Cyber Supply Chain's contribution to cyber security has been assessed, and that policies and procedures for continued Cyber Supply Chain assurance have been generated; and

i. subject to clause 6.1.2, any additional supporting evidence reasonably required by the Commonwealth for the purposes of demonstrating that the cyber-related Security Outcomes for the SSoI have been, or will be, met.

6.2.3.3 The CSCR shall contain a summary statement, signed by the Contractor's technical authority, declaring that the cyber-related Security Outcomes for an SSoI have been met and the SSoI is ready to undergo test, to operate, or to otherwise proceed into the next phase of its life cycle.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-DCERT-V5.3

2. TITLE: DESIGN CERTIFICATE

3. DESCRIPTION AND INTENDED USE

3.1 The Design Certificate (DCERT) is the document that certifies that a design conforms to the specified design requirements (with the exception of any items quoted on the DCERT) and is compliant with statutory obligations. The DCERT either includes, or refers to, the objective evidence necessary to support the claims of conformance.

3.2 The Contractor uses the DCERT to enable the individual approving each design or design change to certify that the design meets the contractual and statutory requirements and provide the certification required by any applicable ADF regulatory / assurance framework.

3.3 The Commonwealth uses the DCERT to provide confidence that a design meets the stated requirements, that the risks associated with a design are defined and have been controlled, and that the designer has addressed statutory obligations including the duties of a designer in accordance with Section 22 of the *Work Health and Safety Act 2011 (Cth)*.

4. INTER-RELATIONSHIPS

4.1 The DCERT inter-relates with the following data items, where these data items are required under the Contract:

a. System Specification (SS) for a Mission System, or specification for a modification;

b. Support System Specification (SSSPEC);

c. System Architecture Description (SAD);

d. design documents; and

e. Acceptance Verification and Validation (AV&V) data items.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

AAP 8000.011	Defence Aviation Safety Regulations (DASR)
ANP3411-0101	Navy Materiel Assurance Publication
LMSM	Land Materiel Safety Manual
DEOP 100 Vol 2 Pt2 Chap 3	Explosive Ordnance Safety Regulations

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item shall comply with any formatting requirements specified in the applicable ADF regulatory / assurance framework manual specified in the Statement of Work (SOW).

6.2 Specific Content

6.2.1 Identification of Certified Product

6.2.1.1 The DCERT shall identify the product to which the DCERT applies, including:

a. item name;

b. NATO Stock Number (NSN), if applicable;

c. manufacturer's code (ie, the NATO Commercial and Government Entity (NCAGE) code);

d. manufacturer's part / reference number; and

e. any additional information required to ensure that the product identification is clear and unambiguous.

6.2.2 Design Requirements and Evidence of Conformance

6.2.2.1 The DCERT shall include:

a. an index of the specifications / requirements, including applicable standards, against which the design was developed;

b. an index of the design documentation;

c. an index of the documentation that Verifies that the design conforms with the design requirements;

d. confirmation of successful completion of all Acceptance V&V activities required under the Contract;

e. details of any applicable ADF regulatory / assurance framework;

f. certification that, except for any exceptions listed on the design certificate in accordance with subclause g, the design, or design change:

(i) conforms with the design requirements;

(ii) is suitable for use in the intended environment and operating scenarios as documented in the Operational Concept Document or Operational and Support Concept (as applicable to the Contract); and

(iii) that all calculations made during the course of the design are warranted correct;

g. a list of exceptions from the design requirements;

h. certification that the designer has met any statutory obligations including the further duties of a designer in accordance with Section 22 of the *Work Health and Safety Act 2011 (Cth)*; and

i. details of the registration of any design or item requiring registration under Part 5.3 of the *WHS Regulations 2011 (Cth)*.

6.2.2.2 The DCERT shall include additional evidence reasonably required by the Commonwealth Representative, the *Work Health and Safety Act 2011 (Cth)*, and any ADF regulatory / assurance framework authority, in support of the requirements of clauses 6.2.2.1 and 6.2.4.

6.2.3 Issuing Authority

6.2.3.1 The DCERT shall identify the name and authority held by the individual approving the design, and the name and address of the company to which the individual belongs.

6.2.3.2 The DCERT shall be jointly signed by:

a. the individual approving the design, as authorised by the Contractor and in accordance with any applicable ADF regulatory / assurance framework requirements; and

b. the Contractor Representative.

6.2.4 ADF Regulatory / Assurance Framework Requirements

6.2.4.1 When a system certification program is required under the Contract, the DCERT shall include any additional supporting evidence required by the applicable ADF regulatory / assurance framework publication, as listed in clause 5.1 and specified in the SOW (including specifications), and the Approved governing plan for the system certification program.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-ECARS-V5.3

2. TITLE: EQUIPMENT CERTIFICATION TO ACCESS RADIOFREQUENCY SPECTRUM

3. DESCRIPTION AND INTENDED USE

3.1 The Equipment Certification to Access Radiofrequency Spectrum (ECARS) is required for the equipment, systems, sub-systems, Configuration Items (CIs), or end products that rely on the Radiofrequency Spectrum for their operation ('spectrum-dependant equipment'), as identified in accordance with the clause titled 'Access to the Radiofrequency Spectrum' in the SOW.

3.2 Radiofrequency Spectrum is a limited resource that must be shared between numerous Defence and civilian systems. The ability of a materiel solution to meet Defence's capability requirements may depend on sufficient Radiofrequency Spectrum access. Conversely, restricted and/or limited Radiofrequency Spectrum access may limit the capability of a solution.

3.3 The Australian regulatory framework for Radiofrequency Spectrum access is unique to that of other jurisdictions. In Australia, the Commonwealth may need to place restrictions on its utilisation of solutions that are compatible with other regulatory environments. Similarly, the Commonwealth may need to place restrictions on its utilisation of solutions that are designed to operate in Radiofrequency Spectrum designated for civilian.

3.4 The Contractor uses ECARS to advise the Commonwealth of the Radiofrequency Spectrum needs of proposed solutions and actual delivered.

3.5 The Commonwealth uses ECARS to:

a. assess proposed solutions for their compliance with Australian regulatory and Defence-specific requirements, and any restrictions on spectrum availability that may affect operational capability or system performance; and

b. obtain details of the technical characteristics of the delivered solution to support Radiofrequency Spectrum management for the operation of the delivered solution.

4. INTER-RELATIONSHIPS

4.1 The ECARS is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP); and

b. Contractor Engineering Management Plan (CEMP).

4.2 The ECARS inter-relates with the following data items, where these data items are required under the Contract:

a. Electromagnetic Environmental Effects Management Plan (E3MP);

b. System Specification (SS);

c. Support System Specification (SSSPEC);

d. Design Documentation; and

e. Design Certificate (DCERT).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

AA 763 form	Technical Characteristics for Spectrum-Dependent Equipment
EMS Manual	Electromagnetic Spectrum Manual

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.2 Specific Content

6.2.1 General Requirements

6.2.1.1 An AA 763 form is required for each separate equipment or system component that requires access to, use of, or relies on the Radiofrequency Spectrum for its operation.

6.2.2 Specific Requirements

6.2.2.1 The AA 763 shall consist of information entered onto all pages for each piece of equipment, system, sub-system, CI or end product that requires access to, use of, or relies on the Radiofrequency Spectrum for its operation.

6.2.2.2 The AA 763 forms are to be amended, as required, to reflect any hardware or software design changes that affect radiofrequency performance.

Note: Refer to the ‘DSO Guidance Document – Completing Form AA 763’ for further guidance when completing the AA 763. The Defence Spectrum Office Spectrum Planning and Engineering section, contactable at spectrum.planners@defence.gov.au, can provide further advice on the completion of the AA 763 form.

Annex:

A. Form AA 763

AA763 ECARS

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-HAR-V5.3

2. TITLE: HAZARD ANALYSIS REPORT

3. DESCRIPTION AND INTENDED USE

3.1 The purpose of the Hazard Analysis Report (HAR) is to document and communicate the results from a range of hazard analyses for achieving Materiel Safety and Environment related legislative compliance and contractual requirements. With regards to Materiel Safety and within the context of the individual report, the HAR demonstrates the achievement of Safety Outcomes. With regards to the Environment and within the context of the individual report, the HAR demonstrates the achievement of Environmental Outcomes. The HAR is used to report on a range of analyses, including the:

a. preliminary hazard analysis,

b. system hazard analysis,

c. subsystem hazard analysis,

d. operating and support hazard analysis,

e. health hazard assessment,

f. functional hazard analysis,

g. system-of-systems hazard analysis, and

h. environmental hazard analysis.

3.2 The Contractor uses the HAR to record and present the:

a. identified hazards to health, safety and the environment;

b. assessment of risks to health, safety and the environment associated with the identified hazards;

c. results of calculations, analyses, tests and examinations performed to confirm that:

(i) Safety Outcomes will be, or have been, met; and

(ii) Environmental Outcomes will be, or have been, met; and

d. identified controls and follow-on actions to be used in order to achieve Safety Outcomes and Environmental Outcomes.

3.3 The Commonwealth uses the HAR to:

a. understand the hazards and associated risks to health, safety and the environment associated with the Materiel System;

b. evaluate the Contractor's proposed controls for the identified hazards and risks;

c. assist with evaluating whether:

(i) Safety Outcomes will be, or have been, met; and

(ii) Environmental Outcomes will be, or have been, met; and

d. determine any follow-up actions that need to be undertaken by the Commonwealth in order to achieve Safety Outcomes and Environmental Outcomes.

4. INTER-RELATIONSHIPS

4.1 The HAR is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. System Safety Program Plan (SSPP);

c. Contractor Engineering Management Plan (CEMP); and

d. In-Service Materiel Safety Plan (IMSP).

4.2 The HAR inter-relates with the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP);

b. Hazard Log (HL);

c. Safety Case Report (SCR);

d. System Specification (SS);

e. Support System Specification (SSSPEC);

f. Design Documentation; and

g. Failure Mode, Effects and Criticality Analysis Report (FMECAR).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

ARPANSA Radiation Protection Series S-1	*Standards for Limiting Exposure to Radiofrequency Fields – 100 kHz to 300 GHz (2021)*
ARPANSA Radiation Protection Series S-1	*Advisory Note: Compliance of mobile or portable transmitting equipment (100 kHz to 300 GHz) (2021)*

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.1.3 When the Contract has specified delivery of another data item that contains aspects of the required information, the data item shall summarise these aspects and refer to the other data item.

6.2 Specific Content

6.2.1 Summary Results

6.2.1.1 The HAR shall include a summary of the results of the hazard analyses, including:

a. **System/Element Description:** A summary description of the physical and functional characteristics of the system, subsystems or other elements to which the analysis applies. The description shall identify and describe the major elements considered during the analysis and identify the boundaries associated with the elements and to the analysis. Reference to more detailed descriptions, including specifications and design documentation, is included where such documentation is available.

b. **Hazard analysis methods and techniques:** A description of each method and technique used to conduct the hazard analysis, including the assumptions made, the qualitative and quantitative data used, and traceability to the source data.

c. **Hazard Analysis Results Summary:** A summary of the significant hazard analysis results including a conclusion about the level of risk identified and that expected to remain after the application of the identified controls and recommendations.

6.2.2 Hazard Analysis Results

6.2.2.1 The data item shall contain the results from the hazard analyses applicable to the type of HAR required, as described by options 1 to 8 below, and in accordance with the Approved SSPP or Approved IMSP, as applicable.

6.2.2.2 Where a HL is required under the Contract and the HL is concurrently accessible to the Commonwealth, then the delivered HAR should minimise duplication and refer to the applicable update / data release of the HL to supplement and form part of the HAR.

6.2.3 Option 1 – Preliminary Hazard Analysis Report

6.2.3.1 When the HAR is to include a Preliminary Hazard Analysis Report (PHAR), the hazard analysis results within the PHAR shall include:

a. the identification and description of each hazard and its associated risks;

b. the severity category, probability of occurrence, and initial Hazard Risk Index (HRI) assigned to each of the hazard’s associated risks; and

c. a description of the potential risk mitigation measures.

6.2.4 Option 2 – System Hazard Analysis Report

6.2.4.1 When the HAR is to include a System Hazard Analysis Report (SHAR), the hazard analysis results within the SHAR shall, in respect of subsystems and interrelationships, include:

a. Verification of system compliance with the requirement to achieve Safety Outcomes;

b. previously unidentified hazards associated with the design and the analysis of associated risks;

c. recommended actions to eliminate the previously unidentified hazards and achieve Safety Outcomes;

d. a description of system and subsystem events and the results of associated failure analysis that could create hazards or result in increased risk;

e. the degradation of a subsystem or the total system;

f. design changes that affect subsystem hazards and associated risks;

g. the effects of human errors; and

h. the determination as to:

  (i) the contribution of system hardware and software events on potential mishaps;

  (ii) whether related design requirements in the System Specification (SS) and Support System Specification (SSSPEC), as applicable, have been met; and

  (iii) whether the methods for implementing design requirements and mitigating risk have introduced new hazards.

6.2.5 Option 3 – Subsystem Hazard Analysis Report

6.2.5.1 When the HAR is to include a Subsystem Hazard Analysis Report (SSHAR), the hazard analysis results within the SSHAR shall include:

a. Verification of subsystem compliance with the requirement to achieve Safety Outcomes;

a. previously unidentified hazards and the analysis of the associated risks; and

b. the determination as to:

  (i) the contribution of subsystem hardware and software events on potential mishaps;

  (ii) whether related design requirements in the System Specification (SS) and Support System Specification (SSSPEC), as applicable, have been met; and

(iii) whether the methods for implementing design requirements and mitigating risk have introduced new hazards; and

c. recommended actions to eliminate the previously unidentified hazards and achieve Safety Outcomes.

6.2.6 Option 4 – Operating and Support Hazard Analysis Report

6.2.6.1 When the HAR is to include an Operating and Support Hazard Analysis Report (O&SHAR), the hazard analysis results within the O&SHAR shall include:

a. details of operating and support activities involving known hazards;

b. required changes to functional and design requirements for system hardware, software and Support Resources, needed to achieve Safety Outcomes;

c. required features, devices, and equipment needed to achieve Safety Outcomes;

d. requirements for Personal Protective Equipment (PPE), including details of its limitations with regards to minimising health and safety risks;

e. requirements for warnings, cautions, and special emergency procedures within Technical Data;

f. requirements for packaging, handling, storage, and transportation to achieve Safety Outcomes;

g. requirements for the packaging, handling, storage, transportation, and disposal of Hazardous Chemicals;

h. Training requirements associated with the reduction of risks;

i. the effects of non-developmental items with other system components or subsystems;

j. potentially hazardous system modes under operator control; and

k. where applicable, details of existing comparable systems that provide background information relevant to operating and support hazard analysis.

6.2.7 Option 5 – Health Hazard Assessment

6.2.7.1 When the HAR is to include a Health Hazard Analysis Report (HHAR), the hazard analysis results within the HHAR shall include:

a. hazard identification and description, including the exposure pathway to persons (eg, inhalation, absorption) and exposure characterisation (eg, rate of exposure);

b. severity classification, probability of occurrence and the resulting HRI for each associated risk; and

c. recommended actions for achieving Safety Outcomes including, where a hazard cannot be eliminated, the risk level(s) expected to be achieved through mitigation.

6.2.7.2 In addition to the requirements of clause 6.2.7.1, if the hazard involves a Hazardous Chemical, the hazard analysis results shall include, for the Hazardous Chemical:

a. a cross-reference to the Safety Data Sheet (SDS), which shall be prepared in accordance with the requirements of DID-PM-HSE-SDS and delivered to the Commonwealth as supporting information to the HAR;

b. characteristics, including the quantity and hazard class;

c. a description of how it is used in each process or system component;

d. an estimated rate of use within each process or component for the subsystem, system, and the program-wide impact; and

e. the recommended disposition including, where applicable, possible substitution with less harmful alternatives.

6.2.7.3 In addition to the requirements of clause 6.2.7.1, if the hazard involves ergonomic factors, the hazard analysis results shall include:

a. a description, including all work performance criteria such as:

(i) physical properties of all system components that personnel will manually handle or wear, or that will support personnel body weight;

(ii) a task analysis that lists the physical and cognitive actions that personnel will perform during typical operations and routine maintenance; and

(iii) exposures to mechanical stress encountered while performing work tasks;

(iv) characteristics in the design of the system or work processes that could degrade performance or increase the likelihood of erroneous actions that may result in mishaps; and

b. requirements to operate and maintain the system from the sum of the physical and cognitive demands imposed on personnel and recommended strategies to reduce these demands through equipment or job redesign when considered necessary.

6.2.7.4 In addition to the requirements of clause 6.2.7.1, if the hazard involves environmental factors, the hazard analysis results shall include:

a. a description of anticipated whole body movement, including whole body vibration, vehicle shock, and motions that are likely to result in musculoskeletal disorders, disorientation, or motion sickness;

b. a description and quantification of the potential for blast overpressure and other sudden barotrauma and the estimated pressure changes, time and rate of onset, and frequency of occurrence;

c. the identity and categorization of the main noise and vibration sources in the new or modified system(s);

d. calculated estimates for noise, blast, and vibration levels and the identification of potential alternative processes and equipment that could minimise the adverse impacts;

e. a description of the anticipated effect of protective equipment and engineering changes, if required, for mitigating personnel exposures to noise and vibration; and

f. a description of the limitations of the protective equipment and the burden imposed with regard to weight, comfort, visibility, and the range of the population that would be accommodated.

6.2.7.5 In addition to the requirements of clause 6.2.7.1, where the hazard involves ionising and/or non-ionising radiation, the hazard analysis results shall include:

a. the physical characteristics of radiation hazards and the physiological processes by which the hazard can affect or harm people as well as the criteria for assessing the resulting risk;

b. an assessment of the RF exposure to personnel against the mandatory limits set in the ARPANSA Radiation Protection Series S-1, *Standard for Limiting Exposure to Radiofrequency Fields – 100 kHz to 300 GHz (2021)*; and

c. where the RF device is designed to be used close to the human body, an assessment of the specific absorption rate against the criteria in ARPANSA Radiation Protection Series S-1, *Advisory Note: Compliance of mobile or portable transmitting equipment (100 kHz To 300 GHz)*.

6.2.8 Option 6 – Functional Hazard Analysis Report

6.2.8.1 When the HAR is to include a Functional Hazard Analysis Report (FHAR), the hazard analysis results included within the FHAR shall include:

a. a decomposition of the system and its related subsystems to the major component level;

b. a functional description of each subsystem and component identified;

c. a functional description of interfaces between subsystems and components;

d. identified hazards associated with the loss of function, degraded function or a malfunction;

e. an assessment of the risk associated with each identified failure of a function, subsystem, or component, including severity classification, probability of occurrence and resulting HRI for each risk;

f. an assessment of whether the functions identified are to be implemented in the design's hardware, software, or human control interfaces;

g. an assessment of software control category and the assigned software criticality index for each safety-significant software function; and

h. a list of requirements and constraints, to be included in the SS and/or SSSPEC, as applicable, that when successfully implemented will achieve Safety Outcomes.

6.2.9 Option 7 – System-of-Systems Hazard Analysis Report

6.2.9.1 When the HAR is to include a System-of-Systems Hazard Analysis Report (SOSHAR), the hazard analysis results within the SOSHAR shall include the:

a. identified unique system-of-systems hazards and traceability of these hazards to architecture locations, interfaces, data, and the stakeholder(s) associated with each hazard;

b. risk assessment(s) for identified unique system-of-systems hazard(s), and recommend control measures for achieving Safety Outcomes; and

c. Verification and Validation of results for the effectiveness of recommended risk-mitigation measures.

6.2.10 Option 8 – Environmental Hazard Analysis Report

6.2.10.1 When the HAR is to include an Environmental Hazard Analysis Report (EHAR), the hazard analysis results within the EHAR shall include:

a. hazard identification and description, as applicable to the system's life-cycle when considering:

(i) the use of Problematic Substances and Problematic Sources and the generation of environmental contaminants during normal system operations and support functions;

(ii) demilitarisation and disposal;

(iii) public health;

(iv) impact on sea, air and land resources and related ecosystems; and

(v) inadvertent release of Problematic Substances or other contaminants (eg, via mishap);

b. severity classification, probability of occurrence and the resulting HRI for each associated risk, including any change to severity class descriptions if applicable;

c. reference to related documentation (eg, environmental impact statements); and

d. recommended actions for achieving Environmental Outcomes including, where a hazard to the Environment cannot be eliminated, the risk level(s) expected to be achieved through mitigation.

6.2.10.2 In addition to the requirements of clause 6.2.10.1, if the hazard involves a Problematic Substance, pollutant (including noise) or other contaminant, the hazard analysis results shall include, where applicable:

a. a cross-reference to the SDS, which shall be prepared in accordance with the requirements of DID-PM-HSE-SDS and delivered to the Commonwealth as supporting information to the HAR;

b. characteristics, including the relevant quantities and hazard class;

c. a description of how it is used or generated in each process or system component;

d. an estimated rate of use within each process or component for the subsystem, system, and the program-wide impact; and

e. the recommended disposition including, where applicable, possible substitution with less harmful alternatives.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-HL-V5.3

2. TITLE: HAZARD LOG

3. DESCRIPTION AND INTENDED USE

3.1 The purpose of the Hazard Log (HL) is to provide a closed-loop hazard tracking system to record the identification, analysis, treatment and management of hazards and their associated risks. The HL provides a repository for the results of hazard analyses and acts as a source of evidence for the evaluation, reporting and, where applicable, certification of Materiel System safety.

3.2 The Contractor uses the HL, consistent with the scope of the Contract, to:

a. record and manage identified hazards to health, safety and the environment associated with the Materiel System;

b. provide a closed-loop record of the risks to health, safety and the environment associated with the identified hazards;

c. record the acceptance and follow-on actions to achieve Safety Outcomes; and

d. provide information for hazard analysis reports and inputs into Technical Data, including operator and Maintenance manuals and Training materials.

3.3 The Commonwealth uses the HL:

a. to understand the hazards and associated risks to health, safety and the environment associated with the Materiel System,

b. to review the Contractor’s controls for the identified risks;

c. to assist with evaluating whether or not the residual risk is acceptable; and

d. as input to any actions arising from the system safety program that need to be undertaken by the Commonwealth with regard to Materiel System implementation.

4. INTER-RELATIONSHIPS

4.1 The HL is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. System Safety Program Plan (SSPP);

c. Contractor Engineering Management Plan (CEMP); and

d. In-Service Materiel Safety Plan (IMSP).

4.2 The HL inter-relates with the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP);

b. Hazard Analysis Report (HAR);

c. Safety Case Report (SCR);

d. Materiel Safety Assessment (MSA);

e. Health and Safety Management Plan (HSMP);

f. design documentation; and

g. Failure Mode, Effects and Criticality Analysis Report (FMECAR).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item shall be based in electronic format acceptable to the Commonwealth (eg, a non-proprietary database), capable of producing outputs for a particular hazard analysis activity (eg, for a Preliminary Hazard Analysis), or each mishap risk and hazard in the HL, or other defined subset of the HL.

6.1.3 When the Contract has specified delivery of another data item that contains aspects of the required information, the data item shall summarise these aspects and refer to the other data item (including, for databases, the appropriate entry records or indices).

6.2 Specific Content

6.2.1 Hazard Log Contents

6.2.1.1 The HL shall include the following information, as relevant to each mishap risk and hazard:

a. **Hazard Identification:** A unique hazard identification (index) number and brief description that identifies the hazard (eg, ‘unintended radiation emitted from radar set waveguide’).

b. **Hazard Description:** A detailed description of the potential/actual hazards inherent in the item being analysed, when resulting from normal or abnormal actions/ mishaps (eg, the hazards associated with the normal handling of a Problematic Substances as well as dealing with a spill of the Problematic Substances). The description is to identify the activities involving the hazard, the time periods, approximate frequency, and the number of personnel involved.

c. **Problematic Substances:** If hazards are associated with Problematic Substances, the following data shall also be recorded:

(i) identification of the Problematic Substances, including the common or trade name, chemical name, chemical formula or ingredients, identifying stock numbers, physical form (solid, liquid, gas), current manufacturers, and suppliers;

(ii) location of the Problematic Substances within the Mission System and Support System Components;

(iii) quantity of the Problematic Substances within the Mission System and Support System Components, with traceability to version-specific hardware designs;

(iv) application, process, or activity whereby quantities of the Problematic Substances are embedded into the Mission System or Support System Components, or used during operations and support of the Mission System;

(v) where a Problematic Substance is generated by the Materiel System, identify the circumstances under which generation occurs (eg, installation, test and evaluation, normal use, maintenance or repair of the system) and the quantity or rate of generation during operations and Maintenance;

(vi) reasonably anticipated quantities that may be discharged and the anticipated exposure rates during mishaps;

(vii) toxicity assessment, including a description of the expected frequency, duration, and amount of exposure (include the reference documentation, methods and calculations used to determine potency/toxicity assessment factors);

(viii) special control, training, handling measures, and Personal Protective Equipment (PPE) needed; and

(ix) reference to the applicable Safety Data Sheets (SDSs), which shall be prepared in accordance with DID-PM-HSE-SDS and delivered to the Commonwealth with the HL as supporting information.

d. **Problematic Sources:** If hazards are associated with Problematic Sources, the following data shall also be recorded:

(i) identification of the Problematic Source, including the name of the item that is or that contains the Problematic Source, the kind of Problematic Source (controlled material or controlled apparatus), type (ie, ionising or non-ionising radiation source) and the frequency or particle nature of the radiation, as applicable;

(ii) location of the Problematic Source within the Mission System and Support System Components;

(iii) the intended purpose and function of the Problematic Source;

(iv) for Problematic Sources that are controlled materials, the element or chemical name and symbol of the nuclide and its atomic mass, physical form (ie, solid, liquid or gas), chemical form (eg, organic compound), activity (in Becquerel), half life, recommended working life; and

(v) for Problematic Sources that are controlled apparatus, the operating parameters (eg, nominal and peak voltage), output parameters (eg, frequency range, wavelength, class), manufacturer and identification numbers, as applicable.

e. **Element Failure Mode(s):** Identify all element failure modes which can result in a hazard including human errors, single point and common mode failures. Include the effects of failures and events occurring in other subsystem elements, hazards arising from functional relationships between elements and the potential contribution of other subsystem (including those developed by other contractors/sources, off-the-shelf, non-developmental items, and GFE hardware or software) events, faults, and occurrences (such as improper timing). In the case of functional hazard analysis, consider modes which include the loss of function, degraded function or malfunction, or functioning out of time or out of sequence for the subsystems, components, and interfaces. Failure modes generally answer the question of ‘how’ it fails.

f. **Failure Propagation Mode(s):** Describe how the element failure mode can affect other elements, components, subsystems and systems. Identify the interfaces involved. In the case of functional hazard analysis, address functional interfaces in terms of connectivity and functional inputs and outputs. Consider the next effect in a possible mishap sequence until the final mishap outcome.

g. **System/Element:** Identify the system and element that this analysis is concerned with. For example, if a portion of the analysis applies to a particular subsystem, then identify the parent system and subsystem. In the case of a functional hazard analysis, indicate whether the function is expected to be implemented by hardware, software, or human control interfaces and, where known, identify implementing hardware or software components. Functions allocated to software should be mapped to the lowest level of technical design or configuration item prior to implementation.

h. **Applicability:** Identification of the version of specific hardware configurations of the system/subsystem or software releases, or Support System Component.

i. **Requirements references:** Identification details for documents that provide traceability to specifications, where applicable.

j. **System Event(s) Phase:** Describe the configuration or phase the system is in when the hazard is encountered; for example, during maintenance, during flight, during pre-flight, full-power applied, etc, or it could be encountered in all system events. Describe what is normally expected to occur as the result of operating the system/element during the system event phase.

k. **Causal factor:** Hardware, software, human, operational environment or other factors contributing to the creation of the hazard or the level of associated risk.

l. **Effect of Hazard:** Describe the detrimental (upstream and downstream) effects which could be inflicted on the subsystem, system, other equipment, facilities or personnel, resulting from this hazard.

m. **Hazard Indication:** Identify all warnings or other indications of the presence of the hazard to operational/maintenance personnel.

n. **Mishap:** Describe an event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

o. **Initial Risk Assessment:** Include an assessment of the risk associated with the hazard (classification of severity and probability of occurrence) and the resulting Hazard Risk Index. This is the assessment of the risk prior to taking any action to eliminate or control hazards and associated risks.

p. **Residual Risk Assessment:** Include an assessment of the residual risk associated with the hazard and the resulting Hazard Risk Index (HRI). This is the assessment of the risk after taking action to achieve Safety Outcomes.

q. **Event Risk Assessment:** Include an assessment of the risk associated with the hazard, and the resulting HRI, as it applies to a specified hardware/software configuration during an event. Typical events include developmental testing, operational testing, demonstrations, fielding, and post-fielding tests.

r. **Recommended Action:** Include risk mitigation measures (identified and selected with traceability to version specific hardware configurations or software releases) and recommended actions necessary to achieve Safety Outcomes. Sufficient technical detail is required in order to permit the Contractor and the Commonwealth to consult and adequately develop and assess criteria resulting from the analysis including the identification of:

(i) changes needed in functional or design requirements for system hardware, software, facilities, tooling, or support/test equipment;

(ii) alternative designs and life cycle cost impact where appropriate. In the case of a functional hazard analysis, identify the requirements and constraints (to be included in the specifications) that, when successfully implemented, will achieve Safety Outcomes (eg, requirements for fault tolerance, detection, isolation, annunciation, or recovery);

(iii) required warnings, cautions, signage, supervision, access controls, safe work methods and special emergency procedures, including those to be included in operator, materials handling and maintenance manuals, and Training;

(iv) requirements for packaging, handling, storage, and transportation;

(v) requirements for Personal Protective Equipment (PPE), where needed, and limitations for PPE use; and

(vi) any other information related to managing risks to health, safety and the environment.

s. **Status:** Provide the status of actions to implement the recommended, or other, hazard controls. The status shall include not only an indication of ‘open’ or ‘closed’ but also reference to the evidence, including applicable drawing(s), specification(s) and procedure(s), which support closure of the particular hazard.

t. **V&V method:** The V&V methods for risks and risk reduction following mitigation.

u. **Owner:** Person(s) and/or organisational element responsible for managing the particular hazard and its associated risks.

v. **Risk Acceptance:** Record of risk acceptance(s), including:

(i) the Contractor’s risk acceptance authority by title and organisation, and date of acceptance;

(ii) the Commonwealth authority’s concurrence, as applicable, by title and organisation, and date of risk acceptance;

(iii) where applicable, the Approval by the Commonwealth Representative of a Problematic Substance or Problematic Source, within the applicable system or element; and

(iv) identification details for the signed risk acceptance document(s).

Note: Commonwealth 'risk acceptance' is not Acceptance. It acknowledges Commonwealth concurrence with the Contractor's approach to minimising health, safety and Environmental risks. If a Problematic Substance or Problematic Source is the subject of risk acceptance, the HL records Commonwealth Approval of that Problematic Substance or Problematic Source, within the context of that risk.

w. **Hazard management log:** A record of the hazard entry and changes made to any part of the hazard record during the system's life-cycle.

x. **Remarks:** Include any other information relating to the hazard not covered elsewhere by this DID (eg, applicable documents, previous failure data on similar systems, or administrative directions).

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-PSECDD-V5.3

2. TITLE: PHYSICAL SECURITY DESIGN DOCUMENT (PSECDD)

3. DESCRIPTION AND INTENDED USE

3.1 The Physical Security Design Document (PSecDD) sets out how the design of the Mission System implements the physical security requirements and guidance contained in:

a. the System Specification (SS) for each different type of Mission System;

b. the applicable documents identified at clause 5.1; and

c. any other applicable physical security standards, as determined by the Contractor.

Notes:

- ***The earlier version(s) of the PSecDD describe the design approach to satisfy the physical security requirements, while the later version(s) set out the record of the actual implementation of the design to provide one of the artefacts required for Security Authorisation(s) for the physical security for the Mission System.***
- ***The Contractor prepares the PSecDD under guidance from the Commonwealth Representative, and the Commonwealth submits the document to the relevant authority(ies) in support of the required Security Authorisation(s) for the physical security of the Mission System.***

3.2 The Contractor uses the PSecDD as one of the physical security artefacts:

a. to detail the design approaches to be used, or that have been used, to address the physical security requirements as they apply to the Mission System;

b. to advise the Commonwealth and the associated Security Authorisation authority(ies) for the physical security of the design solution used to address the physical security requirements for the Mission System, including those physical security requirements needed for Information and Communications Technology (ICT) security and cyber security; and

c. to provide assurance to the Commonwealth that the Contractor’s system security program will enable the physical security requirements for the Mission System to be achieved.

3.3 The Commonwealth uses the PSecDD:

a. to gain assurance that physical security considerations are taken into account during the design and implementation of the Mission System;

b. to understand and evaluate the Contractor’s approach to meeting the physical security requirements for the Mission System as part of the system security program;

c. to identify and understand the Commonwealth’s involvement in the Contractor’s physical security program, including the monitoring of the Contractor’s program; and

d. as one of the suite of physical security artefacts provided to the relevant Defence authorities as part of obtaining the required Security Authorisation(s) for physical security for the Mission System.

4. INTER-RELATIONSHIPS

4.1 The PSecDD is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Contractor Engineering Management Plan (CEMP);

c. Materiel System Security Management Plan (MSSMP);

d. In-Service Security Management Plan (ISSMP); and

e. ADF regulatory / assurance plans.

4.2 The PSecDD inter-relates with the following data items, where these data items are required under the Contract:

a. SS for each different type of Mission System;

b. System Architecture Description (SAD);

c. the security-related data items required under the Contract (other than those identified under clause 4.1);

d. Mission System Technical Documentation Tree (MSTDT); and

e. the Verification and Validation (V&V) data items required under the Contract (eg, V&V Plan (V&VP), Verification Cross Reference Matrix (VCRM), and Acceptance Test Reports (ATRs)).

5. APPLICABLE DOCUMENTS

Note to drafters: Amend the reference documents to suit the requirements of the Contract.

5.1 The following documents form a part of this DID to the extent specified herein:

Governing Security Documents	(see the Glossary for the definition of this term)
	Physical Security Standards – HMA Ships, Submarines & Watercraft, Version 4.0, 17Dec20

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Introduction

6.2.1.1 The PSecDD shall provide a brief overview of the Mission System, including its purpose.

6.2.1.2 The PSecDD shall describe the purpose, scope and objectives of the PSecDD, including identifying the information required by the Security Authorisation authority(ies) in support of the required Security Authorisation(s) for physical security for the Mission System.

6.2.1.3 The PSecDD shall describe the constraints and assumptions associated with the PSecDD, including in relation to the design and implementation of the physical security requirements.

6.2.1.4 The PSecDD shall set out any conventions used throughout the document to satisfy the requirements of this DID.

6.2.2 Physical Security Threat and Risk Assessment

6.2.2.1 The PSecDD shall set out the physical security threat and risk assessment for the Mission System, as determined in accordance with the processes set out in the Approved MSSMP.

6.2.3 General Requirements

6.2.3.1 The PSecDD shall provide a summary of the physical security requirements to be met by the Mission System, including:

a. the requirements contained in the Mission System SS;

b. the requirements derived from the applicable documents identified at clause 5.1;

c. the physical security threat and risk assessment pursuant to clause 6.2.2 of this DID; and

d. any other requirement sources used by the Contractor.

6.2.3.2 The PSecDD shall:

a. identify all elements of the Mission System's design that have a bearing on physical security for the Mission System;

b. provide an assessment on a building-by-building, room-by-room and/or compartment-by-compartment (as applicable) assessment of the physical security design requirements for the Mission System; and

c. summarise all identified security considerations.

6.2.4 Design Description

6.2.4.1 The PSecDD shall describe the design of the Mission System to satisfy the physical security requirements of the Mission System identified pursuant to clause 6.2.3.1 of this DID, including:

a. an overview of the design philosophy employed;

b. details of the physical security design for each of the Mission System buildings/rooms/compartments, including construction details;

c. details on the physical security design associated with following specific subjects:

(i) weapons and deployable systems;

(ii) Digitally Enabled Systems and Equipment (DESE) and associated networks (eg, to prevent tampering and mitigate cyber-related risks);

(iii) drugs and medical supplies;

(iv) classified materials, including documentation and equipment;

(v) cash and valuables;

(vi) attractive areas (ie, attractive targets for theft, misuse or unauthorised access);

(vii) key management containers;

(viii) safes; and

(ix) security hardware; and

d. any other information required by the Security Authorisation authority(ies) to achieve the required Security Authorisation(s) for physical security.

6.2.4.2 The design description shall include drawings, scenarios of operation, and any other materials needed to set out the physical security design of the Mission System so that the Security Authorisation authority(ies) can properly assess the Mission System as designed.

6.2.5 Physical Security Implementation

6.2.5.1 After construction of the Mission System is complete and as required by the CDRL, the PSecDD shall describe the actual implementation to satisfy the physical security requirements, including:

a. the implementation details associated with the items identified under clause 6.2.4 of this DID; and

b. the Verification and Validation results that confirm that the physical security requirements identified pursuant to clause 6.2.3.1 of this DID have been satisfied.

Note: At this time, the PSecDD may be renamed to "Physical Security Design Record (PSecDR)".

6.2.5.2 The implementation description shall include any issues that may have arisen due to changes to the physical security requirements that have changed since the design and construction baselines were established.

6.2.5.3 The implementation description shall include drawings, photographs, and any other materials needed to set out the actual physical security implementation details for the Mission System so that the Security Authorisation authority(ies) can properly assess the Mission System as built.

6.2.6 Physical Security Data Pack

6.2.6.1 This PSecDD shall identify the Engineering Design Data files (eg, three-dimensional modelling and computer-aided design data) for the systems and equipment installed into the Mission System, which document how the Mission System complies with the physical security requirements.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-SCR-V5.3

2. TITLE: SAFETY CASE REPORT

3. DESCRIPTION AND INTENDED USE

3.1 The Safety Case Report (SCR) documents a comprehensive evaluation, at the time of the report, of the mishap and safety hazards and their associated risks prior to test or operation of the system, following system modification, or prior to the Acceptance of Mission Systems and applicable Support System Components. The SCR, including by reference to other system-safety related data items (which in totality form the 'Safety Case'), identifies the hazards, associated risks, and measures to ensure that hazards have been eliminated so far as is reasonably practicable or, if it is not reasonably practicable to eliminate hazards, the measures to eliminate (or, otherwise, minimise) the associated risks so far as is reasonably practicable – in summary, all of the evidence needed to demonstrate that Safety Outcomes have been, or will be[1], met. The SCR documents the consultation outcomes between the Commonwealth and Contractor and formal risk acceptance decisions made.

3.2 The Contractor uses the SCR to present an argument, supported by a body of evidence, to show that:

a. when used in relation to the Acceptance of Supplies, the Materiel System is safe for the purposes which are expressly stated, as Safety Outcomes have been met;

b. the applicable safety requirements, including relevant Australian legislation, design rules, standards, and codes of practice, have been satisfied; and

c. the safety requirements established by any applicable certification authorities have been satisfied.

3.3 The Commonwealth uses the SCR:

a. to determine that the system hazards to health and safety have been identified and that Safety Outcomes have been, or will be, met;

b. to determine that the associated certification requirements have been satisfied;

c. when applicable, as a basis for evaluating Materiel Safety prior to the Acceptance of Supplies;

d. to obtain necessary safety certifications from Defence regulatory and safety authorities; and

e. as the basis for assessing and managing health and safety risks throughout the system's life-cycle.

4. INTER-RELATIONSHIPS

4.1 The SCR inter-relates with the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP);

b. Systems Engineering Management Plan (SEMP);

c. System Safety Program Plan (SSPP);

d. In-Service Materiel Safety Plan (IMSP);

e. Software Management Plan (SWMP);

f. Hazard Analysis Report (HAR); and

[1] Reference to 'will be' acknowledges that some measures can only be established through Defence processes and training.

g. Hazard Log (HL).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the SCR shall summarise these aspects and refer to the other data item as part of the body of evidence.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The SCR shall comprise a comprehensive and structured body of evidence that demonstrates, by reasoned argument, that the delivered Materiel System is suitable for Acceptance with respect to Materiel Safety.

6.2.1.2 The SCR shall include an executive summary.

6.2.1.3 Subject to clause 6.1.2, the SCR shall provide a description of the Materiel System to which the Safety Case relates, including:

a. the applicable configuration(s), roles, functions and environments, system boundaries, major and safety-critical components and areas of safety-related risk that are worthy of particular attention; and

b. where relevant, any interfaces and interactions with other systems and personnel that may present safety-related interface risks that cannot be managed by a single Contractor or Commonwealth entity.

6.2.2 System Safety Program

6.2.2.1 The SCR shall provide a description of the system-safety program employed by the Contractor to provide assurances as to the integrity of the process used to develop and update the Safety Case, including the current assessment of Materiel Safety.

6.2.2.2 The description of the system-safety program shall summarise the analyses performed to achieve Safety Outcomes, which is to include:

a. the safety engineering and safety management processes employed to meet the safety-related requirements of the Contract;

b. internal and external audits conducted during the development of the Supplies to provide assurances that the system-safety management system was implemented as defined;

c. details of relevant design and safety certificates or licences; and

d. the responsibilities and accountabilities of Key Persons involved in the safety engineering and safety management program.

6.2.2.3 The SCR shall summarise the requirements, criteria and methodology used to classify and rank hazards, including any assumptions on which the criteria or methodologies were based or derived including the definitions for the hazard risk indices and of acceptable risk. Where data for extant subsystems, components and interfaces were incorporated into the analysis, the SCR shall summarise how that existing data was validated and, if necessary, adapted for the configuration, role and environment applicable to the Materiel System.

6.2.3 Materiel Safety Assessment

6.2.3.1 The SCR shall demonstrate, through assessment based on objective quality evidence, how the Materiel System achieves safety-related requirements specified under the Contract, the requirements of relevant Australian legislation, codes of practice, civil and Defence regulatory requirements, and applicable design and safety standards.

6.2.3.2 The SCR shall contain the objective quality evidence used to demonstrate Materiel Safety including:

a. a list of all safety-related risks with a residual (ie, post-treatment) risk level (as documented in the hazard risk index) of medium or above, or as otherwise defined in the Approved SSPP;

b. subject to clause 6.1.2, the Hazard Log;

c. subject to clause 6.1.2, results of the hazard analyses conducted;

d. subject to clause 6.1.2, the details of any calculations, analyses, tests or examinations necessary to demonstrate that Safety Outcomes have been, or will be, met including the actions undertaken to:

(i) identify system hazards that could give rise to risks to health and safety, and the associated risks to health and safety;

(ii) evaluate the actions taken to eliminate the hazards and associated risks to health and safety so far as is reasonably practicable and, where elimination is not reasonably practicable, to minimise the associated risks to health and safety so far as is reasonably practicable; and

(iii) validate safety criteria, requirements and analyses;

e. subject to clause 6.1.2, recommendations applicable to hazards at, or caused by, the interface between the Supplies and other system(s), where applicable;

f. for the Mission System subsystems (eg, pressure vessels) and Support System Components (eg, hoists, cranes) included in the Supplies that are or that contain items of plant where registration of the design of that plant is required under WHS Legislation[2], copies of the registration documents provided by the Commonwealth, State or Territory regulator;

g. evidence that all applicable certifications (other than Australian design registration details included in the SCR in accordance with clause 6.2.3.2f) and necessary safety-related compliance assurance activities, as required by applicable third party regulatory and safety authorities, have been met;

h. a list of all pertinent reference materials including reports, standards and regulations, specifications and requirements documents, design documentation, Safety Data Sheets, and operating, maintenance and other manuals; and

i. subject to clause 6.1.2, any additional supporting evidence reasonably required by the Commonwealth for the purposes of demonstrating Materiel Safety.

6.2.3.3 The SCR shall contain a summary statement, signed by the Contractor's technical authority, declaring that the system's Materiel Safety requirements have been met and the system's readiness for test, to operate or to otherwise proceed to the next phase of its life cycle.

[2] Refer to Part 5.3 of the *WHS Regulations 2011* (Cth).

DATA ITEM DESCRIPTION

1. DID NAME: DID-ENG-SOL-SRMP-V5.3

2. TITLE: SECURITY RISK MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Security Risk Management Plan (SRMP) is used to identify and track threats to Information and Communications (ICT) security and cyber security, the associated risk assessments, the risk treatment options, and the existing and proposed risk controls associated with a Security System-of-Interest (SSoI) (eg, the Mission System), including during development, Verification and Validation (V&V), commissioning, operation and support, so that Defence is able to understand the level of risk exposure posed by the system. The Approved governing plan (eg, Materiel System Security Management Plan (MSSMP) or In-Service Security Management Plan (ISSMP)) provides the plan and associated processes for managing the risks associated with ICT security and cyber security, while the SRMP addresses only the risk assessment aspects of ICT/cyber-security risk management for the Targets of Security Assessment (ToSAs) for a SSoI. This includes the Digitally Enabled Systems and Equipment (DESE) within each SSoI.

Note: This DID has been written on the basis that all ToSAs for a SSoI will be addressed within a single SRMP (including when the ToSA and the SSoI are one and the same). Where this is not the case, such as may occur for larger Mission Systems (eg, aircraft or ship), the requirements of the DID should be interpreted in the context of the set of SRMPs and associated ToSAs. The ToSAs are either identified in the Approved governing plan or in the System Security Plan(s) (SSP(s)) for a SSoI.

3.2 The SRMP serves two purposes:

a. during the design and implementation phases for a SSoI, it provides a supporting artefact for the design process, describing the risk assessment and proposed risk treatments for the identified threats, to demonstrate that the ICT/cyber-security controls are suitable and sufficient and the SSoI is likely to be assessed to be As Secure As Reasonably Practicable (ASARP); and

b. during the Security Authorisation assessment phases for a SSoI, it provides a consolidated reference or summary of the risk basis underpinning the ICT/cyber-security controls that have or have not been implemented, and is one of the artefacts for obtaining the required Security Authorisations for ICT security and cyber security.

3.3 The Contractor uses the SRMP:

a. to document the ICT/cyber-security threats and associated risk assessments for a SSoI;

b. to document the risk-treatment options and associated plans, the existing and proposed risk controls, the controls not implemented and not proposed to be implemented, and the residual risk exposure;

c. to advise the Commonwealth and the ICT and cyber Security Authorisation assessor(s) of the ICT/cyber-security threat and risk assessments associated with a SSoI/ToSA during the design, implementation and assessment phases; and

d. as one of the ICT/cyber-security artefacts to provide assurance to the Commonwealth that the Contractor’s ICT/cyber-security activities will enable the Security Outcomes for a SSoI to be achieved, particularly to demonstrate that the SSoI/ToSA is ASARP.

3.4 The Commonwealth uses the SRMP:

a. to understand, assess and manage ICT/cyber-security risks associated with a SSoI, including to review the Contractor’s controls for the identified risks and to assist with evaluating whether or not the residual risk is acceptable;

b. to understand and evaluate the Contractor’s approach to meeting the ICT/cyber-security requirements of the Contract as part of the system security program, including to understand the Commonwealth's involvement in the Contractor's ICT/cyber-security program;

c. as an input to its own planning, including to identify any actions arising from the system security program that need to be undertaken by the Commonwealth with regard to the implementation of a SSoI; and

d. as one of the suite of ICT/cyber-security artefacts provided to the relevant security authorities as part of obtaining the required ICT and cyber Security Authorisations for a SSoI.

4. INTER-RELATIONSHIPS

4.1 The SRMP is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Contractor Engineering Management Plan (CEMP);

c. Materiel System Security Management Plan (MSSMP);

d. In-Service Security Management Plan (ISSMP);

e. System Safety Program Plan (SSPP); and

f. In-service Materiel Safety Plan (IMSP).

4.2 The SRMP inter-relates with the following data items, where these data items are required under the Contract:

a. System Specification (SS) for each different type of SSoI;

b. the security-related data items required under the Contract (other than those identified under clause 4.1); and

c. the safety-related data items (eg, Hazard Log and Safety Case Report (SCR) or Materiel Safety Assessment (MSA)).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Note to drafters: Amend the following list of Applicable Documents to suit the requirements of the Contract. Do not include documents that are included within the 'Governing Security Documents'.

Governing Security Documents	(see the Glossary for the definition of this term)
NIST CSF 2.0	National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Version 2.0, February 26, 2024
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1, September 2012
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations, Revision 5, September 2020
NIST SP 800-53A	Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5, January 2022
NIST SP 800-82	Guide to Operational Technology Security, Revision 3, September 2023
ISA/IEC 62433 series	Security for Industrial Automation and Control Systems

ISO/IEC 27005:2022	Information security, cybersecurity and privacy protection – Guidance on managing information security risks

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 Subject to clause 6.1.2, the data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 Where a SRMP is required for an ICT Security Authorisation, the format and content requirements for the SRMP shall comply with any template for a SRMP issued by Defence in addition to the content requirements set out in clauses 6.1.3 to 6.1.7 and clause 6.2 of this DID.

Note to drafters: The SRMP implements the risk processes defined in the Approved governing plan. Attention is drawn to the Note to drafters in the MSSMP and ISSMP DIDs, which highlights the implications associated with the selection of either the CASG 5x5 matrix or the PSPF 6x6 matrix as the basis for these risk processes.

6.1.3 The SRMP shall be consistent with and, where applicable, comply with the Governing Security Documents. The SRMP shall accord with the risk management framework documented in the Approved governing plan (eg, SEMP, MSSMP or ISSMP), as applicable.

6.1.4 Where the Approved governing plan identifies that more than one SRMP will be developed to address the ToSAs within an SSoI, each SRMP shall identify the full scope of ToSAs and the associated SRMPs for the SSoI, including the relationships between them (if any).

6.1.5 While early versions of the SRMP for a SSoI may contain threats and risk assessments for one or more components of, or ToSAs for, a SSoI, the final version of the SRMP for a SSoI shall contain the complete set of threats and associated risk assessments for all ToSAs within the SSoI.

6.1.6 When the Contract has specified delivery of another data item that contains aspects of the required information, the SRMP should summarise these aspects and refer to the other data item.

6.1.7 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content – Part 1

6.2.1 Executive Summary

6.2.1.1 The SRMP shall include a system-level summary of the SRMP, including:

a. an overview of the ToSAs and the SSoI being assessed;

b. a brief description of the risk-assessment process that has been undertaken, cross-referring to the Approved governing plan, as appropriate;

c. a summary table of the threats considered alongside the severity of risk exposures associated with these threats; and

d. the significant conclusions of the SRMP.

6.2.2 Scope

6.2.2.1 The SRMP shall define the scope of the threat and risk assessment that has been undertaken, identifying the SSoI, the ToSAs addressed by the SRMP, the associated SSP(s), and the SSoI assets under threat.

6.2.2.2 The SRMP shall identify the stakeholders associated with the SSoI and the ToSAs, including the System Owner, project sponsor, acquirer, user, developer, support agencies, and the relevant authorities for each different type of required Security Authorisation.

6.2.2.3 The SRMP shall identify any assumptions and constraints associated with the threat and risk assessments conducted for the ToSAs and/or the SSoI, including any factors relating to the SRMP which are assumed but not confirmed and which have constrained the assessment of security risk for the ToSAs/SSoI.

6.2.3 Threat and Risk Assessment

6.2.3.1 The threat and risk assessment elements of the SRMP shall describe how the Applicable Documents listed at clause 5 have been utilised to ensure that the SRMP will achieve the purposes and required outcomes set out in clause 3.

6.2.3.2 The SRMP shall describe the threat identification and modelling methodology applied (eg, attack trees, MITRE ATT&CK® framework, STRIDE[1] threat model, context analysis, operational scenario analysis, or a combination of methodologies), including the use of threat intelligence sources and reporting.

Note: In addressing the following requirement, the SRMP only needs to address the most applicable threats relevant to the SSoI (or element thereof) and its operating context. The analysis should be informed by both cyber threat intelligence reporting and knowledge of the SSoI design and the associated operational and support concepts.

6.2.3.3 The SRMP shall identify and describe the threats applicable to the scope of the assessment addressed through the SRMP, including identifying the risk threat profile that will help to predict potential future attacks and/or attack trends applicable to the SSoI.

6.2.3.4 The SRMP shall address ICT/cyber-security risks in relation to:

a. confidentiality, integrity and availability of systems and data; and

b. the cyber-security functions of Identify, Protect, Detect, Respond and Recover (as these terms are defined in NIST CSF 2.0).

6.2.3.5 For each identified threat, the SRMP shall include the following information:

a. threat title and unique identifier;

b. threat description, including threat type and characteristics, including the causes of the threat (ie, what needs to occur for the threat to eventuate);

c. threat source(s) (ie, the sources (malicious or otherwise) likely to realise the threat, including the actors or agencies behind the threat (if known));

d. asset(s) affected (ie, which systems, subsystems and assets identified in the 'scope' section are vulnerable to the threat), including any potential downstream or upstream implications for other systems that interact with, or interface to, the SSoI/ToSA;

e. overview (ie, a short description of how the threat sources and affected assets link to the threat for the ToSAs/SSoI, including how the threat accesses or compromises the system, subsystem or asset, or what circumstances, phases or locations does the threat present itself);

f. likelihood of occurrence;

g. consequence of realisation in terms of confidentiality, integrity and availability of systems and data, and the impacts of these consequences on the mission, safe operation of the ToSAs/SSoI, information security, or some other function or combination of functions;

Notes:

a. The information provided in response to the following requirement will evolve as the design and implementation of the ToSA/SSoI progresses (ie, as a control to be implemented becomes an existing control).

b. The Approved SSP will identify the publications from which the controls have been derived, which will include the ISM and DSPF and any complementary publications (eg, NIST SP 800-82 or ISA-62443 series) agreed by the Commonwealth.

h. controls to be incorporated, including:

(i) existing controls (ie, the controls already implemented in the ToSA/SSoI);

[1] STRIDE is an acronym for six threat categories: Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges

(ii) other controls that the Contract intends to implement, either fully or partially;

(iii) other available controls that the Contractor does not intend to implement (either fully or partially),

as set out in the associated SSP(s), including the Contractor's assessment as to whether the controls are effective at managing the threats/risks to the SSoI;

i. resultant risk exposure;

j. treatment option (ie, acceptance, reduction, transfer or avoidance);

k. treatment recommendation(s);

l. residual likelihood of occurrence after the identified treatment recommendations, which involve implementation actions, have been implemented;

m. residual consequence of realisation after the identified treatment recommendations, which involve implementation actions, have been implemented; and

n. residual risk exposure.

6.2.3.6 For all threats that affect the safe operation and/or support of the SSoI, the risk assessments and associated controls for these threats shall be entered into the Hazard Log element of the SCR/MSA, and managed in accordance with the Approved SSPP. The SRMP shall identify the specific ICT/cyber threats and risk assessments that are being managed through the system safety program.

6.2.3.7 The SRMP shall propose security controls for each risk for which the risk-treatment option is to reduce the likelihood and/or reduce the consequence.

6.3 Specific Content – Part 2

Note: During the Security Authorisation assessment phases for a SSoI, the following elements of the SRMP will provide input information for the Plan Of Action and Milestones (POAM), which will be developed by the Commonwealth as one of the required artefacts for obtaining the Security Authorisations for ICT security and cyber security.

6.3.1 Risk Treatment Planning

6.3.1.1 The SRMP shall set out the Contractor's risk-treatment plan for each risk for which the risk-treatment option is to either:

a. reduce the likelihood and/or reduce the consequence; or

b. avoid the risk, but a change to the design of the SSoI is required to enable such avoidance to occur,

with the aim of demonstrating that these risk-treatment plans, once implemented, will be sufficient to ensure that the SSoI will be ASARP.

6.3.1.2 Each risk-treatment plan shall include:

a. the position responsible;

b. a brief description of the required scope of work;

c. the envisaged schedule for implementation, including the associated milestones;

d. the likely resources;

e. the envisaged cost; and

f. any other relevant information (eg, implementation risks and Verification activities).

6.3.2 Residual Risk Exposure

6.3.2.1 The SRMP shall record whether the residual risk exposure associated with each threat has been accepted by the Commonwealth in support of:

a. if applicable, ICT Security Authorisation for the SSoIs (or elements thereof); and

b. cyber Security Authorisation for the SSoIs (or elements thereof).

6.3.2.2 The record of risk acceptance required under clause 6.3.2.1 shall include:

a. the Contractor's risk acceptance authority by title and organisation, and date of acceptance;

b. the Commonwealth authority's concurrence or non-concurrence, as applicable, by title and organisation, and date of risk acceptance; and

c. identification details for the signed risk acceptance document(s).

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-SSOP-V5.3

2. TITLE: SECURITY STANDARD OPERATING PROCEDURE

3. DESCRIPTION AND INTENDED USE

3.1 Security Standard Operating Procedures (SSOPs) provide step-by-step guidance to be followed by each different role (eg, system administrator and system operator) required to undertake security-related tasks and processes for a Security System-of-Interest (SSoI) (eg, Mission System) when the SSoI is being operated and sustained. The SSOPs address Information and Communications Technology (ICT) security, cyber security and, if applicable, physical security, and Emanation Security (EMSEC). SSOPs supplement the information provided in the associated System Security Plan(s) (SSP(s)) and the In-Service Security Management Plan (ISSMP) to:

a. ensure that all parties involved in operating, supporting and managing a SSoI understand their roles and responsibilities in relation to security;

b. assist with mitigating the risks associated with security threats;

c. assist with ensuring that security threats and incidents are appropriately managed and the impacts on the operations of a SSoI are minimised; and

d. assist with managing and maintaining Security Authorisations over the life of the SSoI.

3.2 The Contractor uses the SSOPs:

a. to document the procedures required to undertake security related tasks and processes for a SSoI; and

b. as one of the security artefacts to provide assurance to the Commonwealth that the Contractor’s security activities will enable the required Security Authorisations for a SSoI to be achieved.

3.3 The Commonwealth uses the SSOPs:

a. to gain assurance that the Contractor has a sound security program in place that complies with applicable Government and Defence security requirements and policies;

b. to understand and evaluate the Contractor’s approach to meeting the security requirements of the Contract as part of the system security program;

c. to identify and understand the Commonwealth’s involvement in the Contractor’s security program, including the monitoring of the Contractor’s program;

d. as an input to its own planning, including in relation to attaining the required Security Authorisations for the SSoI covered by the SSOPs; and

e. as one of the suite of security artefacts provided to the relevant Defence authorities as part of obtaining the required Security Authorisations for a SSoI.

4. INTER-RELATIONSHIPS

4.1 SSOPs are subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Contractor Engineering Management Plan (CEMP)

c. Integrated Support Plan (ISP);

d. Materiel System Security Management Plan (MSSMP);

e. In-Service Security Management Plan (ISSMP);

f. System Safety Program Plan (SSPP); and

g. In-service Materiel Safety Plan (ISMP).

4.2 SSOPs inter-relate with the following data items, where these data items are required under the Contract:

a. System Specification (SS) for each different type of SSoI;

b. the security-related data items required under the Contract (other than those identified under clause 4.1 (eg, SSP));

c. the safety-related data items (eg, Safety Case Report (SCR) and Hazard Log); and

d. Verification and Validation (V&V) data items, such as the V&V Plan (V&VP), Verification Cross Reference Matrix (VCRM), Acceptance Test Plans (ATPs), and Acceptance Test Reports (ATRs).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Governing Security Documents	(see the Glossary for the definition of this term)

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 Subject to clause 6.1.2, the data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 Where a set of SSOPs is required for an ICT Security Authorisation, the format and content requirements for the SSOPs shall comply with any template for a SSOP issued by Defence in addition to the content requirements set out in clauses 6.1.3-6.1.5 and clause 6.2 of this DID.

6.1.3 The set of SSOPs for a SSoI shall provide sufficient information to satisfy the objectives and purposes set out in clause 3, including to ensure that the information provided in the SSOPs is suitable for the applicable stages of the security design and implementation activities and the Security Authorisation requirements for the SSoI.

6.1.4 Each SSOP shall be consistent with and, where applicable, comply with the Applicable Documents identified at clause 5.

6.1.5 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

Note: Where there are classified aspects to the employment of an SSoI that have not been provided to the Contractor (eg, utilisation of the Mission System in a tactical environment), the Commonwealth will need to supplement the SSOPs provided by the Contractor to incorporate this information before the SSOPs are issued for use.

6.2.1 Scope

6.2.1.1 Each SSOP shall set out the scope of coverage of the SSOP as it relates to the SSoI.

6.2.1.2 Each SSOP shall identify the set of SSOPs for a SSoI, showing how this SSOP integrates with the set of SSOPs.

6.2.2 Roles

6.2.2.1 The SSOPs shall identify the set of roles that have security responsibilities for the SSoI (eg, security manager, security officer, system administrator, system operator and system support staff) to meet the requirements of the SSP and related documents.

6.2.2.2 For each identified role, the SSOPs shall address any specific security-related requirements and/or restrictions, such as identifying:

a. the security clearance requirements and any security-related restrictions (eg, with respect to dual nationality or particular ‘eyes only’);

b. the personnel who are or will be ‘authorised’ or ‘emergency authorised’ or who are ‘un-authorised’ personnel; and

c. any role-specific restrictions (eg, limitations on duration in roles, whether individuals can perform multiple roles, and conflicting roles).

6.2.3 Procedures

6.2.3.1 The SSOPs shall document the step-by-step requirements and guidance that must be followed by the individuals performing the roles identified through clause 6.2.2 to meet the requirements of the SSP and related documents.

6.2.3.2 In meeting the requirements of clause 6.2.3.1, the set of SSOPs shall address the following procedural requirements, as allocated to each of the identified roles:

a. physical security aspects, such as:

(i) monitoring and managing access control;

(ii) identification and management of personnel authorised for entry, distribution and security of physical keys; and

(iii) the management and storage of cryptographic keying material;

b. access and account management;

c. training, including on-the-job training, in relation to security induction, awareness, responsibilities, incident response, and other matters pertinent to the management, operation and support of the SSoI;

d. security Preventive Maintenance activities (eg, updating anti-virus software; managing removable media; data backup; event log monitoring; and checking the integrity of physical security devices, EMSEC protection measures, and system software);

e. security Corrective Maintenance activities (eg, recovering from a system failure caused by a security incident);

f. managing security incidents, including:

(i) reporting security incidents; and

(ii) ensuring that evidence is protected and not lost, deleted or corrupted;

g. disaster recovery;

h. system updates and upgrades, including Software Configuration Management and Software Release management;

i. supply chain security; and

j. general security matters applicable to all system users and maintainers, such as:

(i) who has responsibility for which aspects of security;

(ii) warnings that user’s actions may be audited and users will be held accountable for their actions;

(iii) guidelines on choosing and protecting passwords;

(iv) guidelines on enforcing need-to-know on the system;

(v) what to do in the case of a suspected or actual security incident;

(vi) the highest level of classified material that can be processed on the system and handling procedures for classified information;

(vii) start of day/shift/operations;

(viii) securing the system or workstation when temporarily absent;

(ix) securing the system or workstation at the end of the day/shift/operations;

(x) controlling and sanitising media;

(xi) adding, removing, decommissioning and undertaking destruction of equipment and media;

(xii) physical data transfer between network enclaves or environments;

(xiii) labelling, handling and disposing of hardcopy;

(xiv) preventing overview of data by visitors;

(xv) what to do for hardware and Software Maintenance; and

(xvi) other operational and security tasks and activities as allocated by the system managers/authorities.

DATA ITEM DESCRIPTION

1. DID NAME: DID-ENG-SOL-SSP-V5.3

2. TITLE: SYSTEM SECURITY PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The System Security Plan (SSP) describes a Security System-of-Interest (SSoI) (eg, Mission System) and/or its Targets of Security Assessment (ToSAs) from the perspectives of Information and Communications (ICT) security and cyber security. This includes the implementation and operation of security controls, practices and procedures required to secure the SSoI at an acceptable level of risk in accordance with the Governing Security Documents. The SSP is derived by selecting all relevant security controls from the Australian Government Information System Manual (ISM) and the Defence Security Policy Framework (DSPF), with additional security controls based on the security risks identified in the Approved Security Risk Management Plan(s) (SRMP(s)). A SSP is raised for one or more ToSA(s) within a SSoI.

Note: This DID has been written on the basis that all ToSAs for a SSoI will be addressed within a single SSP (including when the ToSA and the SSoI are one and the same). Where this is not the case, such as may occur for larger Mission Systems (eg, aircraft or ship), the requirements of the DID should be interpreted in the context of the set of SSPs and associated ToSAs. The ToSAs are either identified in the Approved governing plan for system security or in the System Overview section of this data item.

3.2 The SSP serves two purposes:

a. during the design and implementation phases for a SSoI, it provides a supporting artefact for the design process, describing the security architecture and identifying the ICT/cyber-security controls, practices and procedures that are planned to be implemented and identifies any associated operational and support implications; and

b. during the Security Authorisation assessment phases for a SSoI, it provides a consolidated reference or summary of the ICT/cyber-security controls, practices and procedures that have been implemented, and is one of the required artefacts for obtaining the required Security Authorisations for ICT security and cyber security.

3.3 The Contractor uses the SSP:

a. to describe a SSoI from a ICT/cyber-security perspective to ensure that the scope of ICT/cyber-security activities is clear to all parties and to assist with the identification of security-related risks and vulnerabilities;

b. to document the relevant security controls that will be, or have been, implemented (in full or in part) to address the ICT/cyber-security risks for each SSoI;

c. to describe the implementation and operation of the identified security controls to enable the required ICT and cyber Security Authorisations to be achieved for the SSoI;

d. to describe the plan to Verify that the implemented controls for a SSoI have been properly implemented and are effective; and

e. as one of the ICT/cyber-security artefacts to provide assurance to the Commonwealth that the Contractor’s ICT/cyber-security activities will enable the ICT/cyber-security requirements for the SSoI to be achieved.

3.4 The Commonwealth uses the SSP:

a. to gain assurance that the Contractor has a sound ICT/cyber-security program in place that complies with applicable Government and Defence security requirements and policies;

b. to understand and evaluate the Contractor's approach to meeting the ICT/cyber-security requirements of the Contract as part of the system security program in the SOW;

c. to identify and understand the Commonwealth's involvement in the Contractor's ICT/cyber-security program, including the monitoring of the Contractor's program;

d. as an input to its own planning for the project, including in relation to attaining the required ICT and cyber Security Authorisations for a SSoI; and

e. as one of the suite of ICT/cyber-security artefacts provided to the relevant Defence authorities as part of obtaining the required ICT and cyber Security Authorisations for a SSoI.

4. INTER-RELATIONSHIPS

4.1 The SSP is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Contractor Engineering Management Plan (CEMP);

c. Materiel System Security Management Plan (MSSMP);

d. In-Service Security Management Plan (ISSMP);

e. System Safety Program Plan (SSPP); and

f. In-service Materiel Safety Plan (IMSP).

4.2 The SSP inter-relates with the following data items, where these data items are required under the Contract:

a. System Specification (SS) for the SSoI including, if applicable, the associated Cyber Security Assurance Basis (as a component of this specification);

b. System Architecture Description (SAD);

c. Software List (SWLIST);

d. the security-related data items required under the Contract (other than those identified under clause 4.1);

e. the safety-related data items (eg, Hazard Log, Safety Case Report (SCR) and Materiel Safety Assessment (MSA)); and

f. Verification and Validation (V&V) data items, such as the V&V Plan (V&VP), Verification Cross Reference Matrix (VCRM), Acceptance Test Plans (ATPs), and Acceptance Test Reports (ATRs).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Note to drafters: Amend the following list of Applicable Documents to suit the requirements of the Contract. Do not include documents that are included within the 'Governing Security Documents'. In relation to ACSC documents, ensure that the latest versions are referenced.

Governing Security Documents	(see the Glossary for the definition of this term)

NIST SP 800-82	Guide to Operational Technology Security, Revision 3, September 2023
ISA/IEC 62433 series	Security for Industrial Automation and Control Systems
Australian Government Australian Cyber Security Centre (ACSC) Guidance Documents	Strategies to Mitigate Cyber Security Incidents, February 2017 Strategies to Mitigate Cyber Security Incidents – Mitigation Details, February 2017 System Security Plan (SSP) Annex Template

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 Subject to clause 6.1.2, the data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 Where a SSP is required for an ICT Security Authorisation, the format and content requirements for the SSP shall comply with any template for a System Security Plan issued by Defence in addition to the content requirements set out in clauses 6.1.4-6.1.7 and clauses 6.2 and 6.3 of this DID.

6.1.3 When the system security program clause in the SOW does not include requirements for an ICT Security Authorisation, the SSP should only address those requirements of this DID that relate to assessing cyber security.

6.1.4 The SSP shall be consistent with and, where applicable, comply with the Applicable Documents identified at clause 5. The SSP shall also accord with the risk management framework documented in the Approved governing plan (eg, SEMP, MSSMP or ISSMP, as applicable.

6.1.5 Where the Approved governing plan identifies that more than one SSP will be developed to address the ToSAs within an SSoI, each SSP shall identify the full scope of ToSAs and the associated SSPs for the SSoI, including the relationships between them (if any).

6.1.6 Subject to clause 6.2.4.1, when the Contract has specified delivery of another data item that contains aspects of the required information, the SSP should summarise these aspects and refer to the other data item.

6.1.7 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content – Part 1

6.2.1 Scope

6.2.1.1 The SSP shall define the scope of the SSP, identifying the SSoI and the associated ToSA(s) being addressed through the plan.

6.2.1.2 The SSP shall identify any assumptions and constraints associated with the information provided in the SSP, including (where applicable) how and when:

a. the identified assumptions will be validated; and

b. the identified constraints will be ameliorated.

6.2.2 System and Organisational Stakeholders

6.2.2.1 The SSP shall identify the key stakeholders applicable to the SSoI, including the System Owner, project sponsor, acquirer, user, developer, support agencies, and the relevant authorities for each different type of required Security Authorisation.

6.2.3 General System Overview

6.2.3.1 The SSP shall provide a general description of the SSoI, including its overall mission and capabilities, both functional and non-functional, from a security perspective. This general description shall also identify the external systems to which the SSoI interfaces, including providing a brief description of the purpose of the interactions between the SSoI and each external system.

6.2.3.2 The SSP shall identify and describe the component subsystems of the SSoI, including:

a. internal network interface diagram(s);

b. system block diagram(s);

c. internal system interface block diagram(s); and

d. system / software architecture diagram(s).

6.2.3.3 The SSP shall identify the ToSAs associated with the SSoI, including in relation to component subsystems of the SSoI and the external systems.

6.2.3.4 The SSP shall list:

a. all system-wide operating systems and software in use for the SSoI; and

b. the proposed system-wide security features (eg, cross-domain solutions, firewalls, and procedural controls).

6.2.4 Security Architecture

6.2.4.1 When the Contract has specified the delivery of a System Architecture Description (SAD), the Security Architecture description required by this clause 6.2.4:

a. shall be consistent with the architectural views defined in the system architecture model underpinning the SAD; and

b. should be derived as specific views from the SAD, and these views shall be incorporated explicitly into the SSP and not provided by cross-referencing to the SAD.

6.2.4.2 The SSP shall provide a high-level security architecture description of the SSoI, including identifying the interfaces to the external systems. The SSP shall include the following information:

a. System Operating Environment: Provide a brief (one to three paragraphs) general description of the environment that the SSoI operates within, including the context of that environment on a location basis (eg, when a SSoI element is part of a larger system, such as a platform). Include any environmental or technical factors that raise special security concerns.

b. System Interconnection and Information Sharing: For each interface to an external system, describe the technical implementation of the data flows between the SSoI and the external system, including where data is stored and transiting to, protocols, and what protection the data is given. For each interconnection between external systems that are owned or operated by different organisations, provide information concerning:

(i) the authorisation for the connection to other systems or the sharing of information between those systems; and

(ii) the assessed integrity, from a security perspective, of the data and information resident on the external system that will be used by, or shared with, the SSoI.

Note: System interconnection is the direct connection of two or more Digitally Enabled Systems and Equipment (DESE) for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system owners, information owners, and management obtain as much information as possible regarding vulnerabilities associated with system interconnections and

information sharing. This is essential to selecting the appropriate controls required to mitigate those vulnerabilities.

c. System Connectivity to Development or Test Environments: Describe any connectivity to development or test environments and how separation is maintained.

d. Accreditation Status of External Systems: Provide a table that details the ICT and cyber Security Authorisations of existing external systems, where interconnections are proposed.

e. Internal Data Flow Description and Protocols: Provide a description of the data flows internal to the SSoI, including their protocols. Include relevant diagrams.

f. Physical Environment Security: Include details of the physical security aspects relevant to the management and control of ICT/cyber-security risks (eg, with respect to installation or operational deployment), as well as any (known) physical security area ratings, physical security inspections, and physical security Certifications.

g. Data Security Classification and Categorisation: Detail the classification of the SSoI and the information held/processed by the SSoI, cross-referring to the Security Classification and Categorisation Guide (SCCG), as appropriate. Include details of the mechanisms to report any unauthorised connections or programmable devices (ie, sensors, converters etc.) trying to connect to the SSoI.

h. User Matrix: Detail the types of roles/users, their access levels, responsibilities, clearances required and who authorises their access to the SSoI.

i. Security Authorisation Boundaries: Define the boundaries of the SSoI (and subsystems if separate assessment is required at their level) with respect to the boundaries underpinning the Security Authorisations for, as applicable:

(i) physical security;

(ii) EMSEC;

(iii) ICT security; and

(iv) cyber security.

Note: A system may be made up of a series of subsystems and in some instances all subsystems are included within the assessment boundary but in other instances some of those subsystems may be excluded or assessed separately.

6.3 Specific Content – Part 2

6.3.1 Statement of Applicability / SSP Annex

Note: The SSP Annex Template issued by ACSC will assist with satisfying the ISM-related elements of this clause 6.3.1.

6.3.1.1 The SSP shall include, as an annex to the SSP, a statement of applicability for each ToSA covered by the plan, which identifies:

a. the version of the ISM, DSPF and any complementary publications (eg, NIST SP 800-82 or ISA-62443 series) agreed by the Commonwealth, which have been used to determine the security controls to implement;

b. the security controls from the ISM and DSPF that are, and are not, applicable to security for the ToSA(s), including supporting justification and references to supporting evidence (where applicable);

c. the security controls from the ISM, DSPF or complementary publication(s) that are applicable but are not being implemented or are only being partially implemented (including the rationale behind these decisions);

d. any additional controls that need to be implemented as an outcome of the risk assessment for the ToSA(s) captured in the associated SRMP;

e. any exemptions that have been granted, including (if known) the details of when and by whom;

f. any approvals to operate that have been granted, including (if known) the details of when and by whom; and

g. through the inclusion of cross-references to the relevant risks in the associated SRMP, which risks have been mitigated by each control.

6.3.2 System Security Plan – Design and Implementation Phases

6.3.2.1 During the design and implementation phases for the SSoI, the SSP shall describe the security controls that are being implemented to enable the required ICT and cyber Security Authorisations to be achieved for the SSoI, including identifying the implications for system design, system operation and system support, including in relation to:

a. human system integration,

b. standard operating procedures,

c. incident management and disaster recovery, and

d. Cyber Supply Chain management.

6.3.2.2 The SSP shall identify the ISSMP, Security Standard Operating Procedures (SSOPs), and other manuals and procedures that are required to implement the identified security controls.

6.3.2.3 The SSP shall:

a. identify the eight mitigation strategies from the ACSC Essential Eight Maturity Model and associated ACSC guidance documentation;

b. identify the assessed maturity level for the SSoI against each of these strategies, including describing the implementation status of each control; and

c. provide the associated justification for this assessment.

6.3.2.4 The SSP shall describe the plan to Verify that the controls for each ToSA have been properly implemented and are effective, including references to:

a. industry, regulatory and legislative compliance requirements; and

b. the applicable V&VP, VCRM and associated data items (eg, ATPs).

6.3.3 System Security Plan – ICT and Cyber Security Authorisation Phases

6.3.3.1 During the ICT and cyber Security Authorisation assessment phases for a SSoI, the SSP shall provide a consolidated reference or summary of the ICT/cyber-security controls, practices and procedures that have been implemented.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SW-SWLIST-V5.3

2. TITLE: SOFTWARE LIST

3. DESCRIPTION AND INTENDED USE

3.1 The Software List (SWLIST) identifies and describes each Software product that forms part of the Supplies or would otherwise be developed or acquired under the Contract and includes additional attribute information for each Software product.

3.2 The Contractor uses the SWLIST to:

a. list the Software products to be developed or acquired under the Contract and those to be supplied to the Commonwealth; and

b. document key Software characteristics of interest to the Commonwealth.

3.3 The Commonwealth uses the SWLIST to:

a. achieve early visibility into the criticality, quantity and nature of the Software to be supplied and subsequently supported; and

b. understand the scope of Software to be delivered to the Commonwealth and Associated Parties, and the rights associated with that Software.

4. INTER-RELATIONSHIPS

4.1 The SWLIST is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP); and

b. Software Management Plan (SWMP).

4.2 The SWLIST inter-relates with the following data items, where these data items are required under the Contract:

a. System Architecture Description (SAD);

b. Mission System Technical Documentation Tree (MSTDT);

c. Contract Work Breakdown Structure (CWBS); and

d. Software Support Plan (SWSP).

4.3 The SWLIST inter-relates with the Technical Data and Software Rights (TDSR) Schedule.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The SWLIST shall be provided in soft copy as a structured data file (eg, one or more databases, spreadsheets or other structured data format) that enables the SWLIST content to be accessed, queried, read, printed and used to generate soft copy tabulated text reports.

6.1.3 Except where the soft copy data file is compatible with a standard Software application defined elsewhere in the Contract, or otherwise agreed in advance and in writing by the Commonwealth Representative, the SWLIST shall be accompanied by any Software and Technical Data required to enable the functions identified in clause 6.1.2.

6.1.4 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Identity

6.2.1.1 The SWLIST shall identify each Software product or logical aggregation of Software products using a unique identifier.

6.2.1.2 Where the SWLIST is being used to report the content of a software build or increment, the build or increment shall be uniquely identified.

6.2.2 Location in the System Hierarchy

6.2.2.1 The SWLIST shall identify the location of each Software product in the Materiel System hierarchy (eg, processing element, equipment, subsystem and system) using an indentured numbering system that provides traceability from the Software product to the top-level system. The indentured numbering system shall reflect the CWBS element numbers, unless specified otherwise in the Approved SWMP.

6.2.3 Description

6.2.3.1 The SWLIST shall provide a brief description of the function or purpose of each Software product in terms of its contribution to functionality of the Mission System and / or Support System, cross-referring to the SAD where applicable.

6.2.4 Software Criticality

6.2.4.1 The SWLIST shall identify the criticality of each Software product in accordance with the following table:

Criticality	Effect on Materiel System		Effect on Contract	
	Performance	Support	Cost	Schedule
0	Software product is 'safety critical'. Failure may result in loss of life, injury, or significant damage to property or the environment.		Not applicable.	
1	Product is 'mission critical'. Product failure results in mission failure due to:		Delays in schedule result in:	
	Major degradation of operational capability.	Unresponsive support or unsupportable Software hinders system operation.	Significant cost overrun, budget overrun likely or has occurred.	Scheduled date for first System Acceptance is unachievable.
2	Product failure results in degraded performance to a point where mission success is questionable due to:		Delays in schedule result in:	
	Significant reduction of operational capability.	Software support, or work-around, delays or reduces system operation.	Cost overrun with possible budget overrun.	Possible slippage in scheduled date for System Acceptance.
3	Product failure results in degradation of secondary mission due to:		Delays in schedule result in:	
	Minor reduction of operational capability.	Software support, or work-around, delays or reduces secondary capability.	Cost overrun but sufficient remaining budget.	Compressed schedule, but scheduled Acceptance date is realistic and achievable.
4	Product failure results in inconvenience with:		Delays in schedule result in:	
	No reduction in operational capability.	No noticeable delays caused by Software support.	Minor cost increase with negligible impact to budget.	Negligible impact to the achievement of Acceptance.

6.2.5 Software Categories

6.2.5.1 Each Software product shall be categorised by a single category from the following table. Mission System and Support System Software may include both Bespoke Software (as defined in the table) and Commercial Software. Where a Software product is integrated from lower level Software products, which are of a different category, these lower level products need to be separately identified and reported in the SWLIST.

Software Category	Description	Comments
Bespoke Software	Software that is subject to software development or integration activities.	Source Code may be available to the Commonwealth and allow the Commonwealth to modify and maintain the software independently of the original supplier. May integrate one or more subcomponents that are Commercial Items or Free and Open Source Software.
Commercial Software that is not Free and Open Source Software (CNF)	Commercial Software as defined in the Glossary, exclusive of Free and Open Source Software.	Development is not required to meet the requirements of the system being acquired. Unless agreed in relation to a Key Commercial Item, the Commonwealth is unlikely to be able to acquire Source Code and/or the legal rights to modify or re-engineer the software.
Commercial Software that is Free and Open Source Software (FOSS)	Free and Open Source Software, as defined in the Glossary.	Generally available to the public in Source Code and may also include compiled form. Subject to a variety of open source licences. Ongoing support may be provided from an open source community.

6.2.6 Other Software Attributes

6.2.6.1 The SWLIST shall identify whether each of the attributes, in the following table, applies to each Software product (ie, yes or no for each).

Software Attribute	Description	Comments
Software as Firmware (SAF)	Firmware is a combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device. The software cannot be readily modified under program control.	SAF has not always been recognised as software but treated as hardware or as a component of a hardware item (eg, software-controlled electronics such as radios and GPS). SAF may not always be identified as a supportable item independent of the hardware item that contains it.
Non Deliverable Software (NDS)	Software that is not required to be delivered to the Commonwealth or any other person under the Contract because the Commonwealth does not need it for operation or support of the system (eg, unit test harnesses not required for support). NDS is generally used in the development and testing of other software or system elements.	NDS may be Bespoke Software or Commercial Software (either CNF or FOSS). NDS may be used to test or exercise other software or hardware as part of that product's development. Consideration should be given to Commonwealth needs for access to identified NDS over the life cycle.

6.2.7 Level

6.2.7.1 The SWLIST shall identify the level of the Software product (ie, item, component or unit) in the system hierarchy. Software items may be designated as 'configuration items' while the Software architectural design process transforms items into 'components' and the Software detailed design process refines components into 'units'.

6.2.8 Language

6.2.8.1 The SWLIST shall identify the programming language used / to be used to develop each Software product.

6.2.9 Software Size Information

6.2.9.1 General

6.2.9.1.1 Software size details in the SWLIST shall be provided in Source Lines of Code (SLOC) (or thousand SLOC (KSLOC)), or an equivalent development-related unit of measure (eg, function points) with the Contractor's recommended methodology for converting to SLOC.

6.2.9.1.2 The SWLIST shall clearly identify whether the Software sizing information provided is an actual value (denoted '(A)') or estimated value (denoted '(E)') (eg, '542,341 SLOC (A)').

6.2.9.1.3 Where Software sizing information is an estimated value, the SWLIST shall include the most recent date at which the estimate was considered valid.

6.2.9.1.4 Except for the Estimated Total Size, other size estimates may be expressed either as an absolute value, using the same units as for the Estimated Total Size, or as a relative value (ie, a percentage).

6.2.9.2 Estimated Total Size

6.2.9.2.1 For each item of Bespoke Software the SWLIST shall identify the estimated or actual total size of all code in accordance with the requirements of clause 6.2.9.1.

6.2.9.3 Reused Unmodified Code Required

6.2.9.3.1 For each item of Bespoke Software, the SWLIST shall identify the estimated or actual size of the code to be reused without modification in accordance with the requirements of clause 6.2.9.1.

6.2.9.4 Estimated Modified Code Required

6.2.9.4.1 For each item of Bespoke Software, the SWLIST shall identify the estimated or actual size of the code to be modified (ie, reused with modification) in accordance with the requirements of clause 6.2.9.1.

6.2.9.5 Estimated New Code Required

6.2.9.5.1 For each item of Bespoke Software, the SWLIST shall identify the estimated or actual size of new code to be developed in accordance with the requirements of clause 6.2.9.1.

6.2.10 Development Standard

6.2.10.1 The SWLIST shall identify the software development standard applied to each extant Software product or that will be applied to Software products during development or modification.

6.2.11 Assurance Standard

6.2.11.1 The SWLIST shall identify the software assurance standard applied to each extant Software product or that will be applied to Software products during development or modification.

6.2.12 Software Assurance Level

6.2.12.1 The SWLIST shall identify the Software assurance level applied to each extant Software product or that will to be applied to Software products during development or modification.

6.2.12.2 The SWLIST shall define the Software assurance levels where these differ from the assurance levels specified for an assurance standard that was identified in response to clause 6.2.11.

6.2.13 Source Code Availability

6.2.13.1 For each item of Bespoke Software, the SWLIST shall indicate the availability of Source Code.

6.2.14 Development Agency

6.2.14.1 The SWLIST shall identify the development agency for each Software product.

6.2.15 Support Agency

6.2.15.1 The SWLIST shall identify the support agency for each Software product.

6.2.16 Target Platform

6.2.16.1 The SWLIST shall identify the target (computing) platform for each Software product.

6.2.17 Target Environment

6.2.17.1 The SWLIST shall identify the target environment (eg, operating system) for each Software product.

6.2.18 Software Support Environment

6.2.18.1 The SWLIST shall describe the support environment needed for each Bespoke Software product, including any development and/or test environment(s) (eg, compilers, editors, debuggers, computer aided software engineering tools, and special test equipment (eg, simulators and stimulators)).

6.2.19 Delivery Information

6.2.19.1 The SWLIST shall include delivery information, including for each delivery:

a. if the Software product is delivered separately or as part of a higher level system / hardware component;

b. if the Software product is delivered separately (which may include maintenance / version updates), the method of delivery (eg, online, media);

c. the delivery location, recipient, delivery date and milestone to which it relates; and

d. installation, configuration, adaptation and compatibility information, as applicable.

6.2.20 Software Rights

6.2.20.1 If restrictions (including Intellectual Property rights, Export Approvals or other limitations) apply to Bespoke Software or Commercial Software related to a Key Commercial Item, the SWLIST shall include cross-reference to such provisions as described in the TDSR Schedule for licensing or delivery restrictions, or directly to the applicable agreement (eg, an applicable Technical Assistance Agreement).

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SW-SWMP-V5.3

2. TITLE: SOFTWARE MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Software Management Plan (SWMP) documents the Contractor's plans for the management and development of Software. The SWMP describes the application of the relevant processes described in AS/NZS ISO/IEC/IEEE 12207:2019, *Systems and Software Engineering - Software life cycle processes*, as the Contractor intends to apply them to the activities of the Contract.

3.2 The Contractor uses the SWMP to:

a. document the approach, plans, and procedures for managing Software-related activities under the Contract; and

b. monitor the progress of Software-related activities.

3.3 For Contractors acquiring and/or supplying Software under the Contract, the SWMP is expected to describe the approach, plans and procedures to be applied to the management of the Software being acquired and/or supplied. This would typically include the monitoring and review of Subcontractors developing Software, the Configuration Management of acquired Software, and the integration and Verification of this Software with other elements being supplied under the Contract.

3.4 For Contractors developing Software, this plan is expected to include the approach, plans and procedures for Software development, in addition to those applied to the acquisition and/or supply.

3.5 The Commonwealth uses the SWMP to gain insight into the approach, plans and procedures to be employed by the Contractor in the execution of Software-related activities.

4. INTER-RELATIONSHIPS

4.1 The SWMP is subordinate to the Systems Engineering Management Plan (SEMP).

4.2 The SWMP inter-relates with the following data items, where these data items are required under the Contract:

a. Software List (SWLIST);

b. Contract Master Schedule (CMS); and

c. Software Support Plan (SWSP).

4.3 The SWMP inter-relates with the Technical Data and Software Rights (TDSR) Schedule.

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

DI-IPSC-81427B	Software Development Plan Data Item Description
AS/NZS ISO/IEC/IEE 12207:2019	Systems and Software Engineering - Software life cycle processes

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the data item shall summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The SWMP shall comply with the content requirements of DI-IPSC-81427B, with the exceptions contained in Table 1 below.

6.2.1.2 The SWMP shall, when addressing the content requirements of DI-IPSC-81427B, define Software life cycle processes and Software specific processes that are consistent with AS/NZS ISO/IEC/IEEE 12207:2019, and tailored to the scope of the Contract.

Table 1 – Tailoring to be applied to DI-IPSC-81427B

Affected Paragraph	Tailoring to be Applied
All	Replace all occurrences of 'Software development plan' with 'Software Management Plan'.
All	Replace all occurrences of 'SDP' with 'SWMP'.
All	Delete all occurrences of 'It shall cover all contractual clauses concerning this topic.'
3.6a Software development process	Replace with: This paragraph shall describe the selected Software development life cycle(s) for each component or group of related components together with the rationale for their use within the context of the Contract. The description should justify and link the selected life cycle models to Contract risks, major milestones, work products, deliverables and development phases to demonstrate its appropriateness.
3.7c1 Incorporating reusable Software products	Add: Implications for supporting the Software shall be specifically addressed for each item affected and include an assessment of vendor viability, level of support available, alternate sources of support, ownership of Intellectual Property licensing arrangements (including costs and, by reference to the TDSR Schedule, restrictions), dependencies such as operating system and/or hardware compatibility and constraints.
3.7d1 Safety Assurance	Add: It shall describe the integration of Software safety as part of the system safety program. It shall include the tailoring and use of selected Software assurance standards and guidelines and associated data deliverables.
3.7e (shown as a 2nd d1 in the DI-IPSC-81427B) Assurance of other critical requirements	Add: It shall describe any mission critical Software and the steps either taken or planned to ensure failure of this Software will not compromise the system's mission.
3.7f Computer hardware resource utilisation	Add: It shall describe the interpretation of any resource utilisation requirements and how the satisfaction of these requirements are to be verified.
3.7h Access for acquirer review	Replace with: This paragraph shall describe the approach to be followed for providing the Commonwealth Representative with access to Contractor and Subcontractor facilities for review of work products, activities and data including engineering and measurement data. Access should include at least physical access to facilities and preferably include electronic access to data (eg measurement data) and work products (eg, design information).

Affected Paragraph	Tailoring to be Applied
3.8b1 Software engineering environment	Add: It shall include details of the Software engineering environment including computing resources (number, type, configuration, etc.), and the associated performance requirements of the environment (eg, required compile and link times). This paragraph shall address the certification implications of the environment.
3.8b2 Software test environment	Add: It shall include details of the Software test environment including computing resources (number, type, configuration), special test equipment and the associated performance requirements of the environment (eg, simulator fidelity, instrumentation, recording, etc.). This paragraph shall address the certification implications of the environment.
3.8b5 Non-deliverable Software	Add: It shall identify any non-deliverable Software and describe how this Software will be treated differently from deliverable Software. It shall address specifically the application and tailoring of the standards identified for Software development to non-deliverable Software. This paragraph shall address the certification implications and use of non-deliverable Software.
3.8d1 System-wide design decisions	Replace with: This paragraph shall include details of how system design decisions affecting or affected by Software are to be made and recorded. It should address how such decisions and the rationale for making them will be preserved and applied during through life support of the system.
3.8e Software requirements analysis	Add: It shall describe how Software requirements will be identified and allocated to Software components, how Software requirements will be reviewed to ensure a common understanding with relevant stakeholders and how Software requirements will be managed and controlled.
3.8f1 CSCI-wide design decisions	Add: It shall detail the criteria used to define and select CSCIs, including the rationale for each of the selection criteria. It shall include design decisions regarding the partitioning of the Software and the consideration given to enhancement and modification during through life support of the Software.
3.8o7 Transition to the designated support site	Add: This paragraph shall detail the management strategy and plans for the transition of the Software development capability to the support agency and address any special considerations (eg, preservation of safety certification). It shall identify all items that have any limited or restricted warranty, data rights or licensing agreements, including any other limitation on the delivery or support of the item (by reference to the TDSR Schedule, where applicable). It shall describe all provisions, which ensure the Commonwealth's rights concerning the delivered Software and associated data, and describe the plans for transferring any required licenses, warranties and data rights to the Commonwealth or its nominated representatives. It shall identify and describe those items of the development Software engineering environment that will be transitioned into the Software support environment including those items used for integration and test of the Software and any special test equipment. Where a Transition Plan, covering transition planning for Software as indicated above, is separately available to the Commonwealth Representative, this section may reference that source.
3.8.u1 Risk management	Add: This paragraph shall detail the techniques used for identifying Software related risks and mitigation strategies. Where this information is available to the Commonwealth Representative in the Risk Register or equivalent then this section should provide a reference to the information.

Affected Paragraph	Tailoring to be Applied
3.8u2 Software management indicators	Add: This paragraph shall detail the use of measurement as a management tool. It should identify how the Contractor intends using measurement to manage the development and acquisition of Software for the Contract. Where this information is available to the Commonwealth Representative elsewhere this section should reference the relevant information and provide a summary of the measures used for Software management.
3.8u.4 Subcontractor management	Add: This paragraph shall detail the Contractor's plans for managing the Software engineering activities performed by Subcontractors. It shall identify and describe the scope of the Software activities to be undertaken by the Contractor and each of its Subcontractors performing Software engineering activities. It shall describe the Contractor's plans for review and approval of Subcontractor plan and processes. It shall describe the Contractor's plans for monitoring the progress of Subcontractor activities and how significant deviations from Subcontractor plans will be identified and addressed.
3.8u6 Coordination with associate developers	Add: This paragraph shall describe the plans for coordination of Software engineering efforts with associated developers. Such coordination may include interface definition and control, the use of integrated product teams, as well as the support to be provided during integration and verification activities.
3.8u7 Improvement of project processes	Add: This paragraph shall provide details of the Contractor's and associated organisations Software engineering process improvement activities specific to this Contract. Where this information is available to the Commonwealth Representative in a Process Improvement Plan or equivalent then this section should provide a reference to the information.
3.7u9 Software rights management	Add new requirement 3.7u9 Software rights management: This paragraph shall document the approach, plans and procedures for managing Software rights (including Intellectual Property rights) for the Software acquired, supplied or developed under the Contract. This paragraph shall cross-reference the Technical Data and Software Rights Schedule for details of rights and limitations.
3.8v Schedules and activity network	Add: This paragraph shall present and describe a stand-alone summary of the Software schedule and include a clear mapping of the life cycle development phases and major milestones. This paragraph shall include the rationale for the durations given in the schedule and include the basis of estimate, estimating assumptions, and the selection of coordination points and linkages to the Contract Master Schedule.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-TRACE-RTM-V5.3

2. TITLE: REQUIREMENTS TRACEABILITY MATRIX

3. DESCRIPTION AND INTENDED USE

3.1 The Requirements Traceability Matrix (RTM) describes the Contractor's traceability along design rationale for modifications between specifications and related documents that define the system.

3.2 The Contractor uses the RTM to provide bi-directional traceability between requirements specifications at different levels within the system hierarchy.

3.3 The Commonwealth uses the RTM to evaluate the completeness of the Contractor's design solution and to assess the impact of any changes.

4. INTER-RELATIONSHIPS

4.1 The RTM is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP); and

b. Integrated Support Plan (ISP).

4.2 The RTM inter-relates with the following data items, where these data items are required under the Contract:

a. System Specification (SS) for each Mission System;

b. Support System Specification (SSSPEC); and

c. Verification Cross Reference Matrix (VCRM).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 This DID may be satisfied by an electronic database in a format agreed with the Commonwealth Representative.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The RTM shall show the traceability of requirements from the Contract and other source documents to the System Specification and lower levels of the specification hierarchy.

6.2.1.2 The RTM shall be a Contract-wide repository and include requirements from both Contractor and Subcontractors.

Note: The RTM may be related to the VCRM (ie, either the RTM uses the same database as the VCRM or they are produced from a common data source).

6.2.1.3 The RTM shall clearly explain the format and terminology used for the data of the RTM.

6.2.1.4 The RTM shall identify for each requirement:

a. a unique and unmodifiable identifier for the requirement;

b. the architectural element (CI or interface) to which the requirement belongs;

c. the document and paragraph number of the requirement;

d. the derivation, or reference to the design record that records the derivation, for the requirement from its parent where the requirement has a parent within the database; and

e. other attributes as identified by the design process.

6.2.1.5 The RTM shall identify parent-child and child-parent links that provide the rationale and unambiguous traceability for all requirements.

6.2.1.6 The RTM shall show the parent-child and child-parent traceability through multiple levels of the design hierarchy to assess the impact of potential specification changes.

6.2.1.7 Where the RTM is provided in electronic format it shall be accompanied with user documentation showing the operation, the data relationships and interpretation of all data fields.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-DES-DISP-V5.3

2. TITLE: DISPOSAL PLAN (DISP)

3. DESCRIPTION AND INTENDED USE

3.1 The Disposal Plan (DISP) provides details of the Contractor's analysis of, and proposed recommendations for, the disposal of items delivered under the Contract.

3.2 The DISP enables the Commonwealth to ensure that adequate disposal provisions are established and that the potential safety and environmental impacts are understood prior to any disposal action being undertaken.

4. INTER-RELATIONSHIPS

4.1 The DISP is subordinate to the Integrated Support Plan (ISP), where this plan is required under the Contract.

4.2 The DISP inter-relates with the following data items, where these data items are required under the Contract:

a. Supply Support Development Plan (SSDP);

b. Support System Technical Data List (SSTDL); and

c. Life Cycle Cost Management Plan (LCCMP).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the DISP should summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General Requirements

6.2.1.1 The DISP shall define the disposal methods and procedures required for Mission System and Support System items delivered under the Contract.

6.2.2 Responsibilities

6.2.2.1 The DISP shall include recommendations for those agencies and personnel or positions responsible for the execution of the DISP, including the disposal of items in the Mission System and Support System.

6.2.3 Removal of Items from the Operational Inventory

6.2.3.1 The DISP shall describe the recommended disposal activities to be conducted, which also takes into account any special provisions (eg, de-militarisation requirements, security requirements, and managing Problematic Substances), for items of the Mission System and Support System that:

a. are retired from the inventory as part of planned maintenance, modification or upgrade schedules;

b. are non-repairable and are removed and replaced as part of Corrective Maintenance or Preventive Maintenance;

c. are retired and removed from the inventory at the end of their operational life; and

d. are removed from the inventory when there is no longer any need for the system.

6.2.4 Program Planning Details

6.2.4.1 The DISP shall provide details of:

a. the life of the components of the Mission System and Support System;

b. the schedule for the withdrawal of items with finite lives or with planned retirement times, and the means by which this shall be achieved;

c. the analysis and results of the potential and the planned schedule of items to undergo material recycling when entering the disposal phase;

d. the method of reclamation, re-cycling or disposal of each item;

e. the logistic support required to accomplish the disposal of items, including:

(i) Packaging, handling, storage and transportation;

(ii) security considerations during disposal;

(iii) Technical Data introduction, disposal or amendment;

(iv) financial analysis and accounting of resale potential and achieved values for disposal items;

(v) associated Support and Test Equipment (S&TE); and

(vi) associated Spares (ie, that also require disposal).

6.2.5 Problematic Substances

6.2.5.1 In order to eliminate or reduce identified Problematic Substance items during the design process, the DISP shall:

a. provide a summary of all Problematic Substances required to support a selected end item;

b. identify all items having associated Problematic Substances storage, hazardous waste storage, or disposal costs; and

c. include the quantities and costs, per task, of Problematic Substances required to satisfy the maintenance task requirements.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-FAC-FRAR-V5.3

2. TITLE: FACILITIES REQUIREMENTS ANALYSIS REPORT

3. DESCRIPTION AND INTENDED USE

3.1 The Facilities Requirements Analysis Report (FRAR) describes the detailed requirements for all of the Commonwealth Facilities, including recommended works requirements, to enable the Mission System and the Support System to be operated and supported over the Life-of-Type of the Mission System. The Commonwealth and the Contractor use the FRAR as the basis for a common understanding of the requirements for Commonwealth Facilities.

3.2 The Contractor uses the FRAR to document the outcomes of its Facilities requirements analyses for new Commonwealth Facilities to be constructed by either the Commonwealth or the Contractor, and/or existing Commonwealth Facilities to be modified by either the Commonwealth or the Contractor (or both).

3.3 The Commonwealth uses the FRAR to:

a. assist with the evaluation of the Contractor’s designs for both the Mission System and the Support System;

b. understand, evaluate and monitor the Contractor’s scope of work under the Contract with respect to Facilities;

c. identify and understand the Commonwealth’s scope of work with respect to Facilities; and

d. finalise the scope and scheduling of the respective development and implementation activities for new or to-be-modified Commonwealth Facilities for which either the Contractor, the Commonwealth or both parties have responsibility.

4. INTER-RELATIONSHIPS

4.1 The FRAR is subordinate to the following data items, where these data items are required under the Contract:

a. Integrated Support Plan (ISP); and

b. Site Installation Plan (SIP).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the FRAR should summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The FRAR shall provide sufficient detail to enable the Commonwealth to:

a. be assured that, where Commonwealth Facilities are mandated under the Contract, those Facilities will be suitable for the Contractor’s proposals for the new Mission System and Support System;

b. understand the full scope of the requirements for Commonwealth Facilities, for the new Mission System and Support System; and

c. translate the FRAR into construction bid packages that will build or modify Facilities to be compatible with the new Mission System and the Support System.

6.2.1.2 The FRAR shall include a full description of the required Facilities including recommendations, accompanied by drawings, specifications, and sketch plans, for new Commonwealth Facilities and for existing Commonwealth Facilities to be modified.

6.2.2 Requirements Analysis

6.2.2.1 The FRAR shall provide details of the analysis process used to develop the FRAR (highlighting any differences from the analysis described in the Approved ISP), including:

a. a description of the methodology employed;

b. identification of the data sources used;

c. identification of the key assumptions on which the analysis is based; and

d. sample calculations (if relevant).

6.2.2.2 The analysis shall include Facilities requirements specifically pertaining to existing or planned Commonwealth Facilities located at all operational and logistic support locations.

6.2.3 Facilities Details

6.2.3.1 For each of the Facilities requirements identified, the FRAR shall include specific assessments, and justification for those assessments, of the:

a. space / room requirements;

b. equipment and Personnel needed to operate and support the Mission System and Support System, as applicable, in the applicable Facility;

c. installation requirements for items of equipment that are part of the Mission System and Support System, as applicable (cross-referencing the SIP, if available);

d. intended use of the Defence Wide Area Network (WAN) or of leased data links, in terms of bandwidth and peak capacity requirements;

e. power requirements, including anticipated peak loads, reasonable allowances for growth, earthing, and equipment susceptibility to spikes in the power supply;

f. air conditioning requirements considering working conditions, ventilation and heat generation from plant;

g. equipment-specific cooling requirements (eg, water cooling), which are in addition to the air conditioning requirements and which are recommended to be provided as part of the Facilities;

h. lighting requirements;

i. floor loading requirements;

j. floor levelling requirements where there are, for example, process-specific requirements for particular tolerances in the floor levels;

k. Work Health and Safety issues and safety risk management provisions;

l. facilities for achieving a suitable work environment, as may be described by a code of practice approved under section 274 of the *Work Health and Safety Act 2011* (Cth), *Managing the Work Environment and Facilities*;

m. noise insulation requirements;

n. mechanical constraints, if any;

o. facility-specific fire detection / suppression systems;

p. access requirements for equipment (eg, vehicle loading docks) and personnel;

q. personnel access control and physical security requirements;

r. emanations security and cyber security requirements;

s. Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC);

t. storage requirements, including shelving / racking recommendations;

u. dust control / clean room requirements;

v. compressed air requirements;

w. water supply and extraction / sewerage requirements;

x. trade waste generation and extraction removal requirements; and

y. recommendations for energy and water efficiency.

6.2.3.2 For each of the Facilities identified in the Contract that will be modified for, or provided by, the Commonwealth, the FRAR shall include the Contractor's schedule recommendations with respect to the required works.

6.2.4 Contractor Facilities required for in-service support

6.2.4.1 If the SOW requires the Contractor to address Facilities for the Contractor and/or related parties, in order to provide in-service support, the FRAR shall:

a. identify and briefly describe the significant Facilities (ie, Facilities that must be built or specifically modified to enable in-service support);

b. summarise how these Facilities were analysed; and

c. identify the key points that make these Facilities significant (eg, in terms of size, cost or specialised plant or equipment that needed to be included in the Facility).

6.3 Annexes

6.3.1 Annexes shall be used, as required, to record requirements and document plans for individual Facilities.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-PER-PRRL-V5.3

2. TITLE: PERSONNEL RESOURCE REQUIREMENTS LIST

3. DESCRIPTION AND INTENDED USE

3.1 The Personnel Resource Requirements List (PRRL) documents the types and quantities of Personnel required to perform the functions associated with each of the Support System Constituent Capabilities.

3.2 The Contractor uses the PRRL to:

a. document the outcomes of its Personnel requirements analysis conducted in accordance with the Approved ISP; and

b. advise the Commonwealth of the recommended types and quantities of Personnel, including (where applicable) security clearance requirements.

3.3 The Commonwealth uses the PRRL to:

a. understand and evaluate the Contractor’s approach to meeting the requirements of the Contract and, if applicable, the Contract (Support);

b. assist with the evaluation of the Support System as it evolves under the Contract;

c. assist with monitoring the progress of the Contractor’s developmental activities under the Contract; and

d. enable the Commonwealth to undertake Independent Verification and Validation (IV&V) of the Contractor’s PRRL outcomes.

4. INTER-RELATIONSHIPS

4.1 The PRRL is subordinate to the Integrated Support Plan (ISP).

4.2 The PRRL inter-relates with the following data items, where these data items are required under the Contract:

a. Task Analysis Report (TAR);

b. Logistic Support Analysis Record (LSAR);

c. Level Of Repair Analysis Report (LORAR);

d. Performance Needs Analysis Report (PNAR); and

e. Life Cycle Cost Report and Model (LCCRM).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 This data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Personnel Resource Requirements

6.2.1.1 The PRRL shall identify, for each Support System Constituent Capability, the optimised results and recommendations for the types and quantities of Personnel required as:

a. Commonwealth Personnel, and

b. Contractor (Support) and Subcontractor (Support) Personnel.

6.2.1.2 The PRRL shall identify whether or not any identified type of Commonwealth Personnel (by skill) is available, or could not reasonably be made available through the application of suitable Training to be provided under the Contract

6.2.1.3 The PRRL shall identify the Personnel required to meet the Australian Industry Capability requirements if defined in any accompanying Contract (Support).

6.2.2 Validation Report

6.2.2.1 The PRRL shall include a Validation Report, as an annex, which shall describe the analysis processes undertaken to define the optimal types and quantities of Personnel required to perform all operating and support functions associated with the Mission System and the Support System.

6.2.2.2 The Validation Report shall include:

a. a description of the method and model(s) used, including any organisational model(s), and consideration of the following aspects of identified jobs and duties:

(i) nature of the job or duty (eg, uninterruptible, non-continuous, safety-critical, mission-critical, shift-based, etc);

(ii) frequency of performance;

(iii) level of supervision;

(iv) responsibilities;

(v) performance conditions;

(vi) performance standards;

(vii) security clearance requirements;

(viii) regulatory requirements; and

(ix) consequences of inadequate performance;

b. identification of the data sources including, where applicable, cross-references to the TAR and PNAR, as applicable;

c. identification of the key assumptions on which the analysis is based;

d. calculations and sensitivity analyses for a sample of Personnel (to include each of the categories defined in clause 6.2.2.1) to support the recommendations; and

e. justification for the recommended types and quantities of Personnel for operation and support of the Mission System and Support System.

6.3 Annex

6.3.1 Data justifying the Personnel listed in the PRRL, including the Validation Report, shall be provided as an annex to the PRRL.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-SW-SWSP-V5.3

2. TITLE: SOFTWARE SUPPORT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Software Support Plan (SWSP) describes the Support Resources, methods and procedures required to perform life-cycle support of Software, including Software applications and Software Updates, used for the purpose of providing continuing life-cycle support for Software.

3.2 The Contractor uses the SWSP to:

a. define the management organisation, methodology and tasks necessary to support the deliverable Software, including Software Updates; and

b. identify the Support Resources (eg, Software tools, skills, servicing and programming equipment) required to perform Software maintenance, including Preventive Maintenance and Corrective Maintenance, and the development of enhancements to the Software throughout its life.

3.3 The Commonwealth uses the SWSP to:

a. understand the level and complexity of the Software support required; and

b. assess the Contractor’s proposed program for the provision of Software support.

4. INTER-RELATIONSHIPS

4.1 The SWSP is subordinate to the following data items, where these data items are required under the Contract:

a. Integrated Support Plan (ISP);

b. Systems Engineering Management Plan (SEMP);

c. Software Management Plan (SWMP); and

d. Contractor Engineering Management Plan (CEMP).

4.2 The SWSP inter-relates with the following data items, where these data items are required under the Contract:

a. Software List (SWLIST);

b. Materiel System Security Management Plan (MSSMP);

c. In-Service Security Management Plan (ISSMP);

d. Support System Technical Data List (SSTDL) (applicable to acquisition contracts);

e. Technical Data List (TDL) (applicable to support contracts);

f. Task Analysis Report (TAR); and

g. Life Cycle Cost Report and Model (LCCRM).

4.3 The SWSP inter-relates with the Technical Data and Software Rights (TDSR) Schedule and the Security Classification and Categorisation Guide (SCCG) Attachments to the Contract.

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

MIL-HDBK-1467	Acquisition of Software Environments and Support Software

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The SWSP shall comply with the content requirements of MIL-HDBK-1467 Appendix B, as tailored by the exceptions and changes identified below.

6.2.1.2 If this DID is being used under an acquisition contract, the SWSP shall address Software support for all deliverable Software associated with the Mission System and the Support System.

6.2.1.3 If this DID is being used under a support contract, the SWSP shall address the management and planning of Software Support Services for Software designated as 'Products Being Supported'.

6.2.2 Tailoring to be applied to MIL-HDBK-1467

6.2.2.1 All references to *Life Cycle Software Engineering Environment User's Guide* shall be read as 'Software Support Plan'.

6.2.2.2 All references to 'guide' shall be read as 'plan'.

6.2.2.3 The SWSP shall include in the 'table or matrix', as required by MIL-HDBK-1467 Appendix B paragraph B.3.3.1.1 (Description of the application software to be supported by the LCSEE), a sufficient level of detail describing the application Software in order to cross-reference the target system's functions and the management requirements to be detailed within the SWSP.

6.2.2.4 The SWSP shall address the requirements of MIL-HDBK-1467 Appendix B paragraph B.3.3.1.5 (limited and restricted rights), for the deliverable Software / Software products to be / being supported, as applicable, and the Software used within the support environment, by including:

a. the applicable category of Software rights as defined through clause 5 of the COC (eg, Software product, GFE, or Commercial Software); and

b. cross-references to any restrictions applying to the rights to use and sublicense the Software, and related Technical Data (eg, Source Code), as detailed within the Contract or licences, as applicable.

6.2.2.5 The SWSP shall include, for the Software listed in accordance with the requirements of MIL-HDBK-1467 Appendix B paragraph B.3.5.4 (Software structure), cross-references to the SSTDL or TDL (eg, for Source Code, specifications, and Software design documentation), as applicable.

6.2.2.6 The SWSP shall address the requirements of MIL-HDBK-1467 Appendix B paragraph B.3.6.6.2 (security provisions and other restrictions), for both the application Software to be / being supported and Software used within the support environment, in accordance with the SCCG and any Export Approvals, as applicable.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-TDATA-CDATA-V5.3

2. TITLE: CODIFICATION DATA

3. DESCRIPTION AND INTENDED USE

3.1 As a sponsored nation in the NATO Codification System (NCS), Australia is required to adhere to the policies and principles as published in the NATO Manual of Codification (ACodP-1). Codification of a Stock Item (refer clause 3.4) involves assessing the essential characteristics of an item in order to discern its unique character and to differentiate it from any other item. NATO Standardisation Agreement (STANAG) 4177 details a standard process for the acquisition of data in support of Codification. This DID details the format, content and preparation instructions for the supply of Codification Data (CDATA), which will be used by the Commonwealth for Codification purposes.

3.2 The Contractor uses this data item to provide CDATA to the Commonwealth.

3.3 The Commonwealth uses this data item to enable it to undertake Codification in order to meet its statutory requirements for asset management and financial reporting obligations pursuant to the *Public Governance, Performance and Accountability Act 2014* (PGPA).

3.4 In this DID, the term Stock Item:

a. if this DID is being used under an acquisition contract, means an item of Supplies (that is not data or Software, unless specifically required to be codified, or services); and

b. if this DID is being used under a support contract, has the same meaning as provided in the Glossary.

4. INTER-RELATIONSHIPS

4.1 The CDATA is subordinate to the following data items, where these data items are required under the Contract:

a. Integrated Support Plan (ISP);

b. Support Services Management Plan (SSMP);

c. Supply Support Development Plan (SSDP);

d. Supply Support Plan (SSP);

e. Technical Data Plan (TDP) or Technical Data Management Plan (TDMP) (as applicable); and

f. Support System Technical Data List (SSTDL) or Technical Data List (TDL) (as applicable).

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

STANAG 4177	*Codification of Items of Supply – Uniform System of Data Acquisition*

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

Note: The reference to the SOW clause for 'Deliverable Data Items' in the following clause is applicable for those Contracts that do not include a Contract Data Requirements List (CDRL).

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the SOW clause for 'Deliverable Data Items' and the CDRL clause entitled 'General Requirements for Data Items'.

6.2 Specific Content

6.2.1 Data for Each Item Not Codified in the NATO Codification System

6.2.1.1 For each proposed Stock Item, which is not codified in the NATO Codification System, the CDATA shall detail the following information:

a. name and full address of the true manufacturer of the item – a manufacturer is deemed to be that organisation that controls the design specification of the item;

b. the NATO Commercial and Government Entity Code (NCAGE Code[1]) of the true manufacturer (where this is known);

c. the reference / part Number assigned to the item by the true manufacturer to uniquely identify the item;

d. name and full address of the supplier of the item;

e. the NCAGE Code of the supplier (where this is known);

f. the supplier's reference / part number for the item;

g. the name of the item as it appears in the manufacturer's or supplier's documentation;

h. a proposed NATO group class (if appropriate or known);

i. a proposed item name (using NCS approved nomenclature if appropriate);

j. the reference / part number, manufacturer and name of the next higher assembly;

k. manufacturer's documents that provide a comprehensive description of the item (ie, the design / procurement specification, product or technical data sheet) and that define the characteristics or features required for form, fit and function (noting that, as appropriate, this information includes performance, dimensional, physical, electrical, mechanical, material, finishing and construction characteristics; and, as applicable, this sub-clause might require the provision of design drawings, manuals, tender specifications, design specifications, Safety Data Sheets, and other information);

l. volumetric information, complementary to the dimensional data required by clause 6.2.1.1k, for:

(i) unpackaged Stock Items (including length, width, depth, net weight and units of measure);

(ii) packaged Stock Items (including the quantity of units per pack, the gross length, width, depth, cube and weight per unit pack, units of measure, and unit packs per intermediate container); and

(iii) if applicable, palletisation (including quantity of intermediate containers per pallet layer, number of layers per pallet, pallet width, depth, height and gross weight); and

m. a statement as to whether the particular part identified at clause 6.2.1.1c and 6.2.1.1d above is fully item identifying (noting that a part number is fully item identifying where, without any further definition, any item of production bearing that part number has the characteristics defined at clause 6.2.1.1k above).

6.2.2 Data for Each Item Already Codified in the NATO Codification System

6.2.2.1 For each Stock Item, which is already codified in the NATO Codification System, the CDATA shall list the following information:

a. NATO Stock Number (NSN);

b. item name;

c. true manufacturer's name, NCAGE Code and item reference / part number; and

d. supplier's name, NCAGE Code and item reference / part number.

[1] Note that the abbreviation NCAGE may appear CAGE in other parts of the Contract that directly refer to related US standards.

6.2.3 Changes to Provided Information

6.2.3.1 On occasions, it might become necessary to advise changes to previously provided information. For example, it might be subsequently found that the information supplied originally is incorrect or incomplete, the manufacturer/supplier has advised changes or that additional manufacturer’s references are found to be applicable. In these cases, an amendment to the CDATA shall be provided to the Commonwealth (as required by the CDRL), which details the changed information, appropriately cross-referenced to the NSN (if known), the true manufacturer’s name, NCAGE Code and reference / part number originally advised.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-TDATA-LSAR-V5.3

Note to drafters: Tailorable elements of this DID (eg, the population of tables for each review and the Data Selection Sheet) should be tailored for inclusion in request for tender documents. Subsequently, these elements should also be reviewed pre-contract with the preferred tenderer and in the context of their proposed solution.

2. TITLE: LOGISTIC SUPPORT ANALYSIS RECORD

3. DESCRIPTION AND INTENDED USE

3.1 This Logistic Support Analysis (LSA) Record (LSAR) DID defines the data population requirements for the LSAR, to support project LSA Activities and to produce outputs for ILS products.

3.2 The Contractor and the Commonwealth use the LSAR as common source database for LSA and related analysis processes, and as the basis for a source for the data required to produce specific Technical Data and ILS products derived from the LSA process.

3.3 The Commonwealth also uses the LSAR to:

a. assist with its understanding of the Contractor’s designs for, and scope of work with respect to, both the Mission System and the Support System;

b. assist with monitoring the Contractor’s developmental activities under the Contract; and

c. identify and understand the Commonwealth’s scope of work with respect to reviewing and implementing ILS outcomes.

4. INTER-RELATIONSHIPS

4.1 The LSAR is subordinate to the following data items, where these data items are required under the Contract:

a. Integrated Support Plan (ISP); and

b. Life Cycle Cost Management Plan (LCCMP).

4.2 The LSAR inter-relates with the following data items, where these data items are required under the Contract:

a. Task Analysis Report (TAR);

b. Failure Modes Effects and Criticality Analysis Report (FMECAR);

c. Reliability Centred Maintenance Analysis Report (RCMAR);

d. Level of Repair Analysis Report (LORAR);

e. Life Cycle Cost Report and Model (LCCRM);

f. Recommended Spares Provisioning List (RSPL);

g. Support and Test Equipment Provisioning List (S&TEPL);

h. Packaging Provisioning List (PACKPL);

i. Recommended Provisioning List (RPL);

j. Personnel Resource Requirements List (PRRL);

k. Performance Needs Analysis Report (PNAR);

l. Training Equipment List (TEL);

m. Support System Technical Data List (SSTDL); and

n. Facilities Requirements Analysis Report (FRAR).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

DEF(AUST)5692 Issue 3	*Logistic Support Analysis Record Requirements for the Australian Defence Organisation*

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall be submitted with the delivery advice details provided in a format that complies with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item LSAR data shall comply with the data format, structure, and transfer requirements for validated LSAR systems as defined in DEF(AUST)5692.

6.2 Specific Content

6.2.1 Delivery Advice Details

6.2.1.1 Delivery Overview: This section shall summarise the purpose and contents of the data delivery and shall describe any security or privacy considerations associated with its use.

6.2.1.2 Data Population: This section shall briefly state the data growth for the initial delivery or between the current and previous deliveries. Data growth shall be described in terms of:

a. the system(s) for which data has been populated;

b. the indenture level of systems to which data has been populated; and

c. data tables populated.

6.2.1.3 The term ‘populated data tables’, as used in this DID, does not imply that all data fields within a table must be populated. Only those data fields identified by the Data Selection Sheet at Annex A to this DID and the data required by the LSAR Table Rules for population of that table are required (ie, includes key fields and table rules described in DEF(AUST)5692).

6.2.2 LSAR Data Requirements

6.2.2.1 General

6.2.2.1.1 This section describes the data requirements for delivery as LSAR data via data transfer file, on-line access, or both, as required by the Statement of Work (SOW).

6.2.2.1.2 Where on-line access to the Contractor's LSAR is available, the term ‘delivered data’ is synonymous to that data being available on-line, at the specified time/milestone, with the ability to produce standard and ad hoc reports in accordance with DEF(AUST)5692.

6.2.2.1.3 Each LSAR data delivery shall include the details identified against the Mandated System Reviews, which list applicability, indenture level and the data tables populated for the Mission System and Support System. Data required from those tables is listed in the Data Selection Sheet at Annex A; if there is a conflict between the identification of a data table and the Data Selection Sheet, the Data Selection Sheet takes precedence.

6.2.2.2 System Requirements Review

6.2.2.2.1 The purpose of delivered data for System Requirements Review (SRR) is to ensure that the user/operator requirements have been captured in the LSAR. The requirements of this clause 6.2.2.2 are not applicable if an SRR is not required under the Contract.

6.2.2.2.2 Delivered Data - Systems and Indenture Levels: The following data shall be populated to the following indenture levels unless otherwise specified in the ‘Populated Tables’ section:

a. Mission System - Level 3 Functional only (not applicable to A Tables, refer to the ‘Delivered Data - Populated Tables’ section below); and

b. Support System - Level 1 Functional and Level 1 Physical.

6.2.2.2.3 Delivered Data - Populated Tables: The following table describes the data table requirements, by LSAR table, for the SRR; refer to the Data Selection Sheet at Annex A for the data requirements within each table group/table.

Table Group or Table(s)	Requirement	Objective
XA	As per Data Selection Sheet using a functional structure.	The LSAR shall record the project data identified for this table.
XB, XC	As per Data Selection Sheet	The LSAR shall identify top-level Mission System structures and Support System Components to meet specified requirements.
A Group	As per Data Selection Sheet	The LSAR shall record the specified operational requirements for the Mission System (Level 1) and those subsystems (to Level 2 or 3) with different operating rates.[1]

6.2.2.3 System Definition Review

6.2.2.3.1 The purpose of delivered data for the System Definition Review (SDR) is to capture the high level functional design in the LSAR and verify that intended Reliability, Availability and Maintainability (RAM) characteristics are consistent with specified user/operator requirements. The requirements of this clause 6.2.2.3 are not applicable if an SDR is not required under the Contract.

6.2.2.3.2 Delivered Data - Systems and Indenture Levels: The following data shall be populated to the following indenture levels unless otherwise specified in the 'Populated Tables' section:

a. Mission System - Level 3 Functional items cross-mapped to physical items, at any level, used to substantiate projected RAM characteristics; and

b. Support System - Level 1 Functional and Level 1 Physical.

6.2.2.3.3 Delivered Data - Populated Tables: The following table describes the data table requirements, by LSAR table, for the SDR; refer to the Data Selection Sheet at Annex A for the data requirements within each table group/table.

Table Group or Table(s)	Requirement	Objective
XA	Updates as applicable	
XB, XC, XF	As per Data Selection Sheet	The LSAR shall identify the Mission System functional LCN structure for each proposed configuration via a Usable On Code (UOC). The LSAR shall identify Support System Components where they are specific to an individual UOC.
XG	As per Data Selection Sheet	The LSAR shall record the cross-referencing between the functional and physical Mission System LCN structures.
A Group	Updates as applicable	
BA, BB, BC, BD, BE	As per Data Selection Sheet	The LSAR shall record the allocated / comparative / predicted RAM characteristics for the recorded Mission System components. These will be compared against requirements.

6.2.2.4 Preliminary Design Review

6.2.2.4.1 The purpose of delivered data for the Preliminary Design Review (PDR) is to introduce the physical Mission System structure, its failure modes, and to assess Materiel Safety. Results of FMECA are used to verify analyst understanding of mission criticality by mission phase, and Materiel Safety. Unacceptable safety or mission failures may be identified. RCM analysis results are required for failure modes identified with a severity class affecting safety, including any resulting preventive maintenance or proposed design changes. The requirements of this clause 6.2.2.4 are not applicable if a PDR is not required under the Contract.

[1] Only identify systems/subsystems that have distinctly different operating rates to the Mission System. For example, an aircraft uses flying hours for the Mission System, landings are entered for the 'landing subsystem' (ie, physical undercarriage), etc.

6.2.2.4.2 Delivered Data - Systems and Indenture Levels: The following data shall be populated to the following indenture levels unless otherwise specified in the 'Populated Tables' section:

a. Mission System - Level […INSERT INDENTURE LEVEL…] Physical / Level 3 Functional; and

b. Support System Components - Level 1 Physical and Level 1 Functional.

Note to drafters: The number of physical indenture levels will depend upon the actual number of levels for a Mission System / end item and the depth needed to support the FMECA and RCM analysis data. A decision need to be made on how far down this analysis goes and also for limits of related data for OTS items used within the end item.

6.2.2.4.3 Delivered Data - Populated Tables: The following table describes the data table requirements, by LSAR table, for the PDR; refer to the Data Selection Sheet at Annex A for the data requirements within each table group/table.

Table Group or Table(s)	Requirement	Objective
XA, XB, XC, XF	As per Data Selection Sheet with physical LCN Structure.	The LSAR shall record the Mission System physical LCN structure.
XG	Updates as applicable	
XH	As per Data Selection Sheet	The LSAR shall identify the Contractor and Subcontractors who will provide reference numbered items.
A Group	Updates if applicable	
BA - BE	Updates for physical LCN Structure items, including significant Support System Components.	
BF - BL, RI, VF	As per Data Selection Sheet for FMEA and FMECA data, and RCM analysis of safety critical failures.	The LSAR shall record the identified failure modes of the Mission System. This shall enable verification of criticality (including mission criticality) assessments via LSA-056 and safety related RCM analysis via LSA-050.
CA	Key and Mandatory fields only. For tasks identified from FMECA and RCM.	The LSAR shall identify Mission System tasks resulting from FMECA and RCM analysis for safety critical failures.
EA, EE	As per Data Selection Sheet for special to type Support & Test Equipment (S&TE) and Training Equipment, and those which are LLTIs.	The LSAR shall identify and provide explanations/justification for special-to-type S&TE. The LSAR shall identify S&TE and Training Equipment that are LLTIs through EA, HA and HG.
FA	As per Data Selection Sheet	The LSAR shall identify the names, category and types of facilities required.
HA	Part Identification details and Long Lead Time Item (LLTI) Provisioning Category Code only; excludes other indicator codes, dimensions, etc.	The LSAR shall record known part (reference) numbers to a level that matches the Physical LCN structure. This shall enable a review of LCN structure via LSA-126. The LSAR shall identify LLTIs to enable LLTI provisioning.
HD, HO	As per Data Selection Sheet for LLTIs.	The LLTI Provisioning Technical Documentation (PTD) list shall be recorded in the LSAR.
HG	Key fields.	As per HA.
VR, VS, VT	As per Data Selection Sheet	Identify Mission System roles and role equipment, as applicable.

6.2.2.5 Detailed Design Review

6.2.2.5.1 The purpose of the delivered data for the Detailed Design Review (DDR) is to ensure that there will be no design changes to the Mission System following DDR due to:

a. unacceptable failure modes;

b. unmaintainable designs; or

c. designs that do not represent a solution that minimises LCC, in accordance with the Approved governing plan for LCC under the Contract (eg, the LCCMP).

6.2.2.5.2 Demonstrating that the design has stabilised for the above purposes requires the FMECA and RCM analysis of the Mission System to be complete. The delivered data enables the estimation of In-Service logistic requirements for Personnel and Facilities, and to review the achievability of the Australian Industry Capability (AIC) program from the preliminary maintenance allocations. The requirements of this clause 6.2.2.5 are not applicable if a DDR is not required under the Contract.

6.2.2.5.3 Delivered Data - Systems and Indenture Levels: The following data shall be populated to the following indenture levels unless otherwise specified in the 'Populated Tables' section:

a. Mission System - All project applicable levels Physical / Level 3 Functional; and

b. Support System Components - Level 1 Physical and Level 1 Functional.

6.2.2.5.4 Delivered Data - Populated Tables: The following table describes the data table requirements, by LSAR table, for the DDR; refer to the Data Selection Sheet at Annex A for the data requirements within each table group/table.

Table Group or Table(s)	Requirement	Objective
X, A Groups	Updates as applicable	
BA – BE	Updates as applicable	
BF - BL, RI, VF	As per Data Selection Sheet, including all FMECA and RCM results, and related tasks.	The LSAR shall identify all Mission System maintenance tasks, with traceability to FMECA and RCM analysis.
CA, CB	As per Data Selection Sheet for operator, maintenance and significant support tasks[2]. Include task/subtask identification, frequencies and predicted times.	The LSAR shall identify task requirements and preliminary maintenance allocations. This enables an assessment of achieving preparedness and LCC requirements based on R&M and task information. Review via ad hoc reports and LSA-016.
CD	As per Data Selection Sheet for operator and maintenance tasks.	The LSAR shall identify personnel requirements for on-equipment tasks. Review via LSA-001 and LSA-065.
CG, CI	As per Data Selection Sheet for on-equipment tasks.	The LSAR shall identify spares, S&TE and other provisioned items for on-equipment tasks.
EA, EE	Update as applicable, including all S&TE used or stored on-equipment.	
FA, FE	As per Data Selection Sheet	The LSAR shall identify facilities requirements for operations (if applicable), maintenance, and other listed support tasks.
GA, GB, GC	As per Data Selection Sheet	The LSAR shall document existing applicable ADF skills for allocation to tasks, and new or modified skills (if applicable) required to perform tasks.
HA	As per Data Selection Sheet, excluding Provisioning List Category Code (PLCC) data. Including existing NATO Stock Numbers (NSNs).	The LSAR shall identify part (reference) numbers for all Mission System LSA Candidate Items[3] and all items used in operation and on-equipment maintenance and support.
HD, HG, HO	Update as applicable	
JA, JF	As per Data Selection Sheet	The LSAR shall record requirements and remarks pertinent to the transport of the end items, as required for the operation and support concepts.
MA, ME	Applicable to items/tasks.	
RA, RB	As per Data Selection Sheet	To identify work area codes and descriptions.
VR, VS, VT	Update as applicable	
WV, WY	As per Data Selection Sheet	

[2] Significant support tasks include preparation for transport of the end item or subsystems, special preparations for storage, etc.

[3] Generally, LSA Candidate Items are maintenance significant items, structural items requiring inspection, and any item that must be identified in the supply chain; as specified under the Contract. Bulk items and consumables are generally not Candidate Items.

6.2.2.6 Support System Detailed Design Review

6.2.2.6.1 The purpose of delivered data for the Support System Detailed Design Review (SSDDR) is to agree to the maintenance and support policies and to scope the related resource requirements. The SSDDR enables the development of ILS Products to commence, including provisioning lists, training material, and technical and support manuals. The SSDDR is the final review at which the Contractor demonstrates that its solution for the combined Mission System and Support System:

a. represents a minimum LCC solution, as demonstrated in accordance with the Approved governing plan for the management of LCC under the Contract (eg, LCCMP); and

b. will meet the requirements of the AIC program, as documented in the AIC Plan.

6.2.2.6.2 The requirements of this clause 6.2.2.6 are not applicable if an SSDDR is not required under the Contract.

6.2.2.6.3 Delivered Data - Systems and Indenture Levels. The LSAR data shall be populated to the following indenture levels unless otherwise specified in the 'Populated Tables' section:

a. Mission System - All project applicable levels Physical / Level 3 Functional; and

b. Support System Components - All project applicable levels required for the levels of repair and support of all support equipment, including S&TE and Training Equipment, for the Physical structure / Level 1 Functional.

6.2.2.6.4 Delivered Data - Populated Tables. The following table describes the data table requirements, by LSAR table, for the SSDDR; refer to the Data Selection Sheet at Annex A for the data requirements within each table group/table.

Table Group or Table(s)	Requirement	Objective
X, A, F, G, J Group	As per Data Selection Sheet with updates as applicable.	
XI	As per Data Selection Sheet.	The LSAR shall record Technical Manual Codes and Index Numbers.
B Group	Updates as applicable, including Support System Components requiring support.	The LSAR shall record R&M characteristics for all applicable to items with logistic support requirements.
CA, CB, CD	As per Data Selection Sheet for all tasks. Update maintenance allocations as a result of Level of Repair Analysis (LORA) for all tasks performed in country. Identify tasks with a training requirement.	The LSAR shall record task requirements and optimised maintenance allocations. The LSAR shall identify the tasks that require training for the training task inventory. The LSAR shall be reviewed to assess the achievement of preparedness and LCC requirements based on task information. Review tasks via ad hoc reports, LSA-016, and 023 or 024.
CE, CF, CG, CH, CI	As per Data Selection Sheet.	The LSAR shall identify maintenance task allocations based on non-economic LORA criteria. The LSAR shall identify resource requirements to tasks as required for conducting LORA. Tasks are to be allocated to operator and technical manuals.
E Group	As per Data Selection Sheet.	The LSAR shall identify all support equipment required for calculating the system resource requirements and conducting LORA.
U Group	As per Data Selection Sheet and as required to justify selected Test Equipment.	To justify identified Test Equipment.
HA	Updates as applicable, including Support System Components and items used to support them.	The LSAR shall identify all items for potential provisioning action and screening against existing In-Service items.
HD, HE, HF	As per Data Selection Sheet.	The LSAR shall identify the spares, packaging and resource costs for LORA.

Table Group or Table(s)	Requirement	Objective
HG	As per Data Selection Sheet, including SMR, Maintenance Task Distribution and PTDs identified in the Data Selection Sheet.	As per HA. The LSAR shall identify LRUs, assemblies and overhaul kits, task distributions, etc, for and from LORA.
MA, MC-MF	As applicable.	Narrative to provide sufficient explanation where required.
MB	As per Data Selection Sheet.	Required to describe each Maintenance Policy Trade.
RA, RB, RI	Updates if applicable.	
RM	As per Data Selection Sheet.	The LSAR shall identify each Maintenance Policy Trade.
VR – VT, VF	Updates if applicable.	
VE	As per Data Selection Sheet.	To justify task facilities.
WA – WD, WL – WR	As per Data Selection Sheet.	The LSAR shall identify tasks allocated to servicing schedules.
WV, WY	Updates if applicable.	

6.2.2.7 Task Analysis Requirements Review

6.2.2.7.1 The purpose of delivered data for the Task Analysis Requirements Review (TARR) is to review task narratives and maintenance allocations, personnel and resource requirements, S&TE requirements and application, and training requirements prior to the development of the technical manuals, training courses, and other ILS Technical Data products. Following this review, the production of publications, Training courses, and maintenance plans, can proceed based on consistent and integrated analysis data. The requirements of this clause 6.2.2.7 are not applicable if a TARR is not required under the Contract.

6.2.2.7.2 Delivered Data - Systems and Indenture Levels: The LSAR data shall be populated to the indenture levels described for the SSDDR.

6.2.2.7.3 Delivered Data - Populated Tables: The following table describes the data table requirements, by LSAR table, for the TARR; refer to the Data Selection Sheet at Annex A for the data requirements within each table group/table.

Table Group or Table(s)	Requirement	Objective
X, A, B, E, U, F, G, J, M Groups	Updates as applicable.	
XI	Updates as applicable.	LSAR to include Illustrated Parts Catalogue (IPC) identification.
CA, CB, CD, CE, CF, CG, CH, CI	Updates as applicable.	The LSAR shall record all task data necessary to enable the calculation of resource requirements.
CC	As per Data Selection Sheet.	The LSAR shall record narratives for all tasks to be performed in country for In-service support where existing off-the-shelf manuals have not been approved. Review via LSA-016, 018, 019.
CJ, CK	As per Data Selection Sheet.	The LSAR shall record task inventories for duties and jobs and place tasks in the applicable technical manuals.
HA – HG, HK, HL	As per Data Selection Sheet, with updates as applicable.	
R Group	As per Data Selection Sheet, with updates as applicable.	The LSAR shall document information to produce Technical Maintenance Plans (TMPs) and Planned Servicing Schedules (PSSs).
VE, VF, VR – VT	Updates as applicable.	
WA – WC, WM – WR	Updates as applicable.	

Table Group or Table(s)	Requirement	Objective
WG, WH, WS – WT, WX	As per Data Selection Sheet.	The LSAR shall document information to produce Planned Servicing Schedules.
Z Group	For LRU TMPs and PSSs.	***Note to drafters: These tables are primarily used by Aerospace, see DEF(AUST)5692 Issue 3.*** As per R table group (above) for Maintenance Managed Items (MMIs).

6.2.2.8 Provisioning Preparedness Review

6.2.2.8.1 The purpose of delivered data for the Provisioning Preparedness Review(s) is to review recommended provisioning lists for all spares, consumables, and support, test and training equipment. The requirements of this clause 6.2.2.8 are not applicable if Provisioning Preparedness Reviews are not required under the Contract.

6.2.2.8.2 Delivered Data - Systems and Indenture Levels: The LSAR data shall be populated to the indenture levels described for the SSDDR.

6.2.2.8.3 Delivered Data - Populated Tables: The following table describes the data table requirements, by LSAR table, for the Provisioning Preparedness Review(s); refer to the Data Selection Sheet at Annex A for the data requirements within each table group/table.

Table Group or Table(s)	Requirement	Objective/Note
X, A, B, C, E, U, F, G, J, M, R Groups	Updates if applicable.	
XD, XE	As per Data Selection Sheet.	The LSAR shall record any variations of Mission System or Support System configuration based on Serial Numbered End Items (if applicable).
HA – HF, HK, HL	Update as applicable.	
HG – HJ, HM, HO	As per Data Selection Sheet with updates as applicable.	The LSAR shall record updates to provisioning recommendations for use in approved provisioning lists, including repair and overhaul kits, IPC references and comments.
HN	As per Data Selection Sheet.	LSAR to address provisioning requirements that vary by serial numbered end item.
V Group	Updates as applicable.	
VA – VD	As per Data Selection Sheet.	LSAR shall record demand management details for supply management systems.
W Group	Updates as applicable.	
WE , WF, WI – WK	As per Data Selection Sheet.	LSAR shall record alternative part identification and authority for use details.

6.2.2.9 Functional Configuration Audit and Physical Configuration Audit

6.2.2.9.1 As part of the Functional Configuration Audit (FCA) and Physical Configuration Audit (PCA) the LSAR is to be validated to ensure that the LSAR is consistent with the build structures of, and interfaces between, the Mission System and Support System. The requirements of this clause 6.2.2.9 are not applicable if a FCA and a PCA are not required under the Contract.

6.2.2.9.2 Delivered Data: The LSAR shall have all of the specified data elements completed for all applicable indenture levels for both the Mission System and Support System for the purposes of the FCA and PCA.

6.3 Annex

A. Data Selection Sheet

ANNEX A TO DID-ILS-TDATA-LSAR

DATA SELECTION SHEET

Note to drafters: Identify the required elements in the Data Selection Sheet to suit the requirements of the project.

Data Element	Key	DED	DE CODE	Required
CROSS FUNCTIONAL REQUIREMENTS				
TABLE XA: END ITEM ACRONYM CODE				
END ITEM ACRONYM CODE (EIAC)	K	096	EIACODXA	
LCN STRUCTURE		202	LCNSTRXA	
ADMINISTRATIVE LEAD TIME	G	014	ADDLTMXA	
CONTACT TEAM DELAY TIME	G	052	CTDLTMXA	
CONTRACT NUMBER	G	055	CONTNOXA	
COST PER REORDER ACTION	G	061	CSREORXA	
COST PER REQUISITION	G	062	CSPRRQXA	
DEMILITARIZATION COST	G	077	DEMILCXA	
DISCOUNT RATE	G	083	DISCNTXA	
HOLDING COST PERCENTAGE	G	160	HLCSPCXA	
ESTIMATED SALVAGE VALUE	G	102	ESSALVXA	
INITIAL BIN COST	G	166	INTBINXA	
INITIAL CATALOGUING COST	G	167	INCATCXA	
INTEREST RATE	G	173	INTRATXA	
INVENTORY STORAGE SPACE COST	G	176	INVSTGXA	
LOADING FACTOR	G	195	LODFACXA	
OPERATION LEVEL	G	271	WSOPLVXA	
OPERATION LIFE	G	272	OPRLIFXA	
PERSONNEL TURNOVER RATE	G	289	-----	
PRODUCTIVITY FACTOR	G	300	PROFACXA	
RECURRING BIN COST	G	333	RCBINCXA	
RECURRING CATALOGUING COST	G	334	RCCATCXA	
RETAIL STOCKAGE CRITERIA	G	359	RESTCRXA	
SAFETY LEVEL	G	363	SAFLVLXA	
SUPPORT OF SUPPORT EQUIPMENT COST FACTOR	G	421	SECSFCXA	
TRANSPORTATION COST	G	466	TRNCSTXA	
TYPE ACQUISITION	G	478	WSTYAQXA	
TYPE OF SUPPLY SYSTEM CODE	G	484	TSSCODXA	
TABLE XB: LSA CONTROL NUMBER INDENTURED ITEM				
LSA CONTROL NUMBER (LCN)	K	199	LSACONXB	
ALTERNATE LCN CODE	K	019	ALTLCNXB	
LCN TYPE	K	203	LCNTYPXB	
LCN INDENTURE CODE (LCN-IC)		200	LCNINDXB	
LCN NOMENCLATURE		201	LCNAMEXB	
TECHNICAL MANUAL FUNCTIONAL GROUP CODE (MAINTENANCE ALLOCATION CHART)		438	TMFGCDXB	
SYSTEM/END ITEM IDENTIFIER		423	SYSIDNXB	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
SECTIONALIZED ITEM TRANSPORTATION INDICATOR		367	SECITMXB	
RELIABILITY AVAILABILITY MAINTAINABILITY INDICATOR		342	RAMINDXB	
TABLE XC: SYSTEM/END ITEM				
USABLE ON CODE (UOC)	G	501	UOCSEIXC	
SYSTEM/EI PROVISIONING CONTRACT CONTROL NUMBER	G	307	PCCNUMXC	
SYSTEM/EI ITEM DESIGNATOR CODE		179	ITMDESXC	
SYSTEM/EI PROVISIONING LIST ITEM SEQUENCE NUMBER		309	PLISNOXC	
SYSTEM/EI TYPE OF CHANGE CODE		481	TOCCODXC	
SYSTEM/EI QUANTITY PER ASSEMBLY		316	QTYASYXC	
SYSTEM/EI QUANTITY PER END ITEM		317	QTYPEIXC	
TRANSPORTATION END ITEM INDICATOR		467	TRASEIXC	
TABLE XD: SYSTEM/END ITEM SERIAL NUMBER				
SERIAL NUMBER	K	373	-----	
SERIAL NUMBER USEABLE ON CODE		375	SNUUOCXD	
TABLE XE: LCN TO SERIAL NUMBER USABLE ON CODE				
SELECT TABLE XE				
TABLE XF: LCN TO SYSTEM/END ITEM USABLE ON CODE				
SELECT TABLE XF				
TABLE XG: FUNCTIONAL/PHYSICAL LCN MAPPING				
SELECT TABLE XG				
TABLE XH: COMMERCIAL AND GOVERNMENT ENTITY CODE				
COMMERCIAL AND GOVERNMENT ENTITY (CAGE) CODE	K	046	CAGECDXH	
CAGE NAME		047	CANAMEXH	
CAGE ADDRESS		047	-----	
TABLE XI: TECHNICAL MANUAL CODE AND NUMBER INDEX				
TECHNICAL MANUAL (TM) CODE	K	437	TMCODEXI	
TECHNICAL MANUAL NUMBER	G	440	TMNUMBXI	
OPERATIONS AND MAINTENANCE REQUIREMENTS				
TABLE AA: OPERATIONS AND MAINTENANCE REQUIREMENT				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
SERVICE DESIGNATOR CODE	K	376	SERDESAA	
REQUIRED MAXIMUM TIME TO REPAIR	G	222	MAXTTRAA	
REQUIRED PERCENTILE	G	286	PERCENAA	
REQUIRED ACHIEVED AVAILABILITY	G	001	ACHAVAAA	
REQUIRED INHERENT AVAILABILITY	G	164	INHAVAAA	
OPERATIONAL MEAN ACTIVE MAINTENANCE DOWNTIME	G	223	OMAMDTAA	
TECHNICAL MEAN ACTIVE MAINTENANCE DOWNTIME	G	223	TMAMDTAA	
REQUIRED OPERATIONAL MEAN TIME TO REPAIR	G	236	OPMTTRAA	
REQUIRED TECHNICAL MEAN TIME TO REPAIR	G	236	TEMTTRAA	

Data Element	Key	DED	DE CODE	Required
NUMBER OF OPERATING LOCATIONS	G	262	NUOPLOAA	
CREW SIZE	G	064	CREWSZAA	
TOTAL SYSTEMS SUPPORTED	G	454	TOSYSUAA	
RELIABILITY CENTERED MAINTENANCE LOGIC UTILIZED	G	345	RCMLOGAA	
TABLE AB: WAR/PEACE OPERATIONS AND MAINTENANCE REQUIREMENT				
OPERATIONAL REQUIREMENT INDICATOR	K	275	OPRQINAB	
ANNUAL NUMBER OF MISSIONS	G	021	ANNOMIAB	
ANNUAL OPERATING DAYS	G	022	ANOPDAAB	
ANNUAL OPERATING TIME	G	024	ANOPTIAB	
MEAN MISSION DURATION	G	228	MMISDUAB	
REQUIRED OPERATIONAL AVAILABILITY	G	273	OPAVAIAB	
REQUIRED ADMINISTRATIVE AND LOGISTIC DELAY TIME	G	013	OPALDTAB	
REQUIRED STANDBY TIME	G	403	OSTBTIAB	
TABLE AC: MAINTENANCE LEVEL REQUIREMENT				
OPERATIONS AND MAINTENANCE LEVEL CODE	K	277	OMLVLCAC	
MAINTENANCE LEVEL MAXIMUM TIME TO REPAIR	G	222	MLMTTRAC	
MAINTENANCE LEVEL PERCENTILE	G	286	MLPERCAC	
NUMBER OF SYSTEMS SUPPORTED	G	265	MLNSSUAC	
MAINTENANCE LEVEL SCHEDULED ANNUAL MAN-HOURS	G	020	MLSAMHAC	
MAINTENANCE LEVEL UNSCHEDULED ANNUAL MAN-HOURS	G	020	MLUAMHAC	
SCHEDULED MAN-HOUR PER OPERATING HOUR	G	215	MLSMHOAC	
UNSCHEDULED MAN-HOUR PER OPERATING HOUR	G	215	MLUMHOAC	
UNSCHEDULED MAINTENANCE MEAN ELAPSED TIME	G	499	MLUMETAC	
UNSCHEDULED MAINTENANCE MEAN MAN-HOURS	G	499	MLUMMHAC	
TABLE AD: ORGANIZATIONAL LEVEL REQUIREMENT				
DAILY INSPECTION MEAN ELAPSED TIME	G	280	DINMETAD	
DAILY INSPECTION MEAN MAN-HOURS	G	280	DINMMHAD	
PRE-OPERATIVE INSPECTION MEAN ELAPSED TIME	G	280	PREMETAD	
PRE-OPERATIVE INSPECTION MEAN MAN-HOURS	G	280	PREMMHAD	
POSTOPERATIVE INSPECTION MEAN ELAPSED TIME	G	280	POIMETAD	
POSTOPERATIVE INSPECTION MEAN MAN-HOURS	G	280	POIMMHAD	
PERIODIC INSPECTION MEAN ELAPSED TIME	G	280	PINMETAD	
PERIODIC INSPECTION MEAN MAN-HOURS	G	280	PINMMHAD	
MISSION PROFILE CHANGE MEAN ELAPSED TIME	G	280	MPCMETAD	
MISSION PROFILE CHANGE MEAN MAN-HOURS	G	280	MPCMMHAD	
TURNAROUND INSPECTION MEAN ELAPSED TIME	G	280	TINMETAD	
TURNAROUND INSPECTION MEAN MAN-HOURS	G	280	TINMMHAD	
TABLE AE: SKILL OPERATIONS AND MAINTENANCE REQUIREMENT				
SKILL SPECIALTY CODE	F	387	SKSPCDGA	
AVAILABLE MAN-HOUR	G	028	AVAIMHAE	
AVAILABLE QUANTITY	G	324	QTYAVAAE	
UTILIZATION RATIO	G	503	UTRATIAE	

Data Element	Key	DED	DE CODE	Required
TABLE AF: WAR/PEACE ADDITIONAL REQUIREMENTS NARRATIVE				
ADDITIONAL REQUIREMENTS	G	009	WPADDRAF	
TABLE AG: RELIABILITY REQUIREMENT				
ANNUAL OPERATING REQUIREMENT	M	023	ANOPREAG	
RELIABILITY OPERATIONAL REQUIREMENTS INDICATOR	M	275	OPRQINAG	
REQUIRED OPERATIONAL MEAN TIME BETWEEN FAILURES	G	229	OPMTBFAG	
REQUIRED TECHNICAL MEAN TIME BETWEEN FAILURES	G	229	TEMTBFAG	
REQUIRED OPERATIONAL MEAN TIME BETWEEN MAINTENANCE ACTIONS	G	230	OPMRBMAG	
REQUIRED TECHNICAL MEAN TIME BETWEEN MAINTENANCE ACTIONS	G	230	TMTBMAAG	
REQUIRED MEAN TIME BETWEEN REMOVALS	G	235	MTBRXXAG	
TABLE AH: INTEROPERABILITY REQUIREMENT				
INTEROPERABLE ITEM NAME	K	182	IONAMEAH	
INTEROPERABLE ITEM NUMBER TYPE	K	266	IOINTYAH	
INTEROPERABLE CAGE CODE	G	046	IOCAGEAH	
INTEROPERABLE REFERENCE NUMBER	G	337	IOREFNAH	
INTEROPERABLE ITEM NATIONAL STOCK NUMBER	G	253	-----	
INTEROPERABLE ITEM TECHNICAL MANUAL NUMBER	G	440	IOITNMAH	
TABLE AI: MODELLING DATA				
MODELLING SERVICE DESIGNATOR CODE	K	376	SERDESAI	
MODELLING OPERATIONS AND MAINTENANCE LEVEL CODE	K	277	OMLVLCAI	
LABOUR RATE	G	189	LABRATAI	
NUMBER OF SHOPS	G	263	NOSHPSAI	
REPAIR WORK SPACE COST	G	352	RPWSCSAI	
REQUIRED DAYS OF STOCK	G	357	RQDSTKAI	
TABLE AJ: OPERATIONS AND MAINTENANCE SHIPPING REQUIREMENT				
OPERATIONS AND MAINTENANCE LEVEL FROM	K	277	OMLVLFAJ	
OPERATIONS AND MAINTENANCE LEVEL TO	K	277	OMLVLTAJ	
SHIP DISTANCE	G	085	SHPDISAJ	
SHIP TIME	G	379	TIMESHAJ	
TABLE AK: SYSTEM/END ITEM NARRATIVE				
SYSTEM/END ITEM NARRATIVE CODE	K	424	SEINCDAK	
ADDITIONAL SUPPORTABILITY CONSIDERATIONS	G	010		
ADDITIONAL SUPPORTABILITY PARAMETERS	G	011		
OPERATIONAL MISSION FAILURE DEFINITION	G	274		
ITEM RELIABILITY, AVAILABILITY, AND MAINTAINABILITY REQUIREMENTS; FAILURE MODES EFFECTS AND CRITICALITY ANALYSIS; AND MAINTAINABILITY ANALYSIS				
TABLE BA: RELIABILITY, AVAILABILITY, AND MAINTAINABILITY CHARACTERISTICS				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
MINIMUM EQUIPMENT LIST INDICATOR		243	MEQLINBA	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
CONVERSION FACTOR		059	CONVFABA	
FAULT ISOLATION		143	-----	
BIT DETECTABILITY LEVEL PERCENTAGE		032	-----	
BUILT-IN-TEST CANNOT DUPLICATE PERCENTAGE		031	BITNDPBA	
BUILT-IN-TEST RETEST OK PERCENT		033	BITROPBA	
FAILURE RATE DATA SOURCE		141	FRDATABA	
PILOT REWORK OVERHAUL CANDIDATE		292	PREOVCBA	
SECURITY CLEARANCE		369	SECCLEBA	
SUPPORT CONCEPT		410	SUPCONBA	
WEAROUT LIFE		505	WEOULIBA	
LOGISTIC CONSIDERATIONS		196	-----	
TABLE BB: RELIABILITY, AVAILABILITY, AND MAINTAINABILITY CHARACTERISTICS NARRATIVE				
RAM CHARACTERISTICS NARRATIVE CODE	K	341	RAMCNABB	
ITEM FUNCTION		180		
MAINTENANCE CONCEPT		207		
MINIMUM EQUIPMENT LIST NARRATIVE		244		
QUALITATIVE & QUANTITATIVE MAINTAINABILITY RQMT		315		
MAINTENANCE PLAN RATIONALE		210		
TABLE BC: RELIABILITY, AVAILABILITY, AND MAINTAINABILITY LOGISTICS CONSIDERATIONS				
LOGISTICS CONSIDERATION CODE	K	425	LOCOCOBC	
RAM LOGISTICS CONSIDERATIONS		426	LOGNARBC	
TABLE BD: RELIABILITY, AVAILABILITY, AND MAINTAINABILITY INDICATOR CHARACTERISTICS				
RAM INDICATOR CODE	K	347	RAMINDBD	
ACHIEVED AVAILABILITY		001	ACHAVABD	
INHERENT AVAILABILITY		164	INHAVABD	
FAILURE RATE		140	FAILRTBD	
INHERENT MAINTENANCE FACTOR		165	INHMAFBD	
MAXIMUM TIME TO REPAIR (MAXTTR)		222	MAXTTRBD	
PERCENTILE		286	PERCENBD	
MEAN TIME TO REPAIR OPERATIONAL		236	MTTROPBD	
MEAN TIME TO REPAIR TECHNICAL		236	MTTRTHBD	
MEAN TIME BETWEEN FAILURES OPERATIONAL		229	OPMTBFBD	
MEAN TIME BETWEEN FAILURES TECHNICAL		229	TEMTBFBD	
MEAN TIME BETWEEN MAINTENANCE ACTIONS (MTBMA) OPERATIONAL		230	OMTBMABD	
MEAN TIME BETWEEN MAINTENANCE ACTIONS TECHNICAL		230	TMTBMABD	
MEAN TIME BETWEEN MAINTENANCE INDUCED		231	INMTBMBD	
MEAN TIME BETWEEN MAINTENANCE INHERENT (MTBM INHERENT)		232	INHMTBBD	
MEAN TIME BETWEEN MAINTENANCE NO DEFECT		233	NOMTBMBD	
MEAN TIME BETWEEN PREVENTIVE MAINTENANCE		234	MTBMPVBD	
MEAN TIME BETWEEN REMOVALS (MTBR)		235	MTBRXXBD	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
TABLE BE: WAR/PEACE RELIABILITY, AVAILABILITY, AND MAINTAINABILITY INDICATOR CHARACTERISTICS				
RAM OPERATIONAL REQUIREMENT INDICATOR	K	275	OPRQINBE	
ADMINISTRATIVE AND LOGISTIC DELAY TIME		013	ALDTXXBE	
OPERATIONAL AVAILABILITY		273	OPAVAIBE	
STANDBY TIME		403	STABYTBE	
TABLE BF: FAILURE MODE AND RELIABILITY CENTERED MAINTENANCE ANALYSIS				
FAILURE MODE INDICATOR (FMI)	K	134	FAMOINBF	
ENGINEERING FAILURE MODE MEAN TIME BETWEEN FAILURE (MTBF)		097	EFMTBFBF	
FAILURE MODE CLASSIFICATION		132	FMCLASBF	
FAILURE MODE RATIO		136	FMRATOBF	
RELIABILITY CENTERED MAINTENANCE (RCM) LOGIC RESULTS (01 to 25)		344	-----	
RCM DISPOSITION (A to J)		084	-----	
TABLE BG: FAILURE MODE AND RELIABILITY CENTERED MAINTENANCE NARRATIVE				
FAILURE MODE & RCM NARRATIVE CODE	K	131	FMNCNABG	
FAILURE/DAMAGE MODE EFFECT END EFFECT		125		
FAILURE/DAMAGE MODE EFFECT LOCAL		126		
FAILURE/DAMAGE MODE EFFECT NEXT HIGHER		127		
FAILURE CAUSE		124		
FAILURE/DAMAGE MODE		128		
FAILURE MODE DETECTION METHOD		129		
FAILURE PREDICTABILITY		138		
FAILURE MODE REMARKS		137		
REDESIGN RECOMMENDATIONS		426		
RCM AGE EXPLORATION		343		
RCM REASONING		346		
RCM REDESIGN RECOMMENDATIONS		426		
TABLE BH: FAILURE MODE TASK				
TASK REQUIREMENT LCN	F	199	TLSACNBH	
TASK REQUIREMENT ALTERNATE LCN CODE	F	019	TALCNCBH	
TASK REQUIREMENT LCN TYPE	F	203	TLCNTYBH	
TASK CODE	F	427	TTASKCBH	
TASK TYPE		433	TATYPEBH	
MAINTENANCE INTERVAL		208	MAININBH	
TABLE BI: FAILURE MODE INDICATOR MISSION PHASE CODE CHARACTERISTICS				
SAFETY HAZARD SEVERITY CODE	M	362	FMSHSCBI	
FAILURE EFFECT PROBABILITY		130	FEPROBBI	
FAILURE MODE CRITICALITY NUMBER		133	FACRNUBI	
FAILURE PROBABILITY LEVEL		139	FPROBLBI	
OPERATING TIME		269	FMOPTIBI	
TABLE BJ: FAILURE MODE INDICATOR MISSION PHASE CODE CHARACTERISTICS NARRATIVE				
FMI MISSION PHASE CHARACTERISTICS NARRATIVE CODE	K	135	FMMPCNBJ	

Data Element	Key	DED	DE CODE	Required
COMPENSATING DESIGN PROVISIONS		049		
COMPENSATING OPERATOR ACTION PROVISIONS		050		
TABLE BK: RELIABILITY, AVAILABILITY, AND MAINTAINABILITY CRITICALITY				
RAM SAFETY HAZARD SEVERITY CODE	K	362	FMSHSCBK	
RAM ITEM CRITICALITY NUMBER		178	RICRITBK	
TABLE BL: MISSION PHASE OPERATIONAL MODE				
MISSION PHASE CODE	K	246	MISSPCBL	
MISSION PHASE/OPERATIONAL MODE		247	MPOPLDBL	
TASK ANALYSIS AND PERSONNEL AND SUPPORT REQUIREMENT				
TABLE CA: TASK REQUIREMENT				
END ITEM ACRONYM CODE	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
TASK CODE	K	427	TASKCDCA	
REFERENCED TASK CODE		427	REFTSKCA	
TASK AOR MEASUREMENT BASE		238	AORMSBCA	
TASK IDENTIFICATION	M	431	TASKIDCA	
TASK FREQUENCY	M	430	TSKFRQCA	
TASK CRITICALITY CODE		429	TSKCRCCA	
HARDNESS CRITICAL PROCEDURE (HCP) CODE		152	HRDCPCCA	
HAZARDOUS MAINTENANCE PROCEDURES CODE		155	HAZMPCCA	
PREVENTIVE MAINTENANCE CHECKS AND SERVICES (PMCS) INDICATOR CODE		296	PMCSIDCA	
MEASURED MEAN ELAPSE TIME		224	MSDMETCA	
PREDICTED MEAN ELAPSE TIME		224	PRDMETCA	
MEASURED MEAN MAN-HOURS		225	MSDMMHCA	
PREDICTED MEAN MAN-HOURS		225	PRDMMHCA	
MEANS OF DETECTION		237	-----	
FACILITY REQUIREMENT CODE		358	FTRNRQCA	
TRAINING EQUIPMENT REQUIREMENT CODE		358	TRNRQCCA	
TRAINING RECOMMENDATION TYPE		463	TRNRECCA	
TRAINING LOCATION RATIONALE		461	TRNLOCCA	
TRAINING RATIONALE		462	TRNRATCA	
TOOL/SUPPORT EQUIPMENT REQUIREMENT CODE		358	TSEREQCA	
TASK PERFORMANCE		287	-----	
TASK CONDITION		428	-----	
TABLE CB: SUBTASK REQUIREMENT				
SUBTASK NUMBER	K	407	SUBNUMCB	
REFERENCED SUBTASK NUMBER		407	RFDSUBCB	
SUBTASK MEAN MINUTE ELAPSED TIME		227	SBMMETCB	
SUBTASK WORK AREA CODE		514	SUBWACCB	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
TABLE CC: SEQUENTIAL SUBTASK DESCRIPTION				
SEQUENTIAL SUBTASK DESCRIPTION		372	SUBNARCC	
ELEMENT INDICATOR		095	ELEMNTCC	
TABLE CD: SUBTASK PERSONNEL REQUIREMENT				
SUBTASK PERSON IDENTIFIER	K	288	SUBPIDCD	
SKILL SPECIALTY CODE		387	SKSPCDGA	
NEW OR MODIFIED SKILL SPECIALTY CODE		257	MDCSSCGB	
SUBTASK MEAN MAN-MINUTES		226	SUBMMMCD	
SKILL SPECIALTY EVALUATION CODE		388	SSECDECD	
TABLE CE: TASK REMARK				
TASK REMARK REFERENCE CODE	K	349	TSKRRCCE	
TASK REMARKS		432	TSKREMCE	
TABLE CF: TASK REMARK REFERENCE				
SELECT TABLE CF				
TABLE CG: TASK SUPPORT EQUIPMENT				
TASK SUPPORT CAGE CODE	F	046	TSCAGECG	
TASK SUPPORT REFERENCE NUMBER	F	337	TSREFNCG	
SUPPORT ITEM QUANTITY PER TASK		319	SQTYTKCG	
TABLE CH: TASK MANUAL				
TECHNICAL MANUAL (TM) CODE	F	437	TMCODEXI	
TABLE CI: TASK PROVISIONED ITEM				
TASK PROVISION CAGE CODE	F	046	PROCAGCI	
TASK PROVISION REFERENCE NUMBER	F	337	PROREFCI	
TASK PROVISION LCN	F	199	PROLCNCI	
TASK PROVISION ALC	F	019	PROALCCI	
TASK PROVISION LCN TYPE	F	203	PROLTYCI	
PROVISION QUANTITY PER TASK		319	PQTYTKCI	
TABLE CJ: JOB AND DUTY ASSIGNMENTS				
JOB CODE	K	186	JOBCODCJ	
DUTY CODE	K	091	DUTYCDCJ	
JOB		185	JOBDESCJ	
DUTY		090	DUTIESCJ	
TABLE CK: TASK INVENTORY				
SELECT TABLE CK				
SUPPORT EQUIPMENT AND TRAINING MATERIEL REQUIREMENTS				
TABLE EA: SUPPORT EQUIPMENT				
SUPPORT EQUIPMENT (SE) CAGE CODE	F	046	SECAGEEA	
SE REFERENCE NUMBER	F	337	SEREFNEA	
SE FULL ITEM NAME		412	FLITNMEA	
SE ITEM CATEGORY CODE		177	SEICCDEA	
ACQUISITION DECISION OFFICE	G	002	AQDCOFEA	
END ARTICLE ITEM DESIGNATOR		179	ENDARTEA	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
ADAPTOR/INTERCONNECTION DEVICE REQUIRED		005	AIDRQDEA	
DATE OF FIRST ARTICLE DELIVERY		071	DATFADEA	
CALIBRATION INTERVAL		037	CALINTEA	
CALIBRATION ITEM		038	CALITMEA	
CALIBRATION REQUIRED		040	CALRQDEA	
CALIBRATION STANDARD		041	CALSTDEA	
CALIBRATION TIME		042	CALTIMEA	
CALIBRATION MEASUREMENT REQUIREMENT SUMMARY RECOMMENDED		035	CMRSRCEA	
SE CONTRACT NUMBER		055	CNTRNOEA	
CFE / GFE		056	CFEGFEEA	
CUSTODY CODE		069	CUSTCDEA	
DRAWING CLASSIFICATION		088	DRWCLSEA	
ECONOMIC ANALYSIS		093	ECOANLEA	
FAMILY GROUP		142	FAMGRPEA	
GENERIC CODE		148	GENECDEA	
GOVERNMENT DESIGNATOR		149	GOVDESEA	
HARDWARE DEVELOPMENT PRICE		153	HDWRPREA	
INTEGRATED LOGISTIC SUPPORT PRICE		170	ILSPRCEA	
DESIGN DATA PRICE		080	DSNPRCEA	
EXTENDED UNIT PRICE		103	EXUNPREA	
PASS THROUGH PRICE		285	PASTHREA	
OPERATING AND SUPPORT COST		267	OSCOSTEA	
RECURRING COST		332	RCURCSEA	
LIFE CYCLE STATUS		190	LICYSTEA	
LIFE SPAN		191	LIFSPNEA	
LOGISTIC CONTROL CODE		197	LGCTCDEA	
LOGISTICS DECISION OFFICE	G	198	LGDCOFEA	
LSA RECOMMENDATION CODE		204	LSARCDEA	
MANAGEMENT PLAN	G	216	MGTPLNEA	
MANAGING COMMAND/AGENCY		217	MGCOATEA	
SUPPORT EQUIPMENT MEAN TIME BETWEEN FAILURES		229	SEMTBFEA	
SUPPORT EQUIPMENT MEAN TIME BETWEEN MAINTENANCE ACTIONS		230	SMTBMAEA	
SUPPORT EQUIPMENT MEAN TIME TO REPAIR		236	SEMTTREA	
MOBILE FACILITY CODE		248	MOBFACEA	
MODIFICATION OR CHANGE		252	MODCHGEA	
OPERATING DIMENSIONS		268	-----	
OPERATING WEIGHT		270	OPRWGTEA	
PRINTED CIRCUIT BOARD REPAIR OPERATIONS/MAINTENANCE LEVEL		277	PCBLVLEA	
SE CALIBRATION OPERATIONS/MAINTENANCE LEVEL		277	CALLVLEA	
SE REPAIR OPERATIONS/MAINTENANCE LEVEL		277	RPRLVLEA	
SE SOURCE, MAINTENANCE AND RECOVERABILITY CODE	G	389	SMRCSEEA	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
TECHNICAL MANUAL REQUIRED CODE		441	TMRQCDEA	
OPERATORS MANUAL		278	OPRMANEA	
SKILL SPECIALTY CODE (SSC) FOR SE OPERATOR (SEO)		387	SSCOPREA	
PREPARING ACTIVITY		294	PREATYEA	
PROGRAM ELEMENT	G	301	PROELEEA	
PROGRAM SUPPORT INVENTORY CONTROL POINT	G	303	PSICPOEA	
REPORTABLE ITEM CONTROL CODE		356	SERICCEA	
REVOLVING ASSETS	G	361	REVASSEA	
SELF TEST CODE		370	SLFTSTEA	
SENSORS OR TRANSDUCERS		371	SENTRAEA	
SE SERVICE DESIGNATOR		376	SERDESEA	
USING SERVICE DESIGNATOR CODE		376	USESEREA	
SKETCH		383	SKETCHEA	
SPARE FACTOR	G	390	SPRFACEA	
SPECIAL MANAGEMENT CODE	G	393	SPMGNTEA	
STANDARD INTERSERVICE AGENCY SERIAL CONTROL NUMBER	G	401	SIASCNEA	
STORAGE DIMENSIONS		405	-----	
STORAGE WEIGHT		406	STOWGTEA	
SUPPORT EQUIPMENT SHIPPING DIMENSIONS	G	419	-----	
SUPPORT EQUIPMENT SHIPPING WEIGHT	G	420	SESHWTEA	
SUPPORT EQUIPMENT GROUPING		413	SEGRCDEA	
SUPPORT EQUIPMENT REQUIRED		418	SEREQDEA	
TECHNICAL EVALUATION PRIORITY CODE		435	TECEVLEA	
TEST LANGUAGE		443	TSTLNGEA	
TEST POINTS		446	TSTPTSEA	
TMDE REGISTER CODE		444	TMDERCEA	
TMDE REGISTER INDEX		445	TMDERIEA	
TYPE CLASSIFICATION		479	TYPCLSEA	
TYPE EQUIPMENT CODE	G	480	TYPEEQEA	
YEAR OF FIELDING		518	YRFLDGEA	
TABLE EB: ALLOCATION DATA				
ALLOWANCE DOCUMENT NUMBER	B	016	ALDCNMEB	
ALLOWABLE RANGE 1-10 AND EXTENDED RANGE	G	015	-----	
ALLOCATION DESIGNATION DESCRIPTION	G	015	ALDNDSEB	
ALLOCATION LAND VESSEL CODE	G	015	ALLVCDEB	
ALLOCATION MAINTENANCE LEVEL FUNCTION	G	015	ALMLVLEB	
ALLOCATION STATION IDENTIFICATION CODE	G	015	ALSTIDEB	
TABLE EC: SUPPORT EQUIPMENT PARAMETERS				
CALIBRATION PROCEDURE	K	039	CALPROEC	
SUPPORT EQUIPMENT PARAMETERS		284	-----	
TABLE ED: SUPPORT EQUIPMENT AUTHORIZATION				
SPECIFIC AUTHORIZATION	B	399	-----	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
TABLE EE: SUPPORT EQUIPMENT NARRATIVE				
SUPPORT EQUIPMENT NARRATIVE CODE	K	414	SENARCEE	
FUNCTIONAL ANALYSIS		147		
DESCRIPTION AND FUNCTION OF SE		078		
SUPPORT EQUIPMENT NON-PROLIFERATION EFFORT		415		
CHARACTERISTICS OF SE		44		
INSTALLATION FACTORS OR OTHER FACILITIES		169		
ADDITIONAL SKILLS AND SPECIAL TRAINING REQUIREMENTS		008		
SUPPORT EQUIPMENT EXPLANATION		411		
JUSTIFICATION		188		
TABLE EF: SUPPORT EQUIPMENT RECOMMENDATION DATA				
SE RECOMMENDATION DATA (SERD) NUMBER	K	416	SERDNOEF	
SERD REVISION	K	360	SRDREVEF	
SERD STATUS		404	STATUSEF	
SERD DATE OF INITIAL SUBMISSION		071	INTSUBEF	
SERD DATE OF GOVERNMENT DISPOSITION	G	071	DTGVDSEF	
SERD DATE OF REVISION SUBMISSION		071	DTRVSBEF	
TABLE EG: SUPPORT EQUIPMENT RECOMMENDATION DATA REVISION REMARKS				
SERD REVISION REMARKS		417	REVREMEG	
TABLE EH: ALTERNATE NATIONAL STOCK NUMBER				
ALTERNATE NATIONAL STOCK NUMBER	K	253	-----	
TABLE EI: INPUT POWER SOURCE				
INPUT POWER SOURCE	K	168	-----	
TABLE EJ: SUPPORT EQUIPMENT DESIGN DATA				
DESIGN DATA CATEGORY CODE (DDCC)	K	079	DSNDATEJ	
DDCC CONTRACTOR RECOMMENDED		057	CNTRECEJ	
DDCC ESTIMATED PRICE		101	ESTPRCEJ	
DDCC GOVERNMENT REQUIRED		150	GOVRQDEJ	
DDCC SCOPE		365	DDCCSCEJ	
TABLE EK: SUPERCEDURE DATA				
SE SUPERCEDURE CAGE CODE	F	046	SPRCAGEK	
SE SUPERCEDURE REFERENCE NUMBER	F	337	SPRREFEK	
SE SUPERCEDURE TYPE	M	408	SUTYPEEK	
SE SUPERCEDURE ITEM NAME		182	SUPITNEK	
SE SUPERCEDURE SERD NUMBER		416	SUSRNOEK	
REASON FOR SUPERCEDURE/DELETION		327	REASUPEK	
SUPERCEDURE INTERCHANGEABILITY CODE		172	ICCODEEK	
TABLE EL: SUPPORT EQUIPMENT INTEGRATED LOGISTIC SUPPORT REQUIREMENT CATEGORY CODE				
INTEGRATED LOGISTIC SUPPORT REQUIREMENTS CATEGORY CODE (IRCC)	K	171	IRCCODEL	
IRCC CONTRACTOR RECOMMENDED		057	CONRECEL	
IRCC ESTIMATED PRICE		101	ESTPRCEL	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
IRCC GOVERNMENT REQUIRED		150	GOVRQDEL	
IRCC SCOPE		365	IRCSCOEL	
TABLE EM: SYSTEM EQUIPMENT				
SYSTEM CAGE CODE	F	046	SCAGECEM	
SYSTEM REFERENCE NUMBER	F	337	SREFNOEM	
SYSTEM EQUIPMENT QUANTITY PER TEST		320	QTYTSTEM	
SYSTEM EQUIPMENT ITEM DESIGNATOR		179	GFAEIDEM	
UNIT UNDER TEST REQUIREMENTS AND DESCRIPTION				
TABLE UA: ARTICLE REQUIRING SUPPORT/UNIT UNDER TEST				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
UUTLSA CONTROL NUMBER (LCN)	F	199	UUTLCNUA	
UUT ALTERNATE LCN CODE	F	019	UUTALCUA	
UUT LCN TYPE	F	203	UTLCNTUA	
UUT ALLOWANCE		016	UTALLOUA	
UUT MAINTENANCE PLAN NUMBER	G	209	UMNTPLUA	
UUT TEST REQUIREMENTS DOCUMENT NUMBER		448	UTTRDNUA	
UUT WORK PACKAGE REFERENCE		515	UTWPRFUA	
TABLE UB: UNIT UNDER TEST SUPPORT EQUIPMENT				
SUPPORT EQUIPMENT (SE) CAGE CODE	F	046	SECAGEEA	
SE REFERENCE NUMBER	F	337	SEREFNEA	
UUT CALIBRATION/MEASUREMENT REQUIREMENT SUMMARY (CMRS) STATUS		036	UTSTCDUB	
UUT CMRS RECOMMENDED CODE		035	UTCMRSUB	
TABLE UC: OPERATIONAL TEST PROGRAM				
OPERATIONAL TEST PROGRAM (OTP) CAGE CODE	F	046	OTPCAGUC	
OTP REFERENCE NUMBER	F	337	OTPREFUC	
OTP APPORTIONED UNIT COST		025	-----	
OTP COORDINATED TEST PLAN		060	OTPCTPUC	
OTP STANDARDS FOR COMPARISON		402	OTPSFCUC	
OTP SUPPORT EQUIPMENT RECOMMENDATION DATA NUMBER		416	OTPSRDUC	
TABLE UD: UNIT UNDER TEST SUPPORT EQUIPMENT OPERATIONAL TEST PROGRAM				
SELECT TABLE UD				
TABLE UE: TEST PROGRAM INSTRUCTION				
TEST PROGRAM INSTRUCTION (TPI) CAGE CODE	F	046	TPICAGUE	
TPI REFERENCE NUMBER	F	337	TPIREFUE	
TPI APPORTIONED UNIT COST		025	-----	
TPI SELF TEST		370	TPISTSUE	
TPI TECHNICAL DATA PACKAGE		434	TPITDPUE	
TPI SUPPORT EQUIPMENT RECOMMENDATION DATA NUMBER		416	TPISRDUE	
TABLE UF: UNIT UNDER TEST EXPLANATION				
UUT EXPLANATION		498	UTEXPLUF	
TABLE UG: UNIT UNDER TEST PARAMETER GROUP				
UUT CMRS PARAMETER CODE	K	034	UUTPPCUG	

Data Element	Key	DED	DE CODE	Required
UUT PARAMETERS		284	-----	
UUT PARAMETER TEST ACCURACY RATIO		442	-----	
TABLE UH: UNIT UNDER TEST FAULT ISOLATED REPLACEABLE UNIT				
TASKLSA CONTROL NUMBER (LCN)	F	199	TSKLCNCI	
TASK ALTERNATE LCN CODE (ALC)	F	019	TSKALCCI	
TASK LCN TYPE	F	203	TSKLTYCI	
TASK PROVISION TASK CODE	F	427	TSKTCDCI	
TASK PROVISION LCN	F	199	PROLCNCI	
TASK PROVISION ALC	F	019	PROALCCI	
TASK PROVISION LCN TYPE	F	203	PROLTYCI	
TASK PROVISION CAGE CODE	F	046	PROCAGCI	
TASK PROVISION REFERENCE NUMBER	F	337	PROREFCI	
SUPPORT EQUIPMENT (SE) CAGE CODE	M	046	SECAGEEA	
SE REFERENCE NUMBER	M	337	SEREFNEA	
UUT FIRU FAULT ISOLATION		143	-----	
UUT FIRU TEST REQUIREMENTS DOCUMENT INDICATOR		447	UUTFTDUH	
TABLE UI: ADAPTOR INTERCONNECTOR DEVICE				
ADAPTOR INTERCONNECTOR DEVICE (AID) CAGE CODE	F	046	AIDCAGUI	
AID REFERENCE NUMBER	F	337	AIDREFUI	
AID APPORTIONED UNIT COST		025	-----	
AID SERD NUMBER		416	AIDSRDUI	
AID COMMON UNIT UNDER TEST		048	AIDCUTUI	
TABLE UJ: UNIT UNDER TEST SUPPORT EQUIPMENT ADAPTOR INTERCONNECTOR DEVICE				
SELECT TABLE UJ				
TABLE UK: AUTOMATIC TEST EQUIPMENT TEST STATION				
AUTOMATIC TEST EQUIPMENT (ATE) CAGE CODE	F	046	ATECAGUK	
ATE REFERENCE NUMBER	F	337	ATEREFUK	
ATE GOVERNMENT DESIGNATOR		149	ATEGDSUK	
TABLE UL: UNIT UNDER TEST SUPPORT EQUIPMENT AUTOMATIC TEST EQUIPMENT				
SELECT TABLE UL				
TABLE UM: SUPPORT EQUIPMENT ITEM UNIT UNDER TEST				
SE UNIT UNDER TEST (SE UUT) CAGE CODE	F	046	SUTCAGUM	
SE UUT REFERENCE NUMBER	F	337	SUTREFUM	
SE UUT ALLOWANCE		016	SUTALLUM	
SE UUT CMRS STATUS		036	SUTSTCUM	
SE UUT MAINTENANCE PLAN NUMBER		209	MNTPLNUM	
SE UUT TEST REQUIREMENTS DOCUMENT NUMBER		448	TRDNUMUM	
SE UUT WORK PACKAGE REFERENCE		515	WKPKRFUM	
TABLE UN: SUPPORT EQUIPMENT UNIT UNDER TEST PARAMETER GROUP				
SE UUT PARAMETERS	K	284	-----	
SE UUT CMRS PARAMETER CODE		034	UTPACMUN	
SE UUT PARAMETER TEST ACCURACY RATIO		442	-----	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
FACILITIES CONSIDERATIONS				
TABLE FA: FACILITY				
FACILITY NAME	K	118	FACNAMFA	
FACILITY CATEGORY CODE	K	115	FACCCDFA	
FACILITY TYPE	K	483	FACTYPFA	
FACILITY CLASS		116	FACCLAFA	
FACILITY DRAWING CLASSIFICATION		088	DRCLASFA	
FACILITY DRAWING NUMBER		089	FADNUMFA	
FACILITY DRAWING REVISION		360	FADREVFA	
FACILITY AREA		112	FAAREAFA	
FACILITY AREA UNIT OF MEASURE		491	FAARUMFA	
FACILITY CONSTRUCTION UNIT OF MEASURE PRICE		492	FACNCOFA	
CONSTRUCTION UNIT OF MEASURE		491	CONUOMFA	
TABLE FB: FACILITY NARRATIVE				
FACILITY NARRATIVE CODE	K	119	FNCODEFB	
FACILITY CAPABILITY		114		
FACILITY LOCATION		117		
TABLE FC: BASELINE FACILITY NARRATIVE				
BASELINE FACILITY NARRATIVE CODE	K	113	FBNACDFC	
FACILITIES MAINTENANCE REQUIREMENTS		107		
FACILITIES REQUIREMENTS FOR OPERATIONS		109		
FACILITIES REQUIREMENT FOR TRAINING		110		
FACILITY REQUIREMENTS SPECIAL CONSIDERATIONS		120		
FACILITY REQUIREMENTS SUPPLY/STORAGE		121		
TABLE FD: NEW OR MODIFIED FACILITY NARRATIVE				
NEW OR MODIFIED FACILITY NARRATIVE CODE	K	255	NMFNCDFD	
FACILITY DESIGN CRITERIA		105		
FACILITY INSTALLATION LEAD TIME		106		
FACILITY TASK AREA BREAKDOWN		122		
FACILITIES UTILIZATION		111		
FACILITIES REQUIREMENTS		108		
FACILITY UNIT COST RATIONALE		123		
FACILITY JUSTIFICATION		188		
TYPE OF CONSTRUCTION		482		
UTILITIES REQUIREMENT		502		
TABLE FE: OPERATIONS AND MAINTENANCE TASK FACILITY REQUIREMENT				
END ITEM ACRONYM CODE	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
TASK CODE	F	427	TASKCDCA	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
PERSONNEL SKILL CONSIDERATIONS				
TABLE GA: SKILL SPECIALTY				
SKILL SPECIALTY CODE	K	387	SKSPCDGA	
SKILL LEVEL CODE		386	SKLVCDGA	
HOUR LABOUR RATE		161	HRLARTGA	
TRAINING COST		460	TRNCOSGA	
TABLE GB: NEW OR MODIFIED SKILL				
NEW OR MODIFIED SKILL SPECIALTY CODE	K	257	MDCSSCGB	
NEW OR MODIFIED SKILL LEVEL CODE		386	MDSCLCGB	
SKILL SPECIALTY CODE		387	SKSPCDGA	
DUTY POSITION REQUIRING A NEW OR REVISED SKILL		092	DPRNRSGB	
RECOMMENDED RANK/RATE/PAY PLAN/GRADE		330	-----	
SECURITY CLEARANCE REQUIRED		369	SCRSSCGB	
TEST SCORE		449	SSCTESGB	
ARMED SERVICES VOCATIONAL APTITUDE BATTERY (ASVAB) ARMED FORCES		026	ABAFQTGB	
QUALIFICATION TEST (AFQT) SCORE				
ASVAB AFQT EXPECTED RANGE		026	-----	
ASVAB AFQT LOWEST PERCENTAGE		026	-----	
TABLE GC: NEW OR MODIFIED SKILL NARRATIVE				
NEW OR MODIFIED SKILL NARRATIVE CODE	K	256	NMSNCDGC	
NEW OR MODIFIED SKILL ADDITIONAL REQUIREMENTS		007		
EDUCATIONAL QUALIFICATIONS		094		
SKILL JUSTIFICATION		188		
ADDITIONAL TRAINING REQUIREMENTS		012		
TABLE GD: SKILL APTITUDE DATA				
ASVAB APTITUDE ELEMENT	K	026	ASVAPEGD	
ASVAB APTITUDE ELEMENT EXPECTED RANGE		026	-----	
ASVAB APTITUDE ELEMENT LOWEST PERCENTAGE		026	-----	
TABLE GE: PHYSICAL AND MENTAL REQUIREMENTS NARRATIVE				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
TASK CODE	F	427	TASKCDCA	
SUBTASK NUMBER	F	407	SUBNUMCB	
SUBTASK PERSON IDENTIFIER	F	288	SUBPIDCD	
PHYSICAL AND MENTAL REQUIREMENTS NARRATIVE		290	PAMENRGE	
PACKAGING AND PROVISIONING REQUIREMENTS				
TABLE HA: ITEM IDENTIFICATION				
COMMERCIAL AND GOVERNMENT ENTITY (CAGE) CODE	F	046	CAGECDXH	
REFERENCE NUMBER	K	337	REFNUMHA	
ITEM NAME		182	ITNAMEHA	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
ITEM NAME CODE		183	INAMECHA	
REFERENCE NUMBER CATEGORY CODE		338	REFNCCHA	
REFERENCE NUMBER VARIATION CODE		339	REFNVCHA	
DLSC SCREENING REQUIREMENT CODE		073	DLSCRCHA	
DOCUMENT IDENTIFIER CODE		087	DOCIDCHA	
ITEM MANAGEMENT CODE		181	ITMMGCHA	
NSN PREFIX		253	-----	
NATIONAL STOCK NUMBER (NSN)		253	-----	
NSN SUFFIX		253	-----	
UNIT OF ISSUE CONVERSION FACTOR (UI CONVERSION FACTOR)		489	UICONVHA	
SHELF LIFE (SL)		377	SHLIFEHA	
SHELF LIFE ACTION CODE (SLAC)		378	SLACTNHA	
PROGRAM PARTS SELECTION LIST		302	PPSLSTHA	
DOCUMENT AVAILABILITY CODE		086	DOCAVCHA	
PRODUCTION LEAD TIME		299	PRDLDTHA	
SPECIAL MATERIAL CONTENTS CODE (SMCC)		395	SPMACCHA	
SPECIAL MAINTENANCE ITEM CODE (SMIC)		392	SMAINCHA	
CRITICALITY CODE		066	CRITCDHA	
PRECIOUS METAL INDICATOR CODE		293	PMICODHA	
SPARES ACQUISITION INTEGRATED WITH PRODUCTION (SAIP)		391	SAIPCDHA	
PROVISIONING LIST CATEGORY CODE		308	-----	
PHYSICAL SECURITY PILFERAGE CODE		291	PHYSECHA	
ADP EQUIPMENT CODE		027	ADPEQPHA	
DEMILITARIZATION CODE		076	DEMILIHA	
ACQUISITION METHOD CODE	G	003	ACQMETHA	
ACQUISITION METHOD SUFFIX CODE	G	004	AMSUFCHA	
HAZARDOUS MATERIALS STORAGE COST		156	HMSCOSHA	
HAZARDOUS WASTE DISPOSAL COST		157	HWDCOSHA	
HAZARDOUS WASTE STORAGE COST		158	HWSCOSHA	
CONTRACTOR TECHNICAL INFORMATION CODE		058	CTICODHA	
UNIT WEIGHT		497	UWEIGHHA	
UNIT SIZE		496	-----	
HAZARDOUS CODE		154	HAZCODHA	
UNIT OF MEASURE		491	UNITMSHA	
UNIT OF ISSUE (UI)		488	UNITISHA	
LINE ITEM NUMBER		193	LINNUMHA	
CRITICAL ITEM CODE		065	CRITITHA	
INDUSTRIAL MATERIALS ANALYSIS OF CAPACITY		163	INDMATHA	
MATERIAL LEADTIME		219	MTLEADHA	
MATERIAL WEIGHT		220	MTLWGTHA	
MATERIAL		218	MATERLHA	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
TABLE HB: ADDITIONAL REFERENCE NUMBER				
ARN CAGE CODE	F	46	ADCAGEHB	
ADDITIONAL REFERENCE NUMBER	K	006	ADDREFHB	
ARN REFERENCE NUMBER CATEGORY CODE		338	ADRNCCHB	
ARN REFERENCE NUMBER VARIATION CODE		339	ADRNVCHB	
TABLE HC: CONTRACTOR TECHNICAL INFORMATION CODE (CTIC) CAGE				
CTIC CAGE CODE	F	046	CTCAGEHC	
TABLE HD: ITEM UNIT OF ISSUE PRICE				
UNIT OF ISSUE PRICE (UI PRICE)	K	490	UIPRICHD	
UI PRICE LOT QUANTITY		205	-----	
UI PRICE CONCURRENT PRODUCTION CODE		051	CURPRCHD	
UI PRICE TYPE OF PRICE CODE		485	TUIPRCHD	
UI PRICE PROVISIONING		314	PROUIPHD	
UI PRICE FISCAL YEAR		145	FISCYRHD	
TABLE HE: ITEM UNIT OF MEASURE PRICE				
UNIT OF MEASURE (UM) PRICE	K	492	UMPRICHE	
UM PRICE LOT QUANTITY		205	-----	
UM PRICE CONCURRENT PRODUCTION CODE		051	CURPRCHE	
UM PRICE TYPE OF PRICE CODE		485	TUMPRCHE	
UM PRICE PROVISIONING		314	PROUMPHE	
UM PRICE FISCAL YEAR		145	FISCYRHE	
TABLE HF: ITEM PACKAGING REQUIREMENT				
COMMERCIAL AND GOVERNMENT ENTITY (CAGE) CODE	F	046	CAGECDXH	
REFERENCE NUMBER	F	337	REFNUMHA	
DEGREE OF PROTECTION CODE	K	074	DEGPROHF	
UNIT CONTAINER CODE		486	UNICONHF	
UNIT CONTAINER LEVEL		487	UCLEVLHF	
PACKING CODE		283	PKGCODHF	
PACKAGING CATEGORY CODE		282	PACCATHF	
METHOD OF PRESERVATION CODE		239	MEPRESHF	
CLEANING AND DRYING PROCEDURES		045	CDPROCHF	
PRESERVATION MATERIAL CODE		295	PRSMATHF	
WRAPPING MATERIAL		517	WRAPMTHF	
CUSHIONING AND DUNNAGE MATERIAL		067	CUSHMAHF	
CUSHIONING THICKNESS		068	CUSTHIHF	
QUANTITY PER UNIT PACK		321	QTYUPKHF	
INTERMEDIATE CONTAINER CODE		174	INTCONHF	
INTERMEDIATE CONTAINER QUANTITY		175	INCQTYHF	
SPECIAL MARKING CODE		394	SPEMRKHF	
UNIT PACK WEIGHT		495	UNPKWTHF	
UNIT PACK SIZE		494	-----	
UNIT PACK CUBE		493	UNPKCUHF	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
OPTIONAL PROCEDURES INDICATOR		279	OPTPRIHF	
SPECIAL PACKAGING INSTRUCTIONS (SPI) NUMBER		396	SPINUMHF	
SPI NUMBER REVISION		397	SPIREVHF	
SPI NUMBER JULIAN DATE		187	SPDATEHF	
CONTAINER NSN		253	CONNSNHF	
SUPPLEMENTAL PACKAGING DATA		409	SUPPKDHF	
PACKAGING DATA PREPARER CAGE		046	PKCAGEHF	
TABLE HG: PART APPLICATION PROVISIONING				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
PROVISIONING LIST ITEM SEQUENCE NUMBER (PLISN)		309	PLISNOHG	
QUANTITY PER ASSEMBLY		316	QTYASYHG	
OPTION 1				
OPTION 2	N			
OPTION 3				
SUPPRESSION INDICATOR		422	SUPINDHG	
DATA STATUS CODE		070	DATASCHG	
PROVISIONING SYSTEM IDENTIFIER CODE	C	312	PROSICHG	
PTD SELECTION CODE		313	-----	
TYPE OF CHANGE CODE (TOCC)		481	TOCCODHG	
INDENTURE CODE		162	INDCODHG	
ATTACHING PART/HARDWARE				
OPTION 1				
OPTION 2				
OPTION 3				
OPTION 4				
OPTION 5				
INDENTURE FOR KITS				
OPTION 1				
OPTION 2				
OPTION 3				
QUANTITY PER END ITEM		317	QTYPEIHG	
OPTION 1				
OPTION 2	N			
OPTION 3	C			
PRIOR ITEM PLISN		297	PIPLISHG	
SAME AS PLISN		364	SAPLISHG	
HARDNESS CRITICAL ITEM		151	HARDCIHG	
REMAIN IN PLACE INDICATOR		348	REMIPIHG	
LINE REPLACEABLE UNIT (LRU)		194	LRUNITHG	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
ITEM CATEGORY CODE (ICC)		177	ITMCATHG	
ESSENTIALITY CODE		100	ESSCODHG	
SOURCE, MAINTENANCE AND RECOVERABILITY CODE		389	SMRCODHG	
MAINTENANCE REPLACEMENT RATE I (MRRI)		211	MRRONEHG	
MAINTENANCE REPLACEMENT RATE II (MRRII)		212	MRRTWOHG	
OPTION 1				
OPTION 2				
MAINTENANCE REPLACEMENT RATE MODIFIER	A	213	MRRMODHG	
REPLACEMENT TASK DISTRIBUTION		355	-----	
MINIMUM REPLACEMENT UNIT		245	MINREUHG	
MAXIMUM ALLOWABLE OPERATING TIME (MAOT)		221	MAOTIMHG	
MAINTENANCE ACTION CODE (MAC)		206	MAIACTHG	
RECOMMENDED INITIAL SYSTEM STOCK BUY		328	RISSBUHG	
RECOMMENDED MINIMUM SYSTEM STOCK LEVEL		329	RMSSLIHG	
RECOMMENDED TENDER LOAD LIST QUANTITY	N	331	RTLLQTHG	
TOTAL QUANTITY RECOMMENDED		453	TOTQTYHG	
MAINTENANCE TASK DISTRIBUTION		214	-----	
REPAIR CYCLE TIME		350	-----	
OPTION 1				
OPTION 2				
NOT REPAIRABLE THIS STATION	R	261	NORETSHG	
REPAIR SURVIVAL RATE (RSR)		351	REPSURHG	
DESIGNATED REWORK POINT		081	-----	
WORK UNIT CODE		516	WRKUCDHG	
ALLOWANCE ITEM CODE		017	ALLOWCHG	
ALLOWANCE ITEM QUANTITY		018	ALIQTYHG	
TABLE HH: OVERHAUL-KIT NEXT HIGHER ASSEMBLY PLISN				
NEXT HIGHER ASSEMBLY (NHA) PROVISIONING LIST ITEM SEQUENCE NUMBER	K	258	NHAPLIHH	
(PLISN)				
NHA PLISN INDICATOR		259	NHAINDHH	
OVERHAUL REPLACEMENT RATE		281	OVHREPHH	
TABLE HI: PROVISIONING REMARK				
PROVISIONING REMARKS		311	REMARKHI	
TABLE HJ: PROVISIONING REFERENCE DESIGNATION				
REFERENCE DESIGNATION	K	335	REFDESHJ	
OPTION 1				
OPTION 2				
OPTION 3				
OPTION 4				
OPTION 5				
REFERENCE DESIGNATION CODE		336	RDCODEHJ	
TECHNICAL MANUAL (TM) CODE		437	TMCODEXI	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
FIGURE NUMBER		144	FIGNUMHK	
ITEM NUMBER		184	ITEMNOHK	
TABLE HK: PARTS MANUAL DESCRIPTION				
TECHNICAL MANUAL (TM) CODE	F	437	TMCODEXI	
FIGURE NUMBER	K	144	FIGNUMHK	
ITEM NUMBER	K	184	ITEMNOHK	
TM FUNCTIONAL GROUP CODE (REPAIR PARTS MANUAL)		438	TMFGCDHK	
TECHNICAL MANUAL INDENTURE CODE		439	TMINDCHK	
QUANTITY PER FIGURE		318	QTYFIGHK	
TECHNICAL MANUAL CHANGE NUMBER		436	TMCHGNHK	
TABLE HL: PARTS MANUAL PROVISIONING NOMENCLATURE				
PROVISIONING NOMENCLATURE		310	PROVNOHL	
TABLE HM: ITEM BASIS OF ISSUE				
BASIS OF ISSUE	K	030	-----	
TABLE HN: PROVISIONING SERIAL NUMBER USABLE ON CODE				
S/N PROVISIONING SYSTEM/EI LCN	F	199	LCNSEIHN	
S/N PROVISIONING SYSTEM/EI ALC	F	019	ALCSEIHN	
S/N PROVISIONING SERIAL NUMBER	F	373	-----	
TABLE HO: PROVISIONING SYSTEM/END ITEM USABLE ON CODE				
UOC PROVISIONING SYSTEM/EI LCN	F	199	LCNSEIHO	
UOC PROVISIONING SYSTEM/EI ALC	F	019	ALCSEIHO	
TABLE HP: DESIGN CHANGE INFORMATION				
CHANGE AUTHORITY NUMBER	K	043	CANUMBHP	
REPLACED OR SUPERSEDING (R-S) PROVISIONING LIST ITEM SEQUENCE NUMBER (PLISN)		353	RSPLISHP	
R-S PLISN INDICATOR		354	RSPINDHP	
INTERCHANGEABILITY CODE		172	INTCHCHP	
TOTAL ITEM CHANGES		452	TOTICHHP	
OPTION 1				
OPTION 2				
QUANTITY SHIPPED		323	QTYSHPHP	
QUANTITY PROCURED		322	QTYPROHP	
PRORATED EXHIBIT LINE ITEM NUMBER (ELIN)		305	PROELIHP	
PRORATED QUANTITY		306	PROQTYHP	
TABLE HQ: SERIAL NUMBER EFFECTIVITY				
SERIAL NUMBER EFFECTIVITY	K	374	-----	
TABLE HR: DESIGN CHANGE USABLE ON CODE				
SELECT TABLE HR				
TRANSPORTABILITY ENGINEERING ANALYSIS				
TABLE JA: TRANSPORTATION				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
LCN TYPE	F	203	LCNTYPXB	
TRANSPORTATION INDICATOR		468	TRNINDJA	
SECTIONALIZED IDENTIFICATION		366	SECTIDJA	
ENVIRONMENTAL HANDLING AND TRANSPORTATION INDICATOR		098	ENHATCJA	
DELIVERY SCHEDULE		075	DELSCHJA	
TRANSPORTATION CONTRACT NUMBER		055	CONNUMJA	
PROPER SHIPPING NAME		304	PROPSNJA	
SPEED		400	SPSPEDJA	
TOWING SPEED		455	TWSPEDJA	
MILITARY UNIT TYPE		242	MILUNTJA	
REVISION DATE		071	TRCHRDJA	
THEATRE OF OPERATION		451	TRCHTHJA	
NONOPERABILITY FRAGILITY FACTOR		260	NOPRFFJA	
NET EXPLOSIVE WEIGHT		254	NETEXWJA	
TABLE JB: TRANSPORTATION SHIPPING MODES				
TRANSPORTATION CHARACTER NUMBER	K	465	TRANCNJB	
TRANSPORTATION CHARACTER MODE TYPE	K	464	TRCHMTJB	
TRANSPORTATION ITEM DESIGNATOR		469	TRITDRJB	
SHIPPING CONFIGURATION		380	SHPCONJB	
CONTAINER LENGTH		053	CONLENJB	
CONTAINER TYPE		054	CONTYPJB	
FREIGHT CLASSIFICATION		146	FRCLASJB	
EXTERNAL OR INTERNAL LOAD INDICATOR		104	EOILINJB	
HELICOPTER MISSION		159	-----	
HIGHWAY MODEL LOAD		250	-----	
HIGHWAY MODEL TYPE		251	-----	
RAIL USE		326	RAILUSJB	
RAIL TRANSPORTATION COUNTRY		325	RAILTCJB	
SEA DECK STOWAGE		072	SDECKSJB	
TABLE JC: TRANSPORTED END ITEM				
TRANSPORTED CONFIGURATION NUMBER	K	473	TRCONMJC	
MOBILITY TYPE	K	249	MOBTYPJC	
OPERATIONAL WEIGHT EMPTY/LOADED		276	-----	
MILITARY LOAD CLASSIFICATION EMPTY/LOADED		241	-----	
SHIPPING WEIGHT EMPTY/LOADED		381	-----	
CREST ANGLE		063	CREANGJC	
TRACKED GROUND PRESSURE		456	TRGRPRJC	
TRACKED ROAD WHEEL WEIGHT		459	TRRWWTJC	
TRACKED PADS TOUCHING		458	TRNUPTJC	
TRACKED PAD SHOE AREA		457	TRPSARJC	
WHEELED INFLATION PRESSURE		507	WHINPRJC	
WHEELED NUMBER OF PLIES		508	WHNUPLJC	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
WHEELED NUMBER TIRES		509	WHNUTIJC	
WHEELED TIRE LOAD RATINGS		510	WHTLDRJC	
WHEELED TIRE SIZE		512	WHTIFTJC	
WHEELED WEIGHT RATINGS		513	WHWERAJC	
AXLE LENGTH		029	-----	
SKID NUMBER OF SKIDS		264	SNUMSKJC	
SKID AREA		384	SDSICGJC	
TABLE JD: TRANSPORTED END ITEM NARRATIVE				
TRANSPORTED END ITEM NARRATIVE CODE	K	474	TREINCJD	
WHEELED TIRE REQUIREMENTS		511		
SKID REMARKS		385		
TURNING INFORMATION		477		
WHEELED AXLE AND SUSPENSION REMARKS		506		
TRANSPORTED OTHER EQUIPMENT		475		
TABLE JE: TRANSPORT BY FISCAL YEAR				
TRANSPORT FISCAL YEAR	K	145	TRAFYRJE	
FIRST QUARTER PROCUREMENT QUANTITY		298	FIQPQTJE	
SECOND QUARTER PROCUREMENT QUANTITY		298	SQPQTYJE	
THIRD QUARTER PROCUREMENT QUANTITY		298	TQPQTYJE	
FOURTH QUARTER PROCUREMENT QUANTITY		298	FQPQTYJE	
TABLE JF: TRANSPORTATION NARRATIVE				
TRANSPORTATION NARRATIVE CODE	K	470	TRANCDJF	
TRANSPORTATION SHOCK VIBRATION REMARKS		382		
LIFTING AND TIEDOWN REMARKS		192		
TRANSPORTATION PROJECTION REMARKS		471		
REGULATORY REQUIREMENTS		340		
TRANSPORTATION REMARKS		472		
SPECIALISED SERVICE AND EQUIPMENT		398		
SECTIONALIZED REMARKS		368		
TRANSPORTED TO AND FROM		476		
ENVIRONMENTAL/HAZARDOUS MATERIALS CONSIDERATIONS		099		
MILITARY DISTANCE CLASSIFICATION		240		
UNUSUAL AND SPECIAL REQUIREMENTS		500		
VENTING AND PROTECTIVE CLOTHING		504		
DISASTER RESPONSE FORCE REQUIREMENTS		082		
AUSTRALIAN DEFENCE ORGANISATION M TABLES				
TABLE MA: TASK ID EXTENDED MEMO				
NARRATIVE - TASK		944	NARRATMA	
TABLE MB: SKILL SPECIALITY CODE EXTENDED MEMO				
NARRATIVE - MAINTENANCE POLICY TRADE SKILL		945	NARRATMB	
TABLE MC: TASK INTERVAL EXTENDED MEMO				

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
NARRATIVE - TASK INTERVAL		946	NARRATMC	
TABLE MD: TASK FACILITY EXTENDED MEMO				
NARRATIVE - TASK FACILITY		947	NARRATMD	
TABLE ME: LCN ITEM EXTENDED MEMO				
NARRATIVE - LCN ITEM		948	NARRATME	
TABLE MF: SERVICING EXTENDED MEMO				
NARRATIVE - SERVICING		949	NARRATMF	
AUSTRALIAN DEFENCE ORGANISATION R TABLES				
TABLE RA: WORK AREA CODE LIBRARY				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
WORK AREA CODE	K	940	WACODERA	
WORK AREA CODE NAME		997	WACNAMRA	
WORK AREA CLASSIFICATION		812	INTEXTRA	
ENVIRONMENTAL DAMAGE RATING		814	ENVDAMRA	
ACCIDENTAL DAMAGE RATING		816	ACCDAMRA	
INSPECTABILITY RATING		815	INSPECRA	
OVERALL WORK AREA ASSESSMENT		817	WAASSMRA	
WORK AREA EQUIPMENT INSTALLED		818	EQINSTRA	
TABLE RB: WORK AREA CODE DESCRIPTION				
WAC DESCRIPTION TEXT SEQUENCING CODE	K	450	TEXSEQRB	
WORK AREA CODE DESCRIPTION		---	WACDESRB	
WORK AREA NARRATIVE CODE	K	819	WANCODRB	
TABLE RC: INITIATING TYPES LIBRARY				
INITIATING TYPE	K	915	INTTYPRC	
INITIATING TYPE DESCRIPTION		916	TYPDESRC	
TABLE RD: TASK INITIATING CONDITIONS ASSIGNMENTS				
INITIATING MODE	K	914	INTMODRD	
INITIATING CONDITION SEQUENCE NUMBER	K	912	ICSQNMRD	
INITIATING INSTANCE		913	ININSTRD	
INITIATING LCN		199	INTLCNRD	
INITIATING ALC		019	INTALCRD	
INITIATING LCN TYPE		203	INTLTYRD	
INITIATING INTERVAL		937	ININTVRD	
INITIATING EVENT MEASUREMENT BASE		923	INEVNTRD	
TABLE RE: SERVICING INITIATING CONDITIONS ASSIGNMENTS				
SERVICING INITIATING MODE	K	914	INTMODRE	
SERVICING INITIATING CONDITION SEQUENCE NUMBER	K	912	ICSQNMRE	
SERVICING INITIATING INSTANCE		913	ININSTRE	
SERVICING INITIATING LCN		199	INTLCNRE	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
SERVICING INITIATING ALC		019	INTALCRE	
SERVICING INITIATING LCN TYPE		203	INTLTYRE	
SERVICING INITIATING INTERVAL		937	ININTVRE	
SERVICING INITIATING EVENT MEASUREMENT BASE		923	INEVNTRE	
TABLE RF: SERVICING CLAIMED ACTIVITIES ASSIGNMENTS				
SELECT TABLE RF				
TABLE RG: TASK CLAIMED ACTIVITIES ASSIGNMENTS				
SELECT TABLE RG				
TABLE RI: REFERENCED FAILURE MODES				
SELECT TABLE RI				
TABLE RJ: LCN LOG REQUIREMENTS				
LOG REQUIREMENT	K	926	LCNLOGRJ	
TABLE RL: MAINTENANCE POLICY TASK CROSS REFERENCE				
SELECT TABLE RL				
TABLE RM: MAINTENANCE POLICY TRADES				
SELECT TABLE RM				
TABLE RN: SERVICING SUBTASKS				
SERVICING SUBTASK NUMBER	K	407	SUBNUMRN	
SERVICING SUBTASK IDENTIFICATION		431	SUBTIDRN	
SUBTASK CERTIFICATION REQUIREMENT		968	SCRTRQRN	
TABLE RO: SERVICING SUBTASK NARRATIVE				
SERVICING SUBTASK NARRATIVE		372	SUBNARRO	
ELEMENT INDICATOR		095	ELEMNTRO	
TABLE RP: SERVICING SUBTASK CROSS REFERENCE				
SELECT TABLE RP				
TABLE RQ: RCM LOGIC DISPOSITION CODE LIBRARY				
RCM LOGIC DISPOSITION CODE	K	807	RCMDISRQ	
DISPOSITION CODE DESCRIPTION		802	DSCDESRQ	
TABLE RR: LCN/ALC RCM LOGIC USED AND ANALYSIS STATUS				
RCM ANALYSIS STATUS		803	RCMSTSRR	
RCM ANALYSIS STATUS DATE/TIME		809	RCMDTERR	
TABLE RS: LCN/ALC RCM ANALYSIS RESULTS				
RCM LOGIC RESULT		804	RCMRSTRS	
TABLE RT: LCN/ALC RCM ANALYSIS JUSTIFICATION				
TEXT SEQUENCE NUMBER		450	TXTSEQRT	
RCM JUSTIFICATION NARRATIVE		805	RCMJSTRT	
TABLE RU: RCM LOGIC QUESTION DEFINITION				
TEXT SEQUENCE NUMBER	K	450	TXTSEQRU	
RCM QUESTION		806	RCMQSTRU	
TABLE RV: RCM LOGICS LIBRARY				
RCM LOGIC NAME	K	345	RCMLOGRV	
RCM LOGIC DESCRIPTION		800	RCMDESRV	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
TABLE RW: RCM LOGIC DEFINITION				
RCM QUESTION NUMBER	K	801	RCMQNMRW	
AFFIRMATIVE QUESTION NUMBER		802	AFQNUMRW	
AFFIRMATIVE DISPOSITION CODE		084	AFDISCRW	
AFFIRMATIVE FAILURE MODE CRITICALITY		962	AFCRITRW	
AFFIRMATIVE TASK REQUIREMENT		808	AFTSKRRW	
NEGATIVE QUESTION NUMBER		801	NGQNUMRW	
NEGATIVE DISPOSITION CODE		084	NGDISCRW	
NEGATIVE FAILURE MODE CRITICALITY		962	NGCRITRW	
NEGATIVE TASK REQUIREMENT		808	NGTSKRRW	
TABLE RX: SERVICING CLAIMED TASK ASSIGNMENTS				
SELECT TABLE RX				
TABLE RY: WORK AREA CODE ANALYSIS DEFINITION				
WORK AREA CONSIDERATION GROUP CODE	K	820	GRPCODRY	
WORK AREA CONSIDERATION SEQUENCE NUMBER	K	828	CONSEQRY	
WORK AREA CONSIDERATION	M	829	CONSIDRY	
AUSTRALIAN DEFENCE ORGANISATION V TABLES				
TABLE VA: LCN ADDITIONAL ADO PROVISIONING DATA				
AUTHORITY TO DEMAND NSN		941	AUTHTDVB	
PROVISIONING REFERENCE		942	PROVRFVA	
REQUIREMENTS AMPLIFICATION CODE		943	RQAMCDVA	
TABLE VB: AUTHORISED TO DEMAND NSN				
AUTHORITY TO DEMAND NSN	K	941	AUTHTDVB	
AUTHORISED TO DEMAND NSN PRICE		950	ATDPRIVB	
AUTHORISED TO DEMAND NSN EXISTING STOCK		952	ATDEXIVB	
AUTHORISED TO DEMAND NSN UNIT OF ISSUE		953	ATDUOIVB	
SERVICING LEVEL		954	SERLEVVB	
TABLE VC: AUTHORISED TO DEMAND NSN - FACILITY				
FACILITY CODE (ADF)		955	FACODEVC	
MAINTENANCE SUPPLY ITEM (MSI) UNIT ENTITLEMENT		956	MSIUENVC	
TABLE VD: ADDITIONAL PART INFORMATION				
HAZARDOUS GOODS UN NUMBER		957	HAZGUNVD	
PART PRIMARY LIFING PARAMETER		923	PLIFPAVD	
EXTENDED ITEM NAME		893	EXTINMVD	
TABLE VE: TASK FACILITY REQUIREMENT EXTENSION				
TASK COST OF REPAIR ESTIMATED		958	ESTCSTVE	
TASK COST OF REPAIR ACTUAL		959	ACTCSTVE	
FACILITY TASK TIME		961	TSKTIMVE	
TABLE VF: ADF FAILURE MODES				
FAILURE MODE CRITICALITY (ADF)		962	FMCRITVF	
FUNCTIONAL LSA CONTROL NUMBER		199	FLSACNXG	
FUNCTIONAL ALTERNATE LCN CODE		19	FALCNCXG	

ANNEX A TO DID-ILS-TDATA-LSAR

Data Element	Key	DED	DE CODE	Required
TABLE VG: ADO ENHANCED CRITICALITY CODES				
SELECT VG TABLE				
TABLE VR: SYSTEM/END ITEM ROLE CODE				
END ITEM ACRONYM CODE (EIAC)	F	96	EIACODXA	
ROLE CODE	K	965	ROLCODVR	
ROLE DESCRIPTION		967	ROLDESVR	
TABLE VS: ROLE CODE TO MISSION PHASE CROSS REFERENCE				
SELECT TABLE VS				
TABLE VT: ROLE TO LCN CROSS REFERENCE				
ROLE REQUIRED FIT		966	ROLREQVT	
AUSTRALIAN DEFENCE ORGANISATION W TABLES				
TABLE WA: EVENT MEASUREMENT BASE LIBRARY				
EVENT MANAGEMENT BASE	K	923	EVNTMBWA	
EVENT MEASUREMENT BASE DESCRIPTION		922	DESCRPWA	
TABLE WB: TASK/EVENT CROSS REFERENCE				
TASK INTERVAL		937	TSKINTWB	
TABLE WC: TASK REQUIREMENT EXTENSION				
CONTINGENCY REQUIREMENT		921	CONTINWC	
HISTORICAL TASK FREQUENCY		430	HTSKFQWC	
HISTORICAL TASK FREQUENCY NARRATIVE		964	TFQNARWC	
STANDARD ACTIVITY CODE		836	STNACTWC	
TABLE WD: MAINTENANCE TASK ENHANCED CRITICALITY CODES				
ENHANCED CRITICALITY CODE	K	834	ECCODEWD	
TABLE WE: ALTERNATE CAGE AND REFERENCE NUMBER BATCH INFORMATION				
BATCH NUMBER	K	917	-----	
BATCH IDENTIFICATION	M	918	BTCHIDWE	
TABLE WF: ALTERNATE CAGE AND REFERENCE NUMBER SET IDENTIFICATION				
ACRN SET SEQUENCE NUMBER	K	919	SEQNUMWF	
TABLE WG: TECHNICAL MANAGEMENT CODE LIBRARY				
TECHNICAL MANAGEMENT CODE	K	938	TMNTCDWG	
TECHNICAL MANAGEMENT CODE STATUS	M	939	TMCSTAWG	
MAXIMUM FIT		927	MAXFITWG	
TABLE WH: TECHNICAL MANAGEMENT CODE TO PHYSICAL LCN CROSS REFERENCE				
SELECT TABLE WH				
TABLE WI: ALTERNATE CAGE AND REFERENCE NUMBER SET				
SELECT TABLE WI				
TABLE WJ: AUTHORITY TO FIT ACRN ON SERIAL NUMBER SYSTEM/END ITEM				
AUTHORITY TO FIT SERIAL NUMBER	M	911	AUTHTFWJ	
TABLE WK: AUTHORITY TO FIT ACRN ON SYSTEM/END ITEM				
AUTHORITY TO FIT	M	911	AUTHTFWK	
TABLE WL: MAINTENANCE TASK TO SYSTEM CROSS REFERENCE				
SELECT TABLE WL				

Data Element	Key	DED	DE CODE	Required
TABLE WM: SERVICING LIBRARY				
END ITEM ACRONYM CODE (EIAC)	F	96	EIACODXA	
SERVICING IDENTIFIER	K	933	SRVCIDWM	
TABLE WN: SERVICING IDENTIFICATION				
SERVICING TITLE		935	SVTITLWN	
SIGN UP REQUIREMENT		936	SIGNUPWN	
STANDARD ACTIVITY CODE		836	STNACTWN	
TABLE WO: SERVICING TASK				
SELECT TABLE WO				
TABLE WP: SERVICING INTERVAL AND EVENT MEASUREMENT BASE				
SERVICING INTERVAL		934	SVCINTWP	
TABLE WQ: SERVICING FACILITY				
SELECT TABLE WQ				
TABLE WR: SERVICING TECHNICAL MANUAL				
SELECT TABLE WR				
TABLE WS: SERVICING GROUP				
SERVICING GROUP IDENTIFIER	K	930	GRUPIDWS	
SERVICING GROUP SEQUENCE NUMBER		931	GRPSEQWS	
TABLE WU: TECHNICAL MANAGEMENT CODE LOG				
LOG REQUIREMENT	K	926	LOGREQWU	
TABLE WV: LCN ENHANCED CRITICALITY CODE				
SELECT TABLE WV				
TABLE WX: COMPARTMENT CODE LIBRARY				
COMPARTMENT CODE	K	831	COMPCDWX	
COMPARTMENT CODE NAME		832	CCNAMEWX	
COMPARTMENT CODE DESCRIPTION		833	CCDESCWX	
TABLE WY: LCN INFORMATION EXTENSION				
PRIME CAGE CODE		46	CAGECDWF	
PRIME REFERENCE NUMBER		337	REFNUMWF	
ACRN SET SEQUENCE NUMBER		919	SEQNUMWF	
ITEM CRITICALITY		925	CRITEMWY	
CONFIGURATION CODE		920	CFGCODWY	
REQUIRED FIT		929	REQFITWY	
MEAN TIME BETWEEN FAILURE-B		928	MTBFBXWY	
WORK AREA CODE		940	WACODERA	
EXTENDED NOMECLATURE		909	EXTNOMWY	
LCN REPLACEMENT LEVEL		910	REPLEVWY	
COMMON MANAGEMENT CODE		908	CMCODEWY	
CONFIGURATION ITEM NUMBER (CIN)		830	CINCODWY	
COMPARTMENT CODE		831	COMPCDWX	
ASSEMBLY ITEM DESIGNATOR		835	AIDCODWY	
ADAASS REFERENCE NUMBER (HEADER)		837	ADRNHDWY	

Data Element	Key	DED	DE CODE	Required
ADAASS REFERENCE NUMBER (HEADER VARIANT)		838	ADRNHVWY	
AUSTRALIAN DEFENCE ORGANISATION Z TABLES				
TABLE ZC: MMI PROCESS LIBRARY				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
MMI PROCESS CODE	K	810	MMIPROZC	
MMI PROCESS CODE DESCRIPTION		811	MPRDESZC	
MMI SERV SIGNUP REQUIREMENT		936	SIGNUPZC	
TABLE ZD: MMI SERVICING GROUPS				
END ITEM ACRONYM CODE (EIAC)	F	096	EIACODXA	
LSA CONTROL NUMBER (LCN)	F	199	LSACONXB	
ALTERNATE LCN CODE	F	019	ALTLCNXB	
LCN TYPE	F	203	LCNTYPXB	
TASK CODE	F	427	TASKCDCA	
SERVICING GROUP IDENTIFIER	K	930	GRUPIDZD	
SERVICING GROUP SEQUENCE NUMBER		931	GRPSEQZD	
TABLE ZE: MMI SERVICING TASK LIST				
SELECT TABLE ZE				
TABLE ZF: MMI SERVICING GROUPED TASKS				
SERVICING GROUP TASK SEQUENCE NUMBER	K	932	TSKSEQZF	
TABLE ZG: MMI SERVICING TASK REQUIREMENT EXTENSION				
MMI SERVICING TITLE		935	MSTITLZG	
STANDARD ACTIVITY CODE		836	STNACTZG	
TABLE ZL: ALCS WITHIN ALCS				
SELECT TABLE ZL				

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-TDATA-PUBPACK-V5.3

2. TITLE: PUBLICATIONS PACKAGES

3. DESCRIPTION AND INTENDED USE

3.1 A Publications Package (PUBPACK) contains publications and amendments to publications that are to be delivered to the Commonwealth, and other parties if applicable, in accordance with the Approved Publications Tree (PUBTREE). The use of PUBPACKs enables new publications and amendments to publications to be managed as deliverable data items under the Contract.

3.2 The Contractor uses PUBPACKs to manage the delivery of those publications and amendments to publications that will be used in the operation and support of the Mission System and the Support System. This DID acts as a specification for the publications and amendments to publications within the PUBPACK, when these requirements have not been specified elsewhere in the Contract.

3.3 The Commonwealth uses PUBPACKs to obtain publications and amendments to publications, and to manage these as deliverable data items under the Contract.

4. INTER-RELATIONSHIPS

4.1 The publications and amendments to publications to be included in each PUBPACK are defined in the Approved PUBTREE. The PUBTREE is derived from the Master Technical Data Index (MTDI).

4.2 Each PUBPACK is subordinate to the following data items, where these data items are required under the Contract:

a. Integrated Support Plan (ISP);

b. Technical Data Plan (TDP); and

c. Verification and Validation Plan (V&VP).

4.3 The distribution and use of publications delivered in accordance with this DID are subject to the rights and limitations in the Technical Data and Software Rights (TDSR) Schedule.

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

S1000D™	*International Specification for Technical Publications using a Common Source Database*, Issue 5.0
DEF(AUST)5629C	*Production of Military Technical Manuals*
DEF(AUST)IPS-5630	*Developing S1000D Interactive Electronic Technical Publications (IETPs)*
ASD-STE100	*International specification for the preparation of technical documentation in a controlled language*

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 This data item shall **not** comply with the CDRL clause entitled ‘General Requirements for Data Items’.

6.2 Specific Content

6.2.1 Specific Requirements

6.2.1.1 Where the publication standard is specified in the Contract (including in the Support System Functional Baseline), this standard shall have precedence over any Approved plan, unless otherwise agreed by the Commonwealth Representative in writing.

6.2.1.2 Unless otherwise specified in the Contract or agreed by the Commonwealth Representative in writing, all new publications and amendments to existing publications, which are to be delivered to the Commonwealth, shall be developed using a Simplified Technical English (STE) dictionary derived from ASD-STE100.

6.2.1.3 Unless otherwise specified in the Contract or in the Approved ISP or the Approved TDP (whichever is the governing plan under the Contract):

Note: The term 'Business Rule Decision Points (BDRP)' in the following clause has the meaning given in DEF(AUST)IPS-5630.

a. all new publications to be developed and delivered to the Commonwealth shall comply with S1000D, DEF(AUST)IPS-5630, and the Business Rule Decision Points (BRDP) specified in the Approved TDP or the Approved ISP (as applicable); and

b. all amendments to existing Commonwealth publications, to be delivered to the Commonwealth, which:

(i) are in S1000D Issue 5.0 format, shall be prepared in accordance with DEF(AUST)IPS-5630 and be consistent with the existing publication's BRDP;

(ii) are in a legacy S1000D format, shall be prepared in accordance with DEF(AUST)IPS-5630 and be consistent with the existing publication; and

(iii) are not in S1000D format, shall comply with DEF(AUST)5629C.

6.2.1.4 All amendments to existing Contractor and Subcontractor publications, which are to be delivered to the Commonwealth, shall be prepared in the same style and format as the publication being amended.

6.2.1.5 Unless otherwise agreed by the Commonwealth Representative in writing, the following criteria shall be utilised for producing amendments to existing publications that are to be delivered to the Commonwealth:

a. where a single or multiple S1000D Common Source Database (CSDB) object(s) have been identified as changed, these will be delivered as a complete or partial data exchange package in accordance with clause 6.2.2;

b. if less than or equal to five percent of the pages of an existing publication are affected by the amendment, a page-for-page change to the affected publication is required; and

c. if more than five percent of the pages of an existing publication are affected by the amendment, a new publication incorporating all of the required changes shall be provided.

6.2.1.6 Third-party publications, where source data is not reasonably available to the Contractor, may be provided to the Commonwealth in existing vendor layout and format.

6.2.1.7 All amendments to third-party publications, which are to be delivered to the Commonwealth, shall be provided in the same style and format as the parent publication.

6.2.2 Specific Requirements – S1000D Delivery Requirements

6.2.2.1 Each delivery of S1000D Issue 5.0 Technical Data shall include:

a. the Data Management List (DML), which contains the current list of all CSDB objects to be delivered for the Contract (and which may be delivered as an S1000D listing from the Approved Publications Tree);

b. a data exchange package, which includes:

(i) a Data Dispatch Note (DDN), which lists all of the CSDB objects that are ready for delivery and their status (ie, in either draft or a completed format);

(ii) as a minimum, the CSDB objects (ie, S1000D Data Modules developed using eXtensible Markup Language (XML) files or Standard Generalized Markup Language (SGML) files, illustrations, multimedia, and legacy data formatted files) for those S1000D Data Modules identified for delivery in accordance with the Approved Publications Tree; and

(iii) a Business Rules Exchange (BREX) file for the validation of the CSDB objects.

6.2.2.2 The S1000D Data Modules referred to in clause 6.2.2.1b(ii) shall be:

a. developed to a compliant S1000D XML schema, as defined in S1000D issue 5.0;

b. delivered as source S1000D XML files with all associated information objects that make up the completed technical publication data, as defined in DEF(AUST)IPS-5630;

c. delivered with all supporting information objects, developed consistent with the system, sub system and sub subsystem breakdown structure used for operation and maintenance of the applicable products;

d. validated using the Approved BREX file, to confirm that they comply with Commonwealth requirements in DEF(AUST)IPS-5630 and the supporting BRDP.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-TDATA-TDP-V5.3

2. TITLE: TECHNICAL DATA PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Technical Data Plan (TDP) describes the Contractor's strategy, plans, methodology, and processes for meeting Contract requirements for the identification, control, assembly, preparation, verification, validation and delivery of Technical Data.

3.2 The Contractor uses the TDP to:

a. document the strategy, plans and procedures to define, manage and monitor the Technical Data activities under the Contract; and

b. ensure that those parties (including Subcontractors) who are undertaking Technical Data related activities understand their respective responsibilities, the processes to be used, and the time-frames involved.

3.3 The Commonwealth uses the TDP to:

a. ensure that the full scope of Technical Data associated with the Contract will be appropriately defined, developed, and monitored, and that there are coherent management arrangements in place;

b. understand and evaluate the Contractor's approach to meeting the Technical Data requirements of the Contract; and

c. understand the Commonwealth's involvement in the Contractor's Technical Data activities, including the monitoring of the Contractor's activities.

4. INTER-RELATIONSHIPS

4.1 The TDP is subordinate to the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP);

b. Integrated Support Plan (ISP);

c. Systems Engineering Management Plan (SEMP); and

d. Configuration Management Plan (CMP).

4.2 The TDP inter-relates with the following data items, where these data items are required under the Contract:

a. Contract Work Breakdown Structure (CWBS);

b. Configuration Status Accounting Report (CSAR);

c. all data items derived from the Master Technical Data Index (MTDI);

d. Software List (SWLIST);

e. Data Accession List (DAL);

f. Publications Packages (PUBPACK); and

g. Verification and Validation Plan (V&VP).

5. APPLICABLE DOCUMENTS

Note to drafters: The following list is indicative of the range of Technical Data standards available. Project Offices need to amend the list to ensure that the references align with current Defence policy and requirements of the Contract. See also the standards listed in Annex A.

5.1 The following documents form a part of this DID to the extent specified herein:

S1000D™	*International specification for technical publications using a common source database, Issue 5.0*
DEF(AUST)5629C	*Production of Military Technical Manuals*
DEF(AUST)IPS-5630	*Developing S1000D Interactive Electronic Technical Publications (IETPs)*
DEF(AUST)CMTD-5085C	*Engineering Design Data for Defence Materiel*
ISO 10303	*Automation systems and integration — Product data representation and exchange*
ISO 10918	JPEG
ISO 32000-1	*Document management – Portable document format*
MIL-PRF-28000	*Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols*
MIL-PRF-28001	*Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text*
MIL-PRF-28002	*Raster Graphics Representation in Binary Format*
	ADF Service Publication standard(s), as specified in the Statement of Work

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 This data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the TDP shall summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The TDP shall describe the objectives, scope, constraints, and assumptions associated with the Contractor's Technical Data activities. Any risks associated with these activities shall be documented in the Risk Register; however, the TDP shall describe the risk management strategies associated with any global risks relating to Technical Data.

6.2.2 Technical Data Organisation

6.2.2.1 The TDP shall describe the Contractor's organisational arrangements for meeting the Technical Data requirements of the Contract, including:

a. identification of the Contractor's Technical Data manager, who will have managerial responsibility for meeting the Technical Data requirements of the Contract;

b. the Contractor's and Approved Subcontractors' organisations with a primary responsibility for managing Technical Data, showing how these arrangements integrate into the higher-level management structures and organisations;

c. the interrelationships and lines of authority between all parties involved in the Contractor's Technical Data activities; and

d. the Contractor's and Approved Subcontractors' management positions with significant responsibilities for Technical Data activities.

6.2.3 Overview of Technical Data and Related Activities

6.2.3.1 The TDP shall provide an overview of the Contractor's program for meeting the Technical Data requirements of the Contract, including:

a. the major activities to be undertaken, when, and by whom;

b. the integration of Subcontractors into the Contractor's Technical Data activities;

c. the personnel (including categories, expected numbers (by category) and associated skills/competencies) required by the Contractor and Subcontractors to meet the Technical Data requirements of the Contract, including the proposed sources for obtaining those personnel;

d. the interfaces between the Technical Data activities and the Systems Engineering (SE) and Integrated Logistics Support (ILS) programs, including the mechanisms for ensuring that the Technical Data activities and outcomes are consistent with the developmental outcomes and support concepts for both the Mission System and the Support System;

e. the interfaces between the Technical Data activities and the Configuration Management (CM) program;

f. if not addressed in other data items delivered to the Commonwealth, the Contractor's strategy and methodology for electronic data interchange, if required, including the use of a Data Management System (DMS);

g. if escrow is a requirement under the Contract, the identification of the proposed escrow agent, categories of Technical Data to be placed in escrow, and an outline plan for maintaining the currency of the Technical Data stored in escrow for the duration of the Escrow Agreement; and

h. any training related to Technical Data that the Contractor's and Subcontractors' staff need to undertake, including details of any proposed Training courses.

6.2.3.2 If not addressed in other data items delivered to the Commonwealth, the TDP shall identify the issues, methodologies and processes for controlling and enabling access to Technical Data that is subject to restrictions, such as restrictions from Intellectual Property rights, security, Export Approvals, Technical Assistance Agreements, escrow arrangements, or other.

6.2.3.3 The TDP shall describe the Contractor's expectations of the Commonwealth with respect to the management of Technical Data including, if applicable, the interfaces and interactions with Commonwealth organisations external to the project office.

6.2.4 Technical Data Requirements Analysis

6.2.4.1 The TDP shall describe the Contractor's strategy, methodology, and processes to be utilised to undertake a Technical Data requirements analysis, including:

a. the system for categorising Technical Data based on its intended purpose (eg, Maintenance manual, specification, drawing, presentation for a system review, etc), origin, management approach, and any other criteria defined by the Contractor;

b. determining the appropriateness of using existing Technical Data to enable the Materiel System to be operated and supported through life, considering Defence's requirements for the configuration, roles and environments that are applicable to the Materiel System;

c. undertaking cost-benefit analyses, if required, to determine the applicable Technical Data standards and specifications to be used;

d. optimising the 'packaging' of scope and content for publications to:

(i) minimise the number of publications required to be accessed by users to perform specific tasks;

(ii) minimise the duplication of content between publications, and ensuring consistency if duplication cannot be avoided; and

(iii) where publications will be applied to different configurations of the Mission System(s) and Support System Components, clearly identifying the relevance of configuration-specific content to the specific configurations;

e. identifying and optimising the range and quantity of Technical Data required to be delivered under the Contract, including:

(i) existing Technical Data that is expected to be suitable without modification;

(ii) existing Technical Data that is expected to require conversion into a different format;

(iii) existing Technical Data that is expected to require modified content; and

(iv) proposed new Technical Data.

6.2.5 Technical Data Development – General

6.2.5.1 The TDP shall describe:

a. the Contractor's program of activities for managing the Technical Data program;

b. the Contractor's program of activities for the identification, design, development, and delivery of Technical Data (appropriately cross-referenced to activities in the Contract Master Schedule (CMS) and in any subordinate schedules);

c. the Software tools to be applied to the generation and interpretation (authoring and viewing) of Technical Data;

d. the procedures, by category of Technical Data, for the receipt, review, Configuration Control, amendment, production and delivery of all Technical Data and associated supporting hardware and Software for the Support System (eg, to host IETPs, drawings / design data sets, or the Configuration Management System);

e. the procedures for the management and control of:

(i) the MTDI, including the Support System Technical Data List (SSTDL);

(ii) the DAL, if a DAL is required under the Contract; and

(iii) related elements of the TDSR Schedule (with reference to the PMP);

f. the procedures for validating the MTDI, including the individual data items derived from the MTDI;

g. the strategy, methodology and processes to meet the Technical Data related regulatory / assurance requirements of the Contract, and any required organisational accreditations and / or certifications;

Note: Terms 'validate' and 'verify' in the following subclause are as used in DEF(AUST)5629C and DEF(AUST)IPS-5630, and do not apply to other sections of the Contract.

h. the Contractor's overall strategy, methodology and processes to validate Technical Data, including an indicative schedule and standards to be used; and

i. the Contractor's strategy and methodology for assisting the Commonwealth to verify Technical Data.

6.2.6 Technical Data Development – Standards and Specifications

6.2.6.1 The TDP shall describe:

a. the standards, by Technical Data category, for the preparation of Technical Data (refer clauses 6.2.6.2 and 6.2.6.3 of this DID);

b. the strategy, methodology and processes to validate that each data type complies with the relevant Technical Data standard;

c. the strategy, methodology and processes for the Contractor to convert any Technical Data that currently exists in formats that do not comply with the standards and specifications identified at Annex A to formats that do comply;

Note: 'Business Rules' in the following clause has the meaning given in DEF(AUST)IPS-5630.

d. for Technical Data that is produced as Common Source Database (CSDB) Objects in accordance with DEF(AUST)IPS-5630 and S1000D™, the methodology and processes to validate that the structure and the set of eXtensible Markup Language (XML) accords with the required Business Rules;

e. for Technical Data that is produced in accordance with DEF(AUST)5629C, the methodology and processes to validate that the structure and set of the Standard Generalised Markup Language (SGML) tagging accords to the Document Type Definition (DTD) (Army/Navy/RAAF versions) detailed in DEF(AUST)5629C; and

f. the methodology to validate that data file formats comply with the applicable standards used for data exchange and the methodology to validate the data file interpreters (eg, viewing tools) where they are provided as part of the Contract deliverables, including:

(i) the processes and timeframes for conducting compliance testing; and

(ii) details pertaining to whether the Contractor proposes to conduct the testing using an internationally recognised testing authority, a central body, or an agency sub-contracted by the central body.

6.2.6.2 For each of the Technical Data categories identified under clause 6.2.4.1a, the TDP shall identify the Technical Data standards and specifications to be applied, using the following descriptors:

a. ***Primary Compliant Formats*** – digital formats that are compatible with the Commonwealth's policies and business practices;

b. ***Alternative Compliant Formats*** – digital formats that are not current Commonwealth policy or business policy, but may be considered on a case-by-case basis, depending upon the data type, Life Cycle Cost (LCC) considerations, intended management strategy, and application of the data;

c. ***Acceptable Non-Compliant Formats*** – digital formats that may be considered by the Commonwealth, depending on the data type, LCC considerations, intended management strategy, and application of the data; and

d. ***Formats that are not Suitable*** – proprietary digital formats that shall not be considered for delivery, except where the application is in current use in the Commonwealth and the cost-benefit analysis justifies delivery in these formats.

6.2.6.3 In applying the descriptors identified in the preceding clause, the TDP shall take into consideration that the Commonwealth currently utilises the Technical Data standards and specifications identified at Annex A to this DID.

6.2.7 Technical Data Development – Publications

6.2.7.1 The TDP shall describe:

a. the strategy, methodology, processes, and standards associated with the identification, development and delivery of publications;

b. the strategy, methodology and processes for validating the publications for readability, technical accuracy and grammatical correctness;

c. the Contractor's internal review and approval processes and procedures for publications prior to release to the Commonwealth, including in-process reviews, controls, and schedules;

d. the methodology for handling routine and priority changes and supplements;

e. the strategy and methodology for assessing the suitability of existing Commonwealth publications, if applicable; and

f. the procedures to identify the amendments required to existing publications and the management of amendment incorporation.

6.2.8 Technical Data Development – S1000D Technical Data

6.2.8.1 If S1000D Technical Data is applicable to the Contract, the TDP shall describe:

a. the Contractor's strategy, methodology, and processes for the development of S1000D Technical Data, in accordance with the Business Rules defined in accordance with clause 6.2.8.2;

b. the Contractor's program of activities associated with the design, development, and delivery of S1000D Technical Data (including cross-references to related activities in the CMS and in any subordinate schedules);

c. the functionality of the S1000D Technical Data IETPs to be produced;

d. the linkages with any Computer-Based Training required under the Contract;

e. the Contractor's strategy, methodology, processes, and program of activities for undertaking verification and validation of S1000D Technical Data (cross-referenced to the applicable V&V program plans);

f. the Contractor's proposed support strategy for the S1000D Technical Data, including the role and scope of the Commonwealth in the provision of in-service support and the proposed data exchange arrangements, the frequency of delivery for regular updates, and the approach to be implemented for urgent releases; and

g. the methods of data exchange and transfer under the Contract, including data transfer points, in accordance with DEF(AUST)IPS-5630 or as otherwise agreed by the Commonwealth.

6.2.8.2 The TDP shall include (as an annex) a Business Rules Index, based on Annex B to DEF(AUST)IPS-5630, which includes:

a. the (common) Defence Business Rules specified in DEF(AUST)IPS-5630;

b. any additional or modified Business Rules specified at Annex A to the SOW or in the ADF Service Publication standard(s) identified in the SOW; and

Note: Commonwealth agreement to the Contractor-proposed BRDP will be provided through Approval of the TDP.

c. the Business Rules Decision Points (BRDP) proposed by the Contractor for those BRDP designated in Annex B to DEF(AUST)IPS-5630 as "Contractor to propose, Commonwealth to agree".

6.2.9 Technical Data Development – Engineering Drawings

Note: 'Engineering drawings' refers to engineering design data for hardware products of the Materiel System, including technical drawings and data sets (eg, three-dimensional modelling and computer-aided design data).

6.2.9.1 The TDP shall describe:

a. the methodology and processes to analyse the requirements for engineering drawings, including the applicable levels and categories of drawings, required:

(i) to support Contract activities, including Mandated System Reviews; and

(ii) to enable the sustainment of the Materiel System;

b. the strategy, methodology, processes, and standards associated with the development and delivery of engineering drawings, including the Contractor's proposed tailoring and implementation of DEF(AUST)CMTD-5085C;

c. the indexing method employed by the Contractor to manage and control the suite of engineering drawings;

d. the strategy for validating the engineering drawings for technical accuracy;

e. the Contractor's internal review and approval processes and procedures for engineering drawings prior to release to the Commonwealth, including in-process reviews, controls, and schedules; and

f. the methodology for handling routine and priority changes to engineering drawings.

ANNEX A TO DID-ILS-TDATA-TDP

CURRENT COMMONWEALTH TECHNICAL DATA STANDARDS AND SPECIFICATIONS

Note to drafters: Amend the following list to ensure that the standards align with current Defence policy and the requirements of the project, including any requirement to update legacy Technical Data.

1. TECHNICAL PUBLICATIONS

1.1 Primary Delivery Compliant Format:

a. for Interactive Electronic Technical Publications (IETPs), the publications accord with S1000D™ and DEF(AUST)IPS-5630), and any Contract-specific requirements for S1000D™ deliverables; and

b. for page-based publications (including class 1 and 2 electronic technical manuals), the publications accord with either:

(i) S1000D™ and DEF(AUST)IPS-5630 (including for legacy publications produced in accordance with previous versions of S1000D (ie, prior to Issue 5.0)); or

(ii) DEF(AUST)5629C.

1.2 Primary Data-Source Compliant Format – Processable / Dynamic Documents:

a. Text - XML applying the applicable schemas as per DEF(AUST)IPS-5630; and

b. Graphics - vector and raster formats as detailed in S1000D™ (eg, Computer Graphics Metafile (CGM) for vector graphics and TIFF, PNG, JPEG for raster formats).

1.3 Alternative Data-Source Compliant Format:

a. Text - XML applying schemas Approved for use by the Commonwealth;

b. Graphics - vector and raster formats as detailed in S1000D™ (eg, CGM for vector graphics and TIFF, PNG, JPEG for raster formats); and

c. Composed Document - documents provided, which require no amendments throughout the life cycle of the equipment, may be delivered in Portable Document Format (PDF) in accordance with ISO 32000-1:2008.

1.4 Acceptable Data-Source Non-Compliant Format:

a. a neutral data file (platform independent file format) containing as a minimum hyperlink referencing between the table of contents and the applicable text. Preference is for PDF in accordance with ISO 32000-1:2008; and

b. native digital format in use by the Commonwealth (eg, Word 2010 '.docx' or later).

2. ENGINEERING DRAWINGS

2.1 Primary Data-Source Compliant Format:

a. DEF(AUST)CMTD-5085C; and

b. ISO 10303.

2.2 Acceptable Data-Source Non-Compliant Format:

a. AutoCAD native drawing format (DWG) in accordance with versions used by the Commonwealth or as agreed by the Commonwealth Representative. Drawings must be a direct output from the authoring system, and not the result of a translation process. All information necessary to open and manipulate the data files, including libraries, fonts, logical name definitions, and other supporting files shall be delivered with the drawing files; and

b. Autodesk Drawing Exchange Format (DXF) in accordance with versions used by the Commonwealth or as agreed by the Commonwealth Representative.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-TNG-CBT-V5.3

2. TITLE: COMPUTER BASED TRAINING

Note to drafters: Projects teams considering specifying CBT as a Training delivery method should develop the contents of this DID. DID-ILS-TDATA-PUBPACK, which also specifies data items that are Supplies, may be useful as a reference when developing this DID.

3. DESCRIPTION AND INTENDED USE

3.1 This Computer Based Training (CBT) DID defines [... INSERT GENERIC PURPOSE OF DATA ITEM AS SPECIFICATION FOR CBT ...].

3.2 The Contractor uses the CBT DID as the specification for [... INSERT CONTRACTOR USE OF DATA ITEM ...] which are to be delivered to the Commonwealth.

3.3 The Commonwealth uses the CBT DID to specify requirements for and obtain delivery of [... TBD COMMONWEALTH NEED FOR DATA ITEM ...].

4. INTER-RELATIONSHIPS

4.1 Computer Based Training (CBT) is subordinate to the following data items, where these data items are required under the Contract:

a. Integrated Support Plan (ISP);

b. Training Support Plan (TSP); and

c. Learning Management Packages (LMPs).

4.2 CBT inter-relates with the following data items, where these data items are required under the Contract:

a. Support System Technical Data List (SSTDL);

b. Training Materials List (TML);

c. Training Equipment List (TEL);

d. Software List (SWLIST);

e. Interactive Electronic Technical Publications (IETPs); and

f. [... TBD ...].

4.3 The distribution and use of CBT delivered in accordance with this DID are subject to the rights and limitations in the Technical Data and Software Rights (TDSR) Schedule.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

TBD

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 This data item shall **not** comply with the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 [... TBD ...].

6.2 Specific Content

Note to drafters: The specific content should include reference to any required data formats if necessary to ensure compatibility with existing Training delivery systems.

6.2.1 [... TBD ...]

6.2.1.1 [... TBD ...].

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-TNG-LMP-V5.3

2. TITLE: LEARNING MANAGEMENT PACKAGE

3. DESCRIPTION AND INTENDED USE

3.1 The Learning Management Package (LMP) comprises the complete set of documentation necessary for the management and delivery of a Training course, including course design information and lists of the Training Equipment and Training Materials used for delivery. The LMP documents the Contractor's outputs from the '*design'* and the *'develop'* phases of the Systems Approach to Defence Learning (SADL) model (ie, including analyse, design, develop, implement and evaluate phases).

3.2 The Contractor uses the LMP to:

a. document the outcomes of its Training design and development activities;

b. demonstrate to the Commonwealth how the Training course will address the requirements of the performance needs and analysis outcomes, including those within a Training Requirements Specification (TRS) when applicable;

c. demonstrate to the Commonwealth that the Training courses represent part of a solution that minimises Life Cycle Cost; and

d. provide the basis for the management and delivery of the related Training course under the Contract and under the Contract (Support), as applicable.

3.3 The Commonwealth uses the LMP to:

a. assist to evaluate the Contractor’s design and content of the Training course;

b. Verify the suitability of the proposed Training courses including, if applicable, with respect to a TRS;

c. understand the Commonwealth’s scope of work for Sustainment Training; and

d. prepare for the Verification and Validation (V&V) of the Training course(s).

4. INTER-RELATIONSHIPS

4.1 The LMP is subordinate to the following data items, where these data items are required under the Contract:

a. Integrated Support Plan (ISP);

b. Training Support Plan (TSP); and

c. Verification and Validation Plan (V&VP).

4.2 The LMP inter-relates with the following data items, where these data items are required under the Contract:

a. Performance Needs Analysis Report (PNAR);

b. Training Recommendations Report (TNGRECR);

c. Training Requirements Specification (TRS);

d. Support System Technical Data List (SSTDL);

e. Training Materials List (TML), a part of the Master Technical Data Index (MTDI);

f. Training Equipment List (TEL);

g. Software List (SWLIST);

h. Recommended Provisioning List (RPL);

i. Acceptance Test Plans (ATPs);

j. Acceptance Test Procedures (ATProcs); and

k. Acceptance Test Reports (ATRs), including ‘trial course’ reports.

4.3 The LMP inter-relates with the Technical Data and Software Rights (TDSR) Schedule.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

SADL Guide	Defence Learning Manual chapter 4: the *Systems Approach to Defence Learning Practitioners’ Guide*
	ADF Service Training Manual(s), as specified in the Statement of Work
	Standards for Training Packages, Australian Industry and Skills Committee
	Standards For VET Accredited Courses 2021, Australian Skills Quality Authority (ASQA)

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

Note: The SADL Guide identifies further information that may be added to the delivered data item, by the Commonwealth, for the purpose of internal approvals.

6.2.1 General

6.2.1.1 The LMP shall be developed to incorporate the results from the learning solution design and development activities undertaken in accordance with the Approved TSP or ISP (whichever is the governing plan in the Contract), including the following SADL products:

a. in respect of the SADL Analyse Phase (Annexes to the Approved TSP or ISP (whichever is the governing plan in the Contract) that are to be transferred to Annexes of the LMP for the applicable learning solution):

(i) Design Phase Scope Proposal (SADL product DesP1); and

(ii) Risk Assessment Summary (SADL product AP2);

b. in respect of the SADL Design Phase (to be included as Annexes to the LMP):

(i) Task Breakdown Sheet (SADL product DesW1);

(ii) Learning Outcomes Requirements Sheet (SADL product DesW2);

(iii) Draft Learning Outcomes (SADL product DesW3); and

(iv) Mapping Matrix (SADL product DesP3)

6.2.2 Draft Learning Management Package

6.2.2.1 When this DID is invoked for the delivery of a Draft LMP, the delivered data item shall include sections 1 to 3 of the LMP, as defined by clause 6.3.

6.2.2.2 The Draft LMP documents the results of the SADL design phase and shall be substantially complete and sufficient to enable the Commonwealth to:

a. Verify that the curriculum addresses the performance needs and course specifications included within or supporting the TRS or TNGRECR, as applicable;

b. determine if the learning and assessment modules appear suitable and achievable;

c. determine whether the review and evaluation strategies appear suitable; and

d. if applicable to a qualification recognised within the national register of Vocational Education and Training (VET), review the readiness of the Units of Competency (UOCs) and course documents for accreditation by the National VET Regulator (ie, ASQA) or other accrediting body.

6.2.3 Learning Management Package

6.2.3.1 When this DID is invoked for the delivery of a (complete) LMP, the delivered data item shall include sections 1 to 5 of the LMP, as defined by clause 6.3.

6.2.3.2 The LMP incorporates the results of the SADL develop phase and shall be complete in all aspects, and suitable for the management and delivery of the Training course. For the purposes of this clause, ‘complete in all aspects’ includes Training Materials that are items of Technical Data developed for purposes other than Training (eg, operating and maintenance manuals) and which are delivered separately under the Contract.

6.3 Learning Management Package Structure

Note: Words in italics indicate headings within the SADL LMP template guide.

6.3.1 Section 1: Learning Management Information

6.3.1.1 Section 1 of the LMP, *learning management information*, shall contain a *course data description*, including:

a. the identifying course code, the course name, and short name;

b. the highest security classification of course content (often related to Technical Data or Software that supports but was not developed for Training purposes) as defined by the Security Classification and Categorisation Guide;

c. a statement of the course aim;

d. a brief course description, including an overview of the scope of the learning outcomes to be covered, core learning activities and other associated learning programs that, together, form a learning and development solution;

e. the type of course (eg, continuation, familiarisation or specialist);

f. the minimum and maximum number of students per course;

g. the primary delivery method (eg, distance learning, instructor led, etc);

h. applicable trade / profession (ie, ‘skills domain’ or ‘job family’) of the participants;

i. total course duration; and

j. if applicable, the Registered Training Organisation.

6.3.1.2 Section 1 of the LMP shall contain a list of the course *learning outcomes* including a sequence number, description and, if applicable, the related UOCs from training packages and qualifications within the national register of VET.

6.3.1.3 Section 1 of the LMP shall contain an outline of the *summative assessments* and identify the required assessor qualifications.

6.3.1.4 Section 1 of the LMP shall contain details of course prerequisites including:

a. *course Service prerequisites* (eg, Defence prerequisites, student rank or grade, required security clearance, and so on) when this information is provided by the Commonwealth;

b. *course qualifications prerequisites* including, as applicable:

(i) education qualifications and language prerequisites;

(ii) prerequisite military proficiencies;

(iii) prerequisite UOCs identified from training packages and qualifications within the national register of VET; and

(iv) prerequisite courses, including courses that are not included within the national register of VET; and

c. *any additional prerequisites* identified by the course designers and developers.

6.3.1.5 Section 1 of the LMP shall list *course targets* in terms of proficiencies, competencies, qualifications and licences, as applicable.

6.3.1.6 If the course is a '*program course*', comprising a series of component or 'child courses', section 1 of the LMP shall list the *program course components* by course code and title.

6.3.1.7 Section 1 of the LMP shall contain a list of major items of *course equipment* (ie, Training Equipment) identified by part number (if available), equipment name and the required quantity (note that additional details will be included in section 3).

6.3.1.8 Section 1 of the LMP shall identify *Defence training authority details*, when this information is provided by the Commonwealth.

6.3.1.9 Section 1 of the LMP shall include an *evaluation plan* (ie, a SADL evaluation phase plan) that consists of:

a. a learning review plan, which includes:

(i) a summary of the V&V activities (eg, trial courses) to Verify the suitability of the course curriculum and to provide assurance of the quality of the learning and assessment materials;

(ii) cross-references to the ATPs and ATProcs applicable to the evaluation; and

(iii) focus areas for the evaluation process based on specific areas of risk (eg, safety critical and complex tasks); and

b. a *workplace evaluation plan*, which includes:

(i) a summary of the activities to Validate the learning outcomes and competencies applied in the workplace, including Contractor V&V program activities and recommended Defence activities, as applicable;

(ii) cross-references to the ATPs and ATProcs applicable to the evaluation; and

(iii) focus areas for the evaluation process based on specific areas of risk (eg, safety critical and complex tasks).

6.3.1.10 Section 1 of the LMP shall describe any *alternate learning pathways*, if applicable, such as assessment only, or recognition of competencies based on existing evidence.

6.3.1.11 Section 1 of the LMP shall identify course *accreditation* details including, when applicable:

a. the VET regulator for course accreditation (eg, ASQA);

b. Australian Vocational Education and Training Management Information Statistical Standard ('AVETMISS') codes and reporting requirements;

c. proposed accreditation period; and

d. recognition by other relevant professional or industry bodies.

6.3.1.12 Section 1 of the LMP shall include contact details for organisations able to grant *authority to use* the LMP and related Training Materials, consistent with Technical Data and Software Rights Schedule for the Contract.

6.3.1.13 Section 1 of the LMP shall identify *Intellectual Property holders* (ie, Defence, Contractor or third parties) including for course content imported from VET training packages, and cross-reference any related restriction of rights detailed in the TDSR Schedule.

6.3.1.14 Section 1 of the LMP shall incorporate, where applicable, any additional information:

a. including special information or instructions provided by the course developers; and

b. provided by the Commonwealth in relation to the above information requirements.

6.3.2 Section 2: Curriculum

6.3.2.1 Section 2 of the LMP shall describe the course curriculum, excluding cost information.

6.3.2.2 The course curriculum details shall include:

a. a *course overview*, including a course map (ie, graphical representation) showing the sequence of course modules and mapping of UOCs; and

b. course duration, identifying each learning and assessment module and any other activity, the duration of each module or other activity, and the total duration.

6.3.2.3 The course curriculum shall describe the *modules* within the course (where modules are used to group learning outcomes with a similar purpose or goal) including:

a. the module content, described in a single sentence and a list of the learning outcomes in the module;

b. identification of prerequisite modules;

c. the security classification of the content;

d. a list of the module's assessment activities;

e. a summary of the learning / Training delivery methods used within the module;

f. a list of key Support Resources, such as significant items of Training Equipment;

g. any WHS requirements; and

h. any additional information relevant to defining the scope of the module.

6.3.2.4 The course curriculum shall describe the *learning outcomes* for each module, including:

a. a learning outcome identifier (eg, LO1.1) and descriptive name;

b. performance conditions (ie, the learning and assessment environment);

c. performance standards to be attained in order to achieve competency;

d. assessment criteria, addressing the required skills, knowledge, and attitudes / behaviours;

e. identification of the related formative and summative assessment modules;

f. any related UOCs from VET;

g. a content summary, describing the skills, knowledge, etc, to be covered;

h. security classification of the content;

i. the Training level, if applicable (as defined in the SADL Guide);

j. any pre-requisite learning outcomes;

k. the learning / Training delivery method;

l. a summary of the resources required, including human resources, Facilities and Training Equipment;

m. a list of related Technical Data (ie, that was not developed as Training Materials);

n. any additional information relevant to describing the learning outcome; and

o. if there are no subordinate learning outcomes, a description of the teaching points applicable to this learning outcome.

6.3.2.5 The course curriculum shall describe each *subordinate learning outcome* (ie, being subordinate to a learning outcome in clause 6.3.2.4), as applicable, including:

a. identification of the related (parent) learning outcome;

b. a subordinate learning outcome identifier and descriptive name;

c. equivalent details for each topic identified in subclauses b to e and k to n under clause 6.3.2.4; and

d. teaching points.

6.3.2.6 The course curriculum shall describe the course assessments, including:

a. for each formative assessment:

(i) an identifier and name;

(ii) identification of the related learning outcome / subordinate learning outcome;

(iii) the assessment method;

(iv) a description of the assessment and the conditions under which the assessment is to be performed;

(v) the assessment criteria; and

(vi) any additional information relevant to describing the assessment; and

b. for each *summative assessment*:

(i) for the purposes of summative assessment, each requirement as listed in clause 6.3.2.6a; and

(ii) any related UOCs from VET.

6.3.2.7 The course curriculum shall include any *additional information* provided by the Commonwealth, including reference to related Defence policies and procedures.

6.3.3 Section 3: Major Resource Requirements

6.3.3.1 Section 3 of the LMP shall identify the human and other Support Resources required to deliver the course. The list of *major resource requirements* in the LMP shall include:

a. human resources requirements, including:

(i) instructors;

(ii) assessors; and

(iii) administration and support staff;

b. the physical Support Resource requirements, including:

(i) the use of Mission Systems, if applicable;

(ii) proposed Training Facilities, summarising requirements such as the utilities, installed equipment and information systems required;

(iii) significant items of Training Equipment; and

(iv) related services (eg, student transport and access to information systems);

c. the support to be provided by Defence units with a major role in providing learning and assessment activities, including the use of existing Defence resources; and

d. any additional information provided by the Commonwealth in relation to the above.

6.3.3.2 Section 3 of the LMP should cross-reference section 4 instead of detailing the Training Equipment and Training Materials that are not considered to be major resources.

6.3.4 Section 4: Learning and Assessment Materials

6.3.4.1 Section 4 of the LMP shall list the *learning and assessment materials* used for the management and implementation of the course, including:

a. materials developed for learning and assessment purposes including:

(i) student materials (eg, précis, workbooks, exercise and tutorial materials);

(ii) presentation media, exercise and other Training-delivery materials;

(iii) instructor manuals, guides and manuals for the use of Training Equipment;

(iv) student assessment and grading materials;

(v) software and electronic media for learning delivery and assessment;

(vi) competency specifications and graduation requirements;

(vii) requirements for individual Training records and reporting;

(viii) documents required for course evaluation and reporting; and

(ix) any other documents and Software required to enable delivery of Training courses, conduct assessments, and perform administrative functions; and

b. other Technical Data and Software that was developed for another purpose (eg, operating and maintenance manuals) but which is required for course.

6.3.4.2 Training Materials, developed for Training purposes, shall be attached to the LMP as soft copy data items.

6.3.4.3 For Technical Data and Software that were not developed for Training purposes but which are required for the delivery of Training, the LMP shall:

a. identify the reference number or document number, as applicable, including the version / build number for Software;

b. identify the document or Software module / library name, as applicable; and

c. include a cross-reference to the related entry in the SSTDL or SWLIST, as applicable.

6.3.5 Section 5: Supporting Materials

6.3.5.1 Section 5 of the LMP shall list *supporting materials* used for the development of the LMP, but which are not disseminated as part of the course. The list shall identify, for each supporting document, the name, version number and date, and a reference to the applicable annex containing the document.

6.3.5.2 *Supporting materials* to be listed in Section 5 of the LMP include, when required under the Contract:

a. the related TRS or TNGRECR, as applicable;

b. the ATPs, ATProcs and the ATR(s) that include the resulting ‘trial reports’, and

c. learning review reports.

6.4 Annexes

6.4.1 The LMP shall include annexes (or cross-references to supporting materials) for the following, as applicable to the Contract:

a. Design Phase Scope Proposal (SADL product DesP1);

b. Risk Assessment Summary (SADL product AP2);

c. Task Breakdown Sheet (SADL product DesW1);

d. Learning Outcomes Requirements Sheet (SADL product DesW2);

e. Draft Learning Outcomes (SADL product DesW3);

f. Mapping Matrix (SADL product DesP3); and

g. Trial Report (SADL product DP1).

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-MNT-AMOA-V5.2

2. TITLE: APPLICATION FOR MAINTENANCE ORGANISATION APPROVAL

3. DESCRIPTION AND INTENDED USE

3.1 The Application for Maintenance Organisation Approval (AMOA) is a formal submission by the Contractor, to the Commonwealth, to demonstrate that it has the means to perform Maintenance activities that comply with specified ADF regulatory / assurance framework requirements.

3.2 The Contractor uses the AMOA to seek formal recognition of its Maintenance organisation by submitting evidence that the Contractor:

a. can, and will, sustain a Maintenance organisation that complies with the specified ADF regulatory / assurance framework requirements, to the extent that they apply to the Maintenance activities required under the Contract; and

b. will undertake the required Maintenance activities to approved standards, using competent and authorised individuals, who are acting as members of the complying Maintenance organisation.

3.3 The Commonwealth uses the AMOA, to assess the Contractor’s capability and readiness to apply the specified ADF regulatory / assurance framework requirements to the Maintenance activities required under the Contract.

4. INTER-RELATIONSHIPS

4.1 The AMOA inter-relates with the following data items, where these data items are required under the Contract:

a. Maintenance Management Plan (MMP); and

b. Configuration Management Plan (CMP).

5. APPLICABLE DOCUMENTS

5.1 The following documents form part of the DID to the extent specified herein:

AAP 8000.011	Defence Aviation Safety Regulations (DASR)
ANP3411-0101	Naval Materiel Assurance Publication
LMSM	Land Materiel Safety Manual

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of other data items that contains aspects of the required information, the AMOA shall summarise these aspects and refer to the other data items.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.1.4 All documents provided as part of the AMOA shall be controlled documents.

6.2 Specific Content

6.2.1 Aerospace - Application for Maintenance Organisation Approval

6.2.1.1 Where the Contractor is required to comply with the DASR, as applicable to the scope of work under the Contract, the AMOA shall include:

a. a completed DASR Form 2 – ‘Application for DASR 145 and DASR M Subpart G Approval’, for the DASR 145 requirements (only); and

b. a *Maintenance Organisation Exposition* (MOE), addressing the requirements of DASR 145.A.70.

6.2.1.2 In meeting the requirements of clause 6.2.1.1, the AMOA shall, except where provided to the Commonwealth by other means, include the MMP and all plans, procedures, and other documents referenced in the MOE.

6.2.2 Land - Application to demonstrate compliance with the LMSM

6.2.2.1 Where the Contractor is required to show compliance with the LMSM, as applicable to the scope of work under the Contract, the AMOA shall:

a. be released under the authority of the Contractor’s Senior Maintenance Manager for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the Maintenance management systems, competent people, processes, data and other resources required to provide Maintenance Services consistent with the applicable LMSM requirements identified in the Contract;

c. except where provided to the Commonwealth by other means, include the MMP and CMP, as applicable, and all other plans, procedures, and related documents containing the objective quality evidence required by clause 6.2.2.1b; and

d. include a compliance matrix showing how the Contractor’s Maintenance management system complies with LMSM requirements applicable to the Maintenance activities under the Contract.

6.2.3 Maritime - Application to demonstrate compliance with Naval Materiel Assurance Publication

6.2.3.1 Where the Contractor is required to comply with the *Naval Materiel Assurance Publication*, as applicable to the scope of work under the Contract, the AMOA shall:

a. be released under the authority of the Contractor’s Senior Maintenance Manager for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the Maintenance management systems, competent people, processes, data and other resources required to provide Maintenance Services in accordance with *Naval Materiel Assurance Publication* requirements;

c. except where provided to the Commonwealth Representative by other means, include the MMP and CMP, as applicable, and all other plans, procedures and related documents containing the objective quality evidence required by clause 6.2.3.1b; and

d. include a compliance matrix showing how the Contractor’s Maintenance management system complies with *Naval Materiel Assurance Publication* requirements applicable to the Maintenance activities under the Contract.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-DEF-CWBS-V5.3

2. TITLE: CONTRACT WORK BREAKDOWN STRUCTURE

3. DESCRIPTION AND INTENDED USE

3.1 The Contract Work Breakdown Structure (CWBS) is the Contractor's extension of the Contract Summary Work Breakdown Structure (CSWBS) and forms the framework for Contract planning, management and status reporting, and for estimating costs, schedule and technical achievements at completion.

3.2 The Contractor uses the CWBS to:

a. define the work effort necessary to successfully achieve the end-objective of the Contract;

b. assist with estimating the cost, schedule and resource requirements for the Contract;

c. ensure that there is a clean structure for the organisation and management of the project and that there are clear accountabilities for project outcomes; and

d. achieve integrated cost, schedule and technical control.

3.3 The Commonwealth uses the CWBS to:

a. gain visibility into the Contractor's planning;

b. understand and evaluate the Contractor's approach to meeting the requirements of the Contract;

c. assist with monitoring the progress of the Contractor in meeting the requirements of the Contract; and

d. as a source of input to planning performed by the Commonwealth Representative.

4. INTER-RELATIONSHIPS

4.1 The inter-relationship of the CWBS with other plans is as described in the Project Management Plan (PMP).

4.2 The CWBS is related to, and shall be consistent with, the Contract Master Schedule (CMS).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

DEF(AUST) 5664A	Work Breakdown Structures for Defence Materiel Projects

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.1.2 The CSWBS shall form the basis for preparation of the CWBS by the Contractor.

6.2 Specific Content

6.2.1 General

6.2.1.1 The CWBS shall comprise a Work Breakdown Structure (WBS) index, a WBS graphic (optional), and a WBS dictionary.

6.2.1.2 The CWBS, including the WBS dictionary, shall comply with DEF(AUST) 5664A, including Recommended Practices 2, 5, 9, 10, 11, and any other Recommended Practices as determined by the Contractor.

6.2.2 WBS Index

Note: The WBS index is an indentured list of WBS elements and sub-elements, starting with a single level 1 element (the Contract), incorporating the high-level WBS element structure which is invoked contractually (the CSWBS), and the lower-level elements of the Contractor's WBS necessary to provide an appropriate framework throughout the project for product and service definition and control.

6.2.2.1 The CWBS shall include a WBS index delivered in a tool that has an Outline Mode (such as Microsoft Word), such that it can be reviewed at any level of expansion.

6.2.2.2 The WBS index shall be derived from the WBS dictionary and each record in the WBS index shall include:

a. WBS element number;

b. WBS element title;

c. WBS element revision date and revision number;

d. task agency; and

e. cross references to the conditions of contract and Statement of Work.

6.2.3 WBS Graphic

6.2.3.1 The CWBS may include a WBS graphic, which contains the same information as the WBS index, but shown in a graphical form, usually a tree structure.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-DEF-DCOD-V5.3

2. TITLE: DATA MANAGEMENT SYSTEM CONCEPT OF OPERATION DOCUMENT

3. DESCRIPTION AND INTENDED USE

3.1 The Data Management System (DMS) Concept of Operation Document (COD) describes the Contractor's implementation of the DMS Contract requirements to enable electronic interchange and processing of Contract data.

3.2 The Contractor uses the DMS COD to:

a. describe the Contractor's implementation of the DMS;

b. detail the requirements for implementing the DMS at the Commonwealth's premises; and

c. provide an operators' manual for all authorised users, including Commonwealth Authorised Users, to enable the DMS to be effectively operated.

3.3 The Commonwealth uses the DMS COD to:

a. understand the Contractor's implementation of the DMS;

b. determine any Commonwealth actions to implement, operate and manage the DMS; and

c. operate the DMS.

4. INTER-RELATIONSHIPS

4.1 The DMS COD is subordinate to the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP);

b. Integrated Support Plan (ISP); and

c. Technical Data Plan (TDP).

4.2 The DMS COD inter-relates with the following data items, where these data items are required under the Contract:

a. all data items derived from the Master Technical Data Index (MTDI); and

b. Data Accession List (DAL).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.2 Specific Content

6.2.1 DMS Overview

6.2.1.1 The DMS COD shall:

a. explain the purpose of the DMS;

b. describe the physical and logical architecture of the DMS to the extent that all parties need to understand in order to be able to connect with the DMS; and

c. list the computing equipment, including any special hardware or software, required by the Commonwealth Authorised Users of the DMS.

6.2.2 DMS Users

6.2.2.1 The DMS COD shall:

a. identify all users of the DMS, including Commonwealth Authorised Users;

b. detail the access rights of the Commonwealth Authorised Users at all locations to the DMS; and

c. detail the access rights of the Contractor and the Subcontractors to the DMS.

6.2.3 DMS Contract Data

6.2.3.1 The DMS COD shall:

a. list the types of electronic data that shall be available for both formal and informal communications via the DMS;

b. identify the processes for updating and maintaining the index of data within the DMS, including, if required under the Contract, the data defined by the DAL; and

c. list all the electronic data formats used in the DMS for which the Commonwealth Authorised Users will be provided access.

6.2.4 DMS Implementation and Management

6.2.4.1 The DMS COD shall:

a. list all software packages and necessary licences required to be supplied by the Contractor to enable the Commonwealth Authorised Users to access the electronic data in the DMS (both locally and remotely);

b. detail the procedures, which are required to be followed by the Commonwealth Representative, for the configuration of all necessary software that is required to provide full DMS functionality, including the administration procedures to control access rights;

c. detail the Configuration Management (CM) procedures used for the management of the DMS, including:

   (i) cross-platform document CM (eg, across mirrored sites, Contractor-to-Subcontractor, etc);

   (ii) electronic document management; and

   (iii) where these CM procedures are not covered by the Configuration Management Plan (CMP) delivered under the Contract;

d. detail any time restrictions, using Australian Eastern Standard Time, when DMS access may be limited (eg, DMS scheduled maintenance);

e. detail the system security aspects of the DMS, including:

   (i) controlled system access;

   (ii) system administration functions to control data access;

   (iii) file transfer protocols used;

   (iv) security classification of material that will be able to be released on the DMS;

   (v) procedures for the handling, management, transfer, release, etc, of classified material (if required);

   (vi) procedures for periodic back-up of electronic data, including a list of the data files that should be backed up, how the backup is performed, and how such files are recovered; and

(vii) any other requirements to ensure that the DMS appropriately addresses cyber security;

f. detail the system administration functions of the DMS, which Commonwealth Authorised Users may be required to perform, including a description of all routine administration that is to be carried out and the actions required to perform such administration;

g. detail the procedures to be used in formal and informal communications for the following:

(i) notification of actions between the Commonwealth Authorised Users (eg, delivery, receipt, approval, non-approval, comments, etc);

(ii) access and navigation of the DMS;

(iii) downloading, uploading, and viewing DMS data; and

(iv) how comments are to be provided for each document type (eg, native file formats, etc);

h. detail how the DMS manages the promotion of data from one status to the next (eg, working, draft submission, final submission, Approved, and Accepted);

i. detail the point-of-contact for assisting Commonwealth Authorised Users with problem resolution and to answer questions concerning the DMS; and

j. detail any other DMS miscellaneous issues.

6.2.5 DMS Training

6.2.5.1 The DMS COD shall detail the training plan for the DMS, including:

a. proposed venue(s);

b. proposed instructors;

c. participants;

d. length of the training session;

e. scheduled training date(s); and

f. training materials that will be provided.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-HSE-HSMP-V5.3

2. TITLE: HEALTH AND SAFETY MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Health and Safety Management Plan (HSMP) describes how the Contractor will manage Work Health and Safety (WHS) for the work to be performed under the Contract. Except in relation to work carried out on Commonwealth Premises, the HSMP does not address safety considerations in relation to the design, development, implementation or Verification and Validation (V&V) of either the Mission System or the Support System, as these requirements are addressed under the system safety program.

3.2 The Contractor uses the HSMP to:

a. identify the WHS requirements to be met in the performance of work under the Contract, including requirements for Commonwealth Premises, when applicable;

b. define, manage and monitor its program of activities in relation to WHS matters (including hazard and risk management consistent with WHS Legislation);

c. provide direction and guidance to the Contractor's team (including Subcontractors) in relation to WHS matters, their responsibilities and the processes to be used; and

d. ensure that all relevant persons, with a WHS duty in relation to the same matter, consult, co-operate and co-ordinate, in accordance with the WHS Legislation.

3.3 The Commonwealth uses the HSMP to:

a. gain assurance that the Contractor and the Commonwealth can meet their statutory obligations with respect to WHS;

b. gain assurance that the Contractor provides safe outcomes, in terms of safety risks to Commonwealth Personnel and other workers performing work under the Contract;

c. gain visibility of the Contractor's planning for WHS requirements of the Contract, and to provide a basis for evaluating performance in relation to those requirements; and

d. understand the Contractor's activities for co-ordination with the Commonwealth and Associated Parties, to assist the Commonwealth with discharging its WHS duties in relation to work performed under the Contract.

4. INTER-RELATIONSHIPS

4.1 The HSMP is subordinate to the Project Management Plan (PMP).

4.2 The HSMP inter-relates with the following data items, where these data items are required under the Contract:

a. Safety Data Sheets (SDSs), and

b. System Safety Program Plan (SSPP).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

SafetyMan	Defence Safety Manual
AS/NZS ISO 45001:2018	Occupational health and safety management systems—Requirements with guidance for use
	WHS Legislation and Codes of Practice approved under section 274 of the *Work Health and Safety Act 2011* (Cth).

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the HSMP shall summarise these aspects and refer to the other data item.

6.1.3 If a WHS Management System (WHSMS) is required under the Contract, and the WHSMS is accessible to the Commonwealth Representative and contains aspects of the information required by this DID, the HSMP shall summarise these aspects and refer to the WHSMS.

6.1.4 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 Relevant Legislation and Policy

6.2.1.1 The HSMP shall list the legislation relating to WHS, including the WHS Legislation, that is applicable to the work and the site(s) where the work is being, or will be, performed.

6.2.1.2 Where work is to be undertaken on Commonwealth Premises, the HSMP shall list the relevant Defence WHS policies and procedures, as identified in clause 9 of the SOW.

6.2.2 Work Health and Safety Management

6.2.2.1 The HSMP shall describe (including by reference to the WHSMS) how WHS matters applicable to Contract work and Contractor-controlled workplace(s) are managed, including:

a. within the Contractor's organisation, the names, positions and WHS responsibilities of all persons whose positions or roles involve specific WHS responsibilities;

b. the arrangements between the Contractor, Subcontractors, the Commonwealth and Associated Parties for the consultation, co-operation and co-ordination of activities required for compliance with WHS Legislation at workplaces used for the Contract;

c. the arrangements for managing, recording and reporting WHS incidents (including Notifiable Incidents);

d. any site-specific WHS rules (eg, including details of, or reference to, access controls and requirements for personal protective equipment), and the arrangements for ensuring that all persons at the workplace are informed of these rules;

e. processes for hazard identification (including by workplace WHS inspections), risk assessment, elimination and control measures, including safe work method statements where these are required by WHS Legislation;

f. the resources available for the provision of first aid, and the methods for ensuring that all persons at the workplace are informed of these resources;

g. the arrangements for the collection, and any assessment, monitoring and review, of the safe work method statements required by WHS Legislation; and

h. how WHS compliance and performance will be monitored (including through WHS audits), recorded and reported.

6.2.3 Work Health and Safety Management System

6.2.3.1 If a WHSMS is required under the Contract, the HSMP shall describe how the Contractor will establish and maintain a WHSMS that satisfies the requirements of clause 9.3.3 of the SOW.

6.2.3.2 If the Contract requires the WHSMS to be certified by an independent certification organisation, the HSMP shall state how this certification will be maintained.

6.2.4 Work on Commonwealth Premises

6.2.4.1 Where work is to be performed on Commonwealth Premises, the HSMP shall describe the Contractor's processes for participating in, or reporting to, any applicable site management committees, health and safety management committees or similar bodies.

6.2.4.2 Where work is to be performed on Commonwealth Premises, the HSMP shall describe, for Contractor and Subcontractor personnel, how work will be managed to meet Defence's WHS requirements, and not compromise Defence's duty of care, including:

a. provision of appropriate site induction and safety training;

b. monitoring of safe work performance personnel; and

c. safety evaluation of work performed by personnel.

6.2.5 Commonwealth Personnel

6.2.5.1 The HSMP shall describe the requirements for safety induction briefings and training to be provided to Commonwealth Personnel located on Contractor or Subcontractor premises, including any Commonwealth Premises being managed by the Contractor.

6.2.6 Management of Prescribed Activities and Complex Risks

6.2.6.1 The HSMP shall summarise the significant WHS hazards and risks inherent in the work to be performed under the Contract, including work involving Prescribed Activities.

6.2.6.2 The HSMP shall describe the approach to managing the hazards and risks identified in clause 6.2.6.1 where WHS management is inherently complex.

6.2.6.3 If a WHSMS is not required under the Contract and Contract work involves discrete activities for which WHS management is inherently complex and that would benefit from activity-specific planning, the HSMP shall include activity-based WHS plans in Annex B.

6.2.7 Emergency Plans

6.2.7.1 The HSMP shall outline the emergency plans to be maintained for the Contract, including any Commonwealth co-ordination or other arrangements required in an emergency.

6.2.8 Problematic Substances and Problematic Sources

6.2.8.1 Where work under the Contract will be performed on Commonwealth Premises, the HSMP shall include, at Annex A, details of the Problematic Substances and Problematic Sources that have been Approved for use at the Commonwealth Premises. Annex A shall include:

a. identification details for each Problematic Substance, sufficient to identify the applicable Safety Data Sheet;

b. locations, including any discrete sites or buildings within Commonwealth Premises, where the Problematic Substances and/or Problematic Sources will be located;

c. for Problematic Substances, the maximum quantities or volumes, as applicable, to be held at each location;

d. for Problematic Sources, the applicable ARPANSA source licence number;

e. the Approved purpose(s) for use; and

f. Approval details, including the Commonwealth Representative or authorised delegate's details, date of Approval, and related documents (eg, notices or minutes).

6.2.8.2 For Contract work performed in Australia but not performed on Commonwealth Premises, the HSMP shall include reference(s) to the location(s) within the Contractor's WHSMS, or otherwise, where Problematic Substances and Problematic Sources are detailed.

6.3 Annexes

Annex A: Problematic Substances and Problematic Sources Approved for use at Commonwealth Premises

Annex B: Activity-based WHS plans in accordance with clause 6.2.6.3 (if required).

DATA ITEM DESCRIPTION

1. **DID NUMBER: DID-PM-HSE-SDS-V5.3**

2. **TITLE: SAFETY DATA SHEET**

3. DESCRIPTION AND INTENDED USE

3.1 A Safety Data Sheet (SDS) provides information on the properties of Hazardous Chemicals, how they affect health and safety, and how to manage the Hazardous Chemical in the workplace. For Hazardous Chemicals, SDSs shall follow the code of practice approved under section 274 of the *Work Health and Safety Act 2011* (Cth) titled *Preparation of Safety Data Sheets for Hazardous Chemicals* (hereafter referred to as 'approved SDS code of practice'). In addition, SDSs are used by Defence to document the properties of Ozone Depleting Substances (ODSs), Synthetic Greenhouse Gases (SGGs) and Dangerous Goods that are not also classified as Hazardous Chemicals.

4. INTER-RELATIONSHIPS

4.1 The SDS inter-relates with the following data items, or annex to the Statement of Work (SOW), where these data items or annexes are required under the Contract:

a. the Health and Safety Management Plan, Project Management Plan or Support Services Management Plan, as applicable to the Contract for the purposes of recording Approved Substances; and

b. problematic substances and problematic sources in supplies (SOW annex);

c. Hazard Analysis Reports and Hazard Log; and

d. Safety Case Report or Materiel Safety Assessment, as applicable.

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

approved SDS code of practice	code of practice approved under section 274 of the Work Health and Safety Act 2011 (Cth) titled Preparation of Safety Data Sheets for Hazardous Chemicals.
GHS as defined in subregulation 5(1) of the *Work Health and Safety Regulations 2011* (Cth)	*Globally Harmonised System of Classification and Labelling of Chemicals*, Seventh revised edition, published by the United Nations as modified under Schedule 6 of the Work Health and Safety Regulations 2011 (Cth).

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions provided in the approved SDS code of practice.

Note: The approved SDS code of practice acknowledges that certain international SDS formats provide an equivalent standard of information to that required by the approved SDS code of practice. The intention is to permit some flexibility in the format of a SDS, while ensuring that the information contained in the SDS meets the requirements of the approved SDS code of practice.

6.1.2 Non-generic information may be submitted in the Contractor's preferred format.

6.2 Specific Content

6.2.1 The content of the SDS for Hazardous Chemicals shall follow the requirements of the approved SDS code of practice, which is available from the following internet address:

http://safeworkaustralia.gov.au/

6.2.2 Where the Contract requires an SDS for an ODS, SGG or Dangerous Good, which is not also a Hazardous Chemical, and therefore not required under the *code of practice*, the SDS shall include information that relates to the applicable regulatory requirements for those SDS sections that remain valid.

Note: If an SDS exists within the Australian ChemAlert database, then the requirements of this DID may be met if the applicable SDS is identified to the Commonwealth Representative by its unique record within that database.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-MEET-AGENDA-V5.3

2. TITLE: MEETING AGENDA

3. DESCRIPTION AND INTENDED USE

3.1 The Meeting Agenda provides information concerning the purpose, location and schedule of meetings convened for the purpose of discharging the requirements of the Contract.

4. INTER-RELATIONSHIPS

4.1 The Meeting Agenda is subordinate to the following data items, where these data items are required under the Contract:

Nil.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 Non-generic information may be submitted in the Contractor’s preferred format.

6.2 Specific Content

6.2.1 The Meeting Agenda shall incorporate agenda items and other input requested by the Commonwealth Representative and shall include:

a. the purpose or objective of the meeting;

b. the meeting location, date, starting time, and expected duration;

c. a chronological listing of each major discussion topic, including the person responsible to take the lead on the topic;

d. a list of individuals invited to attend the meeting, identifying their appointment and area of responsibility;

e. the identity of the chair person(s);

f. administrative information associated with the meeting including, where appropriate, access arrangements and the facilities available;

g. a list of documentation to be reviewed either for, or at, the meeting; and

h. any other information pertinent to the meeting.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-MEET-MINUTES-V5.3

2. TITLE: MEETING MINUTES

3. DESCRIPTION AND INTENDED USE

3.1 Meetings Minutes are recorded to ensure an accurate account of all discussions, decisions and actions arising from meetings between the Contractor and the Commonwealth.

4. INTER-RELATIONSHIPS

4.1 The Meeting Minutes are subordinate to the following data items, where these data items are required under the Contract:

Nil.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 Non-generic information may be submitted in the Contractor’s preferred format.

6.2 Specific Content

6.2.1 Main Body

6.2.1.1 Meeting Minutes shall include:

a. a list of attendees by name, title, appointment, organisation and contact phone number;

b. a page that provides for agreement to the minutes by the senior representatives (Commonwealth and Contractor) who attended the meeting, with the page to also show details of any representatives who disagree with the minutes;

c. the purpose of the meeting;

d. the actual agenda followed at the meeting;

e. a summary of the discussion, decisions, agreements and directions determined during the course of the meeting;

f. a list of action items agreed at the meeting;

g. other information required by the chairperson to be recorded in the minutes; and

h. details of proposed next meeting.

6.2.2 Action Items

6.2.2.1 The action item list shall be attached to the Meeting Minutes. The action item list shall reflect the current status of all action items, including those that are closed and completed.

6.2.2.2 Actions items shall be numbered either as follows or in the Contractor’s preferred format:

AI:PPPPPP: MMM:NNN

where -

AI stands for Action Item;

PPPPPP is the Project Name or Identification;

MMM is the Meeting Identifier; and

NNN is the Action Item Number.

6.2.2.3 The action item list shall include:

a. the party and individual responsible for undertaking the action item;

b. the timeframe for completing the action item; and

c. the history of the action item, including any transfer of responsibilities or changes in scope.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-MGT-AFD-V5.3

2. TITLE: APPLICATION FOR A DEVIATION

3. DESCRIPTION AND INTENDED USE

3.1 The Application for a Deviation (AFD) is required to document the request and evaluation of a deviation from, or the non-conformance with, an approved design or controlled process.

3.2 The Contractor uses the AFD to inform the Commonwealth of a proposed deviation or non-conformance.

3.3 The Commonwealth uses the AFD as the basis for review and evaluation of the application for a deviation or non-conformance made by the Contractor.

4. INTER-RELATIONSHIPS

4.1 The AFD is subordinate to the following data items, where these data items are required under the Contract:

Nil.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Departmental Quality Assurance Instruction 014, *Applying for a Deviation*

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions required by the form at Annex A to this DID (or equivalent electronic form) and, as applicable, the SOW clause for ‘Deliverable Data Items’ or the CDRL clause entitled ‘General Requirements for Data Items’.

6.2 Specific Content

6.2.1 General Requirements

6.2.1.1 An AFD is required to be submitted for all applications for a deviation or waiver from, or non-conformance with, an approved configuration management baseline or variation from an approved process.

6.2.2 Specific Requirements

6.2.2.1 All AFDs shall be prepared and requested through the submission of a Department of Defence form, as per the example included at Annex A.

6.2.2.2 The AFD form submitted by the Contractor shall, as a minimum, include applicable header information and the completion of all mandatory fields in Part 1 of the form.

Note: If the Contractor has access to the Defence Protected Network, the Contractor should use the electronic form SG002 available from the ‘e-Forms’ application (as updated from time to time). Alternatively, the embedded PDF version may be used instead of the form at Annex A.

Note: For Configuration Management purposes, one AFD may result in one or more ‘requests for variance’.

SG002.pdf

Annex:

A. Application for a Deviation

SG 002
Revised Nov 2020

Department of Defence

Application for a Deviation

Distribution
Original – Applicant's copy
Copy 2 – QAR
Copy 3 – Contracting Authority
Copy 4 – Ordering Authority
Copy 5 – DAA
Copy 6 – User authority

Applicant's reference no.		**Applicant requests decision by**
QAR authority reference no.	Date	(Negotiated with the contract authority)

Note: Policy and procedure for this process are issued as a Department Quality Assurance Instruction

1. Under no circumstances shall the applicant incorporate the deviation until approval from the appropriate contract authority has been received.
2. Approval of this deviation does not represent an authority to change the design nor to extend the non-conformance, of any other item in the contract.
3. The applicant must be a responsible officer of the supplier's, contractor's or subcontractor's organisation acceptable to the contract authority.

Part 1 – To be completed by applicant (Applicant includes, but is not limited to supplier, contractor and in-service provider)

*Denotes mandatory fields

*a. Name and address of applicant		*b. Contract or order no.
*c. Main item or assembly	d. Component	
*e. Relevant documentation (include issue no. and date)	f. Specification no.	g. Part identification no.
h. Batch lot or reference	*i. Period or quantity involved	
*j. Description of deviation (including supporting data – attach additional sheets if necessary). Refer to note 1.		

*k. Effect of deviation

Enter 'S' = Satisfactory, 'A' = Adversely affected, 'N' = Not known
If 'A' or 'N' is used, supporting documentation is to be attached.

□	Interchangeability	□	Function
□	Strength	□	Safety
□	Quality control	□	Life
□	Maintainability	□	Weight
□	Reliability	□	Performance
□	Environmental compliance		

Price variation
□ Yes □ No
□ If 'Yes', Increase □ Decrease
If 'Yes', supporting information is to be attached.

Delivery variation
□ Yes □ No
□ If 'Yes', Longer □ Shorter
If 'Yes', supporting information is to be attached.

Are there other critical factors affected which are not listed? □ Yes □ No
Is 'Yes', attach details

*l. Is permanent design change proposed?

□ Yes □ No If 'No', box n. is to be completed and box o. is to be completed where applicable.

*m. Applicant's design department (if applicable, attach agreed conditions)

Signature – (Design department)	Printed name	Appointment	Phone number	Date
n. Proposed corrective action for deviation application *(Attach additional sheets where necessary)*				
o. Proposed action to prevent recurrence *(Attach additional sheets where necessary)*				

*p. Agreed by applicant (All details are correct, and design department signatory is authorised)

Signature – Application	Printed name	Appointment	Phone number	Date

- When Part 1 is complete, forward both pages of the form and all attachments to Defence Quality Assurance Representative.

Applicant’s reference no.
QAR authority reference no.

Part 2 – To be completed by the Defence Quality Assurance Representative

a. General comments (including, based on objective evidence, that effects identified in Part 1 k. are verified)

b. Application referred to

User authority (in-service applications) □ and/or □Design acceptance authority

c. ‘For information’ copy provided to CA

□ Contract authority

d. QAR (Sections a. and b. above have been completed where applicable and details supplied in Part 1 are assessed as being complete and accurate)

Signature	Printed name	Appointment	Phone number	Date

Part 3 – To be completed by the User Authority *(Where applicable to in-service requirements)*

a. Application is

□ Endorsed Is restriction attached? □ Yes *(Attach response)* □ No □ Not endorsed *(Attach reasons)*

b. User representative

Signature	Printed name	Appointment	Phone number	Date

Part 4 – To be completed by the Design Acceptance Authority or delegate

a. Category	Category guidelines	
	Critical	Mission critical and/or threat to life
	Major	Significant issues that do not affect the mission or pose no threat to life.
	Minor	Lesser issues affecting configuration.

b. Need for permanent design change is agreed

□ Yes □ No

c. If ‘No’, return to agreed specification by

Date

d. Engineering Change Number (ECN) and Comments

e. Technical endorsement □ Endorsed □ Not endorsed

Signature	Printed name	Appointment	Phone number	Date

Part 5 – Approval — To be completed by the Contract Authority or representative

Contract authority or representative
(Cost and schedule implications have been accessed)

Application is: □ Approved □ Not Approved *(Attach reasons)*

(CCP and/or ECP action has been initiated)

□ CCP □ ECP □ N/A

Signature	Printed name	Appointment	Phone number	Date

Part 6 – To be completed by the Defence Quality Assurance Representative

Application close out (The details on this form have been recorded and copies dispatched as per distribution list)

Signature	Printed name	Appointment	Phone number	Date

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-MGT-QP-V5.3

2. TITLE: QUALITY PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Quality Plan (QP) describes the Contractor's strategy, methodology and processes for the management and control of Quality, commensurate with the nature and complexity of the requirements of the Contract, and the nominated Quality standards.

3.2 The Contractor uses the QP to:

a. define, manage and monitor its activities for meeting the Quality requirements of the Contract; and

b. ensure that those parties (including all Subcontractors) who are undertaking Quality-related activities understand their respective responsibilities, the processes to be used, and the time-frames involved.

3.3 The Commonwealth uses the QP to:

a. understand and evaluate the way that the Contractor proposes to meet the Quality requirements of the Contract, including any applicable ADF regulatory / assurance framework requirements;

b. assist with monitoring the performance of the Contract; and

c. identify and understand the Contractor's expectations of the Commonwealth with respect to the Quality requirements of the Contract.

4. INTER-RELATIONSHIPS

4.1 The QP is subordinate to the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP); or

b. Support Services Management Plan (SSMP).

4.2 The QP inter-relates with all other management plans required under the Contract.

5. APPLICABLE DOCUMENTS

5.1 The Quality standards nominated in the Contract and the following documents form a part of this DID to the extent specified herein:

ISO 10005:2018	Quality Management – Guidelines for Quality Plans
HB 90.9-2000	Software Development – Guide to ISO 9001:2000
AS/NZS ISO/IEC/IEEE 12207:2019	Systems and Software Engineering - Software Life Cycle Processes

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 The QP should be consistent with the guidelines given in ISO 10005:2018.

6.1.3 When the Contract has specified delivery of another data item that contains aspects of the required information, the QP shall summarise these aspects and refer to the other data item.

6.1.4 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The QP shall describe how the Contractor's Quality Management System (QMS) will be applied to fulfil the specific requirements of the Contract and shall describe or provide specific reference to a list of procedures to be used including any new procedures to be developed.

6.2.1.2 The QP shall describe the Contractor's Audit and review activities to be performed during all phases of the Contract.

6.2.1.3 The planned Quality-related activities (eg, tests, walkthroughs, reviews, etc) to be conducted shall be included in the QP. Alternatively, specific reference to where such information is contained can be provided.

6.2.1.4 If Software development, modification or update is required under the Contract, the Software Quality aspects shall:

a. be addressed in a Software quality plan, as an annex to the QP; and

b. meet the requirements of AS/NZS ISO/IEC/IEEE 12207:2019 paragraph 6.3.

6.2.1.5 The QP shall reference any international, national or industry specific standards, codes of practice and conventions adopted by the Contractor for ensuring conformance of the Contract's deliverables with the specified requirements.

6.2.2 Quality Organisation

6.2.2.1 The QP shall describe the Quality Management organisation, key appointments and functional relationships for managing Quality.

6.2.2.2 The QP shall identify the senior manager who has responsibility for the executive control of the Contractor's QMS, as it applies to the Contract.

6.2.2.3 The QP shall identify the resources and the allocated responsibilities and authorities for the Audit and review activities to be performed during the period of the Contract.

6.2.3 Subcontractor Requirements

6.2.3.1 The QP shall identify:

a. for each Approved Subcontractor, the scope of work to be undertaken and the system(s) in place to provide Quality Assurance of the work; and

b. for all other Subcontractors, how Quality Assurance will be achieved for the goods and services that they provide.

6.2.3.2 The QP shall include the Contractor's planned Audit and review activities for each Approved Subcontractor and any additional processes, which may be implemented to ensure that the relevant requirements of the Contract are flowed down to Approved Subcontractors.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-MGT-RP-V5.3

2. TITLE: REMEDIATION PLAN

3. DESCRIPTION AND INTENDED USE

3.1 A Remediation Plan sets out the Contractor's strategy, methodology, activities, resources and timeframes to address the underlying causes of the actual or potential problems, failures or breaches that have led to the requirement for the Contractor to submit a Remediation Plan under the Contract. The Remediation Plan sets out the Contractor's plan to:

a. rectify or prevent (as applicable) the actual or potential problems, failures or breaches;

b. avoid or mitigate the impacts of the actual or potential problems, failures or breaches; and

c. ensure that the actual or potential problems, failures or breaches (or any similar or related problems, failures or breaches) do not occur again.

3.2 The Contractor uses the Remediation Plan to:

a. describe the arrangements for managing the remediation activities, including in relation to Subcontractors;

b. provide direction to the Contractor's management team responsible for achieving the required remediation outcomes, as set out in clause 3.1;

c. ensure that those parties who are undertaking remediation activities understand their responsibilities, the processes to be used, and the time-frames involved; and

d. provide assurance to the Commonwealth that the underlying causes of the problems, failures or breaches will be remediated while ensuring that the other requirements of the Contract will continue to be satisfied.

3.3 The Commonwealth uses the Remediation Plan to:

a. evaluate and gain assurance that the Contractor's Remediation Plan will achieve the required remediation outcomes, as set out in clause 3.1;

b. provide a basis for monitoring and assessing the Contractor's performance in executing the Remediation Plan; and

c. identify any requirements for Commonwealth involvement in the Contractor's Remediation Plan.

4. INTER-RELATIONSHIPS

4.1 The Remediation Plan is subordinate to the following data items, where these data items are required under the Contract:

Nil.

4.2 The Remediation Plan inter-relates with the following data items, where these data items are required under the Contract:

a. Contract Work Breakdown Structure (CWBS);

b. Contract Master Schedule (CMS);

c. Support Services Master Schedule (SSMS); and

d. any plan that is related to the subject matter of the Remediation Plan.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.2 Specific Content

6.2.1 The Remediation Plan shall:

a. describe the actual or potential problem, failure or breach that led to the requirement for submission of the Remediation Plan;

b. describe the objectives of the Remediation Plan and the outcomes to be achieved in tangible, measurable terms and/or the exit criteria to be achieved (ie, in the context of the generic outcomes identified at clause 3.1), including identifying when these objectives and outcomes will be achieved;

c. identify the position responsible for achieving the objectives and outcomes identified pursuant to paragraph b above, including the name of the person filling the identified position;

d. set out the detailed steps that the Contractor will take to achieve the identified objectives and outcomes, including:

(i) the dates by which they will be completed;

(ii) any review points and/or decision points; and

(iii) the locations where the steps will be undertaken;

e. explain:

(i) why each of the steps is necessary and how these steps will achieve the identified objectives and outcomes in the proposed timeframes;

(ii) how the plan minimises the impact on existing Contract work (including schedule) and the Commonwealth; and

Note: Approval of the Remediation Plan does not grant relief for any contractual obligations in accordance with clause 4.4 of the COC.

(iii) where the plan does have an impact on existing Contract work and/or the Commonwealth, why these impacts are unavoidable;

f. if the actual or potential problem, failure or breach was identified or investigated by a Commonwealth or independent audit or other Commonwealth review activity (including as part of the Independent AIC Audit Program), address the recommendations from that audit or review activity, as notified by the Commonwealth Representative;

g. identify any assumptions or risks associated with the plan, and how those assumptions will be managed and the risks mitigated;

h. for each of the steps in the plan, identify:

(i) the resources required, including the people involved (by name), describing the activities that each person will be undertaking and identifying whether or not these people are involved in other Contract work;

(ii) any Subcontractors involved and describe the activities to be performed by these Subcontractors, including explaining how these activities will contribute to achieving the identified objectives and outcomes;

i. identify any inputs required to be provided by the Commonwealth to implement the steps (which, for clarity, shall be minimised and not include any additional requirements for GFM, GFF or GFS);

j. describe the reports that will be provided to the Commonwealth on the progress of the plan, which shall:

  (i) be provided on a monthly basis;

  (ii) identify the activities undertaken since the last report, the steps completed, any difficulties encountered, and the actions being taken to address the difficulties; and

  (iii) identify any envisaged changes to the Approved Remediation Plan and provide justification as to why these are considered necessary;

k. if applicable, describe any ongoing monitoring that will be implemented after all of the steps in the Approved Remediation Plan have been completed to ensure that the situation, which has led to the requirement for the Contractor to submit a Remediation Plan, does not recur; and

l. include any other information pertinent to the plan.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-MGT-SAC-V5.3

2. TITLE: SUPPLIES ACCEPTANCE CERTIFICATE

3. DESCRIPTION AND INTENDED USE

3.1 The Supplies Acceptance Certificate (SAC) provides for formal Acceptance of deliverables without prejudice to any remedies that the Commonwealth may have under the Contract when the deliverables do not conform to the requirements, or do not comply with the terms of the Contract.

3.2 The Contractor uses the SAC to detail the type and quantities of products being delivered to the Commonwealth for Acceptance.

3.3 The Commonwealth uses the SAC for formally acknowledging and recording the Acceptance of products from the Contractor.

4. INTER-RELATIONSHIPS

4.1 The SAC is subordinate to the following data items, where these data items are required under the Contract:

Nil

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions required by the form at Annex A to this DID (or equivalent electronic form) and, as applicable, the SOW clause for 'Deliverable Data Items' or the CDRL clause entitled 'General Requirements for Data Items'.

6.2 Specific Content

6.2.1 General Requirements

6.2.1.1 A SAC is required to be submitted with all products submitted to the Commonwealth for Acceptance in accordance with the Contract.

6.2.2 Specific Requirements

6.2.2.1 Except as otherwise specified in the Contract, all SACs shall be prepared using a Department of Defence form, as per the example included at Annex A.

6.2.2.2 The SAC form submitted by the Contractor shall include sections 'a' to 'k' completed as applicable, and section 'l', 'Contractor's Certification', signed by an authorised signatory of the Contractor, prior to offering the supplies to the Commonwealth.

Note: If the Contractor has access to the Defence Protected Network, the Contractor should use the electronic form SG 001 available from the 'e-Forms' application (as updated from time to time). Alternatively, the embedded PDF version may be used instead of the form at Annex A.

SG001 SAC May
2020

Annex:

A. Supplies Acceptance Certificate

SG 001
Revised May 2020

Department Of Defence

Supplies Acceptance Certificate

a. Contractor's reference number	b. CAPO or purchase order number	c. Project or ordering authority	d. Invoice number	e. Receipt voucher number

f. From *(full name and address of contractor and ACN)*	**Packaging details**				k. To *(Full name and address of consignee)*
	g. Number	h. Type	i. Gross weight	j. Package markings	

CAPO or order item number. 1	Class 2	Identity. part, catalogue or other reference number 3	Description of Supplies *(Include batch number, lot or serial number, deviation number and remarks)* 4	Qty ordered 5	Previously accepted 6	Offered today 7	Accepted today 8	Total to date 9	Balance due 10

l. Contractor's certification

The supplies detailed hereon and quantified in column 7 are hereby offered for Acceptance by the Commonwealth of Australia. It is hereby certified that the supplies conform in all respects of the conditions and requirements of Contract Number □ (Amendment Number □) *except as stated in the Attachment (delete words in italics if not applicable).* It is also certified that all other conditions and requirements of the Contract have been met in relation to the above - detailed Supplies.

Authorised signatory	Printed name
Position held	Date

m. **Commonwealth's Acceptance**

The Supplies detailed hereon and quantified in Column 8 have been Accepted without prejudice to the Commonwealth's remedies under the Contract in the event that the Supplies do not conform in all respects with the conditions and requirements of the Contract.

Authorised signatory	Printed name
Appointment	Date

n. **Commonwealth's Reference or file number**

o. **Is CAPO or order complete?** □ Yes □ No

p. **Recommended Distribution**

Original – To be forwarded with payment claim
One Copy – To be forwarded by Contractor with supplies
One Copy – To be retained by Commonwealth's authorised signatory
One Copy – To be forwarded to project or ordering authority
One Copy – To be retained by Contractor

Department Of Defence

Supplies Acceptance Certificate

Explanation

The boxes and columns on the Supplies Acceptance Certificate form are to be completed as follows:

Box a **Contractor's Reference Number**. Supplier's number to record an internal file / job number.

Box b **CAPO or purchase order number**. Relevant Contract / purchase order number.

Box c **Project or ordering authority**. The Defence authority that placed the order, also referred to as the procurement authority.

Box d **Invoice number**. The invoice number as supplied by the supplier, when applicable.

Box e **Receipt voucher number**. For use by the receiving officer at the point of receipt.

Box f **From**. The full name, address, and Australian Company Number (ACN) of the supplier, as shown in the Contract.

Boxes g to j **Packaging details**. Enter relevant information.

Box k **To**. The address to which the supplies are to be delivered, as shown in the Contract.

Column 1 **CAPO/Order Item No**. The item number as listed in the contract.

Column 2 **Class**. The first four numbers of the NSN, or the Class number from the 'Classes of Supply' group for the item (see box at right).

Column 3 **Identity, part, catalogue or other reference number**. The remaining nine numbers of the NSN, and/or relevant manufacturer code and item information to identify the item ordered.

Column 4 **Description of Supplies**. A description of the item(s) as shown in the Contract. Reference is to be made to relevant details (ie, batch or lot numbers, serial numbers, and approved Application(s) for a Deviation (including variances, if applicable)).

Column 5 **Qty ordered**. The total number of items ordered under this contract item number.

Column 6 **Previously accepted**. The total number of items ordered under this contract item number, and identified in column 3, which have been Accepted prior to the raising of this SAC.

Column 7 **Offered today**. The number of items ordered under this contract item number, and identified in column 3, which are being submitted by the Contractor for Acceptance vide this SAC.

Column 8 **Accepted Today**. The number of items ordered under this contract item number, and identified in column 3, for which the accepting authority is satisfied, meet the requirements of the Contract and has agreed to Accept on this SAC.

Column 9 **Total to date**. The number of items ordered under this contract item number, and identified in column 3, which have previously been Accepted including the number Accepted vide this SAC.

Column 10 **Balance due**. The number of Items ordered under this contract item number, and identified in column 3, which are still outstanding.

Classes of Supply based on the NATO conventions (from Land Warfare Doctrine 4-1, Supply Support):

Class 1 **Subsistence Items**. Foodstuffs, combat rations and packaged water.

Class 2 **General Stores**. Clothing, tents, tarpaulins, minor equipment, stationery, administrative and housekeeping items.

Class 3 **Petrol, Oils and Lubricants**.

Class 4 **Construction Items**. Construction materials, engineer stores and defence stores.

Class 5 **Ammunition**. All types of ammunition and explosive ordnance.

Class 6 **Personal Demand Items**. Personal items and canteen stores.

Class 7 **Principal Items**. Major items of equipment such as vehicles and weapons, major assemblies and included accessories. Items usually have a serial number.

Class 8 **Medical and Dental Stores**. Pharmaceutical items, medical and dental equipment, and repair parts.

Class 9 **Repair Parts**. Repair parts for maintenance support.

Class 10 **Material Support to Non-military Programs**. Item to support non-government program such as a UN mission or for economic development. Items should be segregated where possible.

Box l **Contractor's certification**. The supplier's authorised representative is required to complete this box, signifying that the Supplies meet the requirements of the Contract in all respects, with the exception of any listed approved production permits and/or concessions.

Box m **Commonwealth's Acceptance**. By signing this box the Accepting Authority provides legal Acceptance of the Supplies on behalf of the Commonwealth.

Box n **Commonwealth's Reference or file number**. Reference to an official file or other document that can at a later date provide traceability of events.

Box o **Is this CAPO/Order complete?** Enter whether the contract is complete when the deliveries of Supplies listed on this SAC have been made.

Box p **Recommended Distribution**. Distribution of the completed SAC by the accepting authority, as required by the procurement authority.

Boxes and columns are not to be left blank on any line of entry on the form. Where it is not necessary to enter information N/A (Not Applicable) is to be inserted.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-RVW-PACKAGE-V5.3

2. TITLE: REVIEW PACKAGE

3. DESCRIPTION AND INTENDED USE

3.1 The purpose of Review Package is to allow the Contractor and Commonwealth Representative to prepare for System Reviews in order to gain maximum value from the reviews.

3.2 The Contractor uses the Review Package to convey the set of information that supports the objectives of the review.

3.3 The Commonwealth uses the Review Package, along with other data items specifically identified in the CDRL, to assist with confirming that the System Review objectives have been met.

4. INTER-RELATIONSHIPS

4.1 The Review Package is subordinate to the following data items, where these data items are required under the Contract:

a. System Review Plan (SRP);

b. Quality Plan (QP); and

c. any other plan that provides details of System Review activities under the Contract.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’ or as otherwise Approved by the Commonwealth Representative.

6.1.2 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 The Review Package shall include information to be reviewed and discussed at the specific System Review, including:

a. documentation that is necessary to show that the objectives of the System Review have been satisfied;

b. presentation material;

c. all relevant documents not previously delivered and needed to meet the objectives of the System Review;

d. status of action items from previous System Reviews;

e. where applicable to the System Review, status of measurement data (eg, design maturity metrics and Technical Performance Measures); and

f. where applicable to the System Review, current configuration status along with any identified discrepancies in Configuration Baselines.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-PM-TRANS-CTXP-V5.3

2. TITLE: CONTRACTOR TRANSITION PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Contractor Transition Plan (CTXP) describes the Contractor's plans, methodologies and processes for meeting the Transition requirements of the Contract, and establishes the ground rules for the transfer of management responsibilities from the developing organisations (ie, Contractor and Subcontractors) to the respective support organisations.

3.2 The Contractor uses the CTXP to:

a. define, manage and monitor the Contractor's Transition program;

b. ensure that those parties (including Subcontractors) who are undertaking Transition activities understand their respective responsibilities, the processes to be used, and the time-frames involved;

c. plan for and coordinate Transition activities with Associated Parties that will provide support for the Materiel System including, when applicable, the Contractor (Support); and

d. define and establish the Contractor's involvement in the Commonwealth's Transition program.

3.3 The Commonwealth uses the CTXP to:

a. understand and evaluate the Contractor's approach to meeting the Transition requirements of the Contract;

b. define and establish the Commonwealth's involvement in the Contractor's Transition program, including the monitoring of the Contractor's program;

c. enable the timely provision of information to In-Service organisations to allow them to plan for the delivery of the Mission System and the Support Resources; and

d. provide input to the Commonwealth Representative's own Transition planning.

4. INTER-RELATIONSHIPS

4.1 The CTXP is subordinate to the following data items, where these data items are required under the Contract:

a. Project Management Plan (PMP).

4.2 The CTXP inter-relates with the following data items, where these data items are required under the Contract:

a. Australian Industry Capability (AIC) Plan;

b. other applicable AIC-related plans (eg, Supply Chain Management Plan (SCMP) and Defence-Required Australian Industry Capability (DRAIC) Plan (DRAICP));

c. System Review Plan (SRP);

d. Verification and Validation Plan (V&VP);

e. Contract Master Schedule (CMS);

f. Support System Description (SSDESC);

g. Support System Technical Data List (SSTDL);

h. Australia and New Zealand (ANZ) Subcontractor Technical Data List (ASTDL);

i. Recommended Spares Provisioning List (RSPL);

j. Packaging Provisioning List (PACKPL);

k. Support and Test Equipment (S&TE) Provisioning List (S&TEPL); and

l. Training Equipment List (TEL).

4.3 When this Contract is linked to a Contract (Support), the CTXP inter-relates with the Contract (Support) Phase In Plan (PHIP) and Ramp Up Management Plan (RUMP).

5. APPLICABLE DOCUMENTS

5.1 The following document forms a part of this DID to the extent specified herein:

DI-IPSC-81429A	Software Transition Plan (STrP)

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the CTXP shall summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

6.2.1 General

6.2.1.1 The CTXP shall describe the objectives, scope, constraints, and assumptions associated with the Contractor’s (and Subcontractor’s) Transition activities. Any risks associated with the Contractor’s Transition program shall be documented in the Risk Register; however, the CTXP shall describe the risk management strategies associated with any global, Transition-related risks.

6.2.2 Transition Organisation

6.2.2.1 If different from that described in the PMP, the CTXP shall describe the Contractor’s organisational arrangements for Transition, including:

a. the Contractor’s and Approved Subcontractor’s organisations and management structures, showing how these arrangements integrate into the higher-level management structures and organisations for the Contract;

b. the interrelationships and lines of authority between all parties involved in the Contractor’s Transition activities; and

c. the responsibilities of all parties involved in the Contractor’s Transition activities, including the identification of the individual who will have managerial responsibility and accountability for meeting the Transition requirements of the Contract.

6.2.3 Transition Overview

6.2.3.1 The CTXP shall provide an overview of the Contractor’s program of activities for transitioning from a development and production environment to a support environment for the Supplies, including:

a. the major activities to be undertaken, when, and by whom;

b. the integration of Subcontractors into the Contractor’s Transition activities;

c. significant activities of the Transition Working Group (TXWG);

d. the interfaces between the Transition activities and the Systems Engineering, Verification and Validation, and Integrated Logistics Support programs;

e. the processes to be employed by the Contractor for undertaking Transition and, if applicable, ramping up to provide support under the Contract (Support);

f. for any new or modified procedures for Transition, an overview of the scope of the new or modified procedures and the responsibilities and timeframes for developing and approving these procedures;

g. if applicable, the Transition activities required to coordinate with the Phase In and Ramp Up activities of the Contractor (Support) and Subcontractors (Support);

h. the expectations of the Contractor with respect to the Commonwealth;

i. the proposed role of the Contractor in assisting the Commonwealth in integrating the Support Resources into the existing Commonwealth infrastructure; and

j. the Contractor's proposed methodology for ensuring that the activities of the Contractor and the Commonwealth are coordinated, including proposed planning and coordination meetings.

6.2.4 Support Responsibilities

6.2.4.1 The CTXP shall identify:

a. each subsystem or component of the Mission System and Support System Component, that is to be supported;

b. the organisations and their support responsibilities for each of the subsystems and components identified under clause 6.2.4.1a, including responsibilities for engineering support, maintenance support, supply support and training support; and

c. the sustainment-related DRAICs and other Industry Capabilities identified as Australian Industry Activities (AIAs), which have been created (in whole or in part), enhanced or maintained within Australian Entities under the Contract, including their relationship to the support of the subsystems and components identified under clause 6.2.4.1a.

6.2.4.2 The information required by clause 6.2.4.1 may be provided as an annex to the CTXP.

6.2.4.3 The identification of components under clause 6.2.4.1a needs sufficient detail to allow each unique set of support responsibilities to be identified in response to clause 6.2.4.1b.

6.2.5 Detailed Transition Activities

6.2.5.1 Using the information derived for clause 6.2.4.1, the CTXP shall detail the Contractor's and Subcontractors' specific activities associated with transitioning from a development and production environment to a support environment for the Supplies, specifically addressing the Contractor's methodology and timeframes for implementing appropriate:

a. engineering support arrangements, including data management and configuration management;

b. maintenance-support arrangements;

c. supply-support arrangements;

d. training and training-support arrangements; and

e. subcontract arrangements.

6.2.5.2 In addressing the requirements of clause 6.2.5.1, the CTXP shall address:

a. the implementation schedule (with this schedule to be included within the CMS);

b. planning and coordination of significant meetings and reviews including, when required under the Contract:

(i) the meetings of the TXWG including, if applicable, the involvement of the Contractor (Support) in applicable Mandated System Reviews; and

(ii) the conduct of the Transition Requirements Review (TXRR);

c. the personnel requirements for both the Contractor and Subcontractors to enable the implementation schedule to be met, including:

(i) the source from which these personnel will be provided; and

(ii) the training to be provided to enable these personnel to undertake their responsibilities during Transition and, if applicable, the Contract (Support);

d. the Facilities, S&TE, and computer-support requirements needed by both the Contractor and Subcontractors to facilitate the transfer of Supplies, if not otherwise identified under the Contract;

e. if applicable, how the Contractor will coordinate with the Contractor (Support) for the development of the procedures to be employed by the Contractor (Support) and Subcontractors (Support) to enable Transition; and

f. any further Transition-related activities required to enable close out of the Contract.

6.2.5.3 In addressing the Transition activities associated with Software, the CTXP shall address the requirements of paragraphs 3-8 of DI-IPSC-81429A.

6.2.5.4 The CTXP shall describe, explicitly or by reference to another document (including any database) that has been delivered to the Commonwealth:

a. the items (such as Support Resources, including Technical Data) to be delivered to the respective support organisations and the proposed recipients;

b. the delivery, installation and checkout of the support environments being implemented by each of the respective support organisations (ie, Commonwealth, Contractor, Subcontractors, Contractor (Support) and Subcontractors (Support), as applicable, in accordance with the Contract and the Contract (Support));

c. the Transition of the sustainment-related DRAICs and other applicable AIAs (including any that have a dual acquisition and sustainment function) as part of establishing the support environment for the Supplies, including any DRAICs or other AIAs that were only partially implemented under the Contract and for which the full implementation is planned to occur under the Contract (Support); and

d. the timeframes in which Commonwealth personnel will be required by the Contractor (eg, for Training) to enable the Contractor to successfully Transition the Mission System and other Supplies to the Commonwealth.

6.2.6 Transition Support for Commonwealth Units

6.2.6.1 If the Contract requires the Contractor to provide specialist personnel to directly support the Transition-related activities of Commonwealth units, the CTXP shall:

a. outline the range and scope of Transition support activities;

b. identify each Commonwealth unit to be supported, the objective or the criteria for completion, and the activities involved;

c. for each Contractor and/or Subcontractor person or work team required, identify:

(i) the numbers and skills of the personnel;

(ii) the duration of the support activity for each Commonwealth unit; and

(iii) the work location (eg, on-site with the Commonwealth unit or remote); and

d. identify any Training requirements (eg, for Defence information systems).

6.2.7 Transition Register

6.2.7.1 The CTXP shall describe the Transition Register used by the Contractor for recording the Transition activities, tasks, risks and issues.

6.2.7.2 The Transition Register shall be a separate entity from the CTXP (due to the dynamic nature of the content of the Transition Register).

6.2.7.3 The Transition Register shall, for each Transition activity, include:

a. a unique activity identification number;

b. a brief description of the activity, including reference to any related clauses in the Contract and an outline of the tasks needed to perform the activity;

c. the priority of the activity;

d. details of the individual in the Contractor’s organisation responsible for the activity;

e. details of other parties involved in the activity, including the identification of any Commonwealth parties that are external to the Project Office;

f. the timeframes for achieving the activity;

g. the action status of the activity (eg, not started, in progress, completed);

h. the associated risks, with cross-references to the Risk Register; and

i. details of any issues to be resolved / action items associated with the activity, including the timeframes for those action items and the party to whom the action items have been assigned.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-SSM-ISSMP-V5.2

2. TITLE: IN-SERVICE SECURITY MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The In-Service Security Management Plan (ISSMP) describes the Contractor's plan for meeting the system security requirements for the in-service phase for those products that are Products Being Supported (or will become Products Being Supported under an associated or linked Contract (Support) when this data item is being developed under a Contract (Acquisition)) and that:

a. could be susceptible to security vulnerabilities that may affect the Commonwealth's security obligations and compliance requirements (as would be determined by a competent contractor acting reasonably in making such a determination);

b. are the subject of, or included within the scope of, a Security Authorisation, including in relation to physical security, Emanation Security (EMSEC), Information and Communications Technology (ICT) security, cyber security, and personnel security (but, for personnel security, only in relation to Contractor Personnel operating, or maintaining or upgrading a Security System-of-Interest (SSoI) or an associated Target of Evaluation (ToE)); and/or

c. are required by the Contractor to undertake the system security services (eg, Software such as Splunk®).

3.2 The Contractor uses the ISSMP to:

a. define, manage and monitor the Contractor's system security and related activities for the in-service phase and to demonstrate how the associated security objectives applicable to the in-service phase will be achieved, including managing any Security Authorisations that will require periodic revalidation during the in-service phase;

b. ensure that those parties (including the Commonwealth and Subcontractors) performing system security activities during the in-service phase understand their respective responsibilities, the processes to be used, and the time-frames involved, including in relation to:

(i) responding to cyber incidents;

(ii) ensuring business continuity and disaster recovery; and

(iii) continuous monitoring; and

c. demonstrate that it has the capability and capacity to meet its system security responsibilities for the SSoIs / ToEs and other security-related Support System Products during the in-service phase.

3.3 The Commonwealth uses the ISSMP:

a. to understand and evaluate the Contractor's approach for meeting the system security requirements of the Contract for the in-service phase;

b. to gain assurance that the Contractor has a sound system security program in place that complies with applicable Government and Defence security requirements and policies and that will satisfy the objectives of the program;

c. to plan the integration of the Contractor's system security activities for the in-service phase with the Commonwealth's security activities, particularly in relation to interacting with the respective security authorities;

d. as an input into the Commonwealth's own planning, particularly in relation to liaising with the applicable security authorities for each SSoI; and

e. as one of the suite of cyber security artefacts provided to the relevant Defence authorities as part of obtaining and/or maintaining the required ICT/cyber Security Authorisations for a SSoI.

4. INTER-RELATIONSHIPS

4.1 The ISSMP is subordinate to the following data items, where these data items are required under the Contract:

a. Support Services Management Plan (SSMP).

4.2 The ISSMP inter-relates with the following data items, where these data items are required under the Contract:

a. the security-related data items required under the Contract (other than those identified under clause 4.1);

b. Materiel System Security Management Plan (MSSMP) governing the acquisition phase; and

c. the plans and Engineering Change Proposal(s) (ECP(s)) associated with any Major Changes.

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Note to drafters: Amend the list of Applicable Documents to suit the Contract. Do not include documents that are included within the 'Governing Security Documents'.

Governing Security Documents	(see the Glossary for the definition of this term)
ANP4605	Navy Cyberworthiness
	National Institute of Standards and Technology (NIST), 'Cybersecurity Framework (CSF)', Version 2.0, February 26, 2024
AS/NZS ISO 31000:2018	Risk Management – Principles and Guidelines
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1, September 2012
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018
NIST SP 800-53A	Assessing Security and Privacy Controls in Information Systems and Organizations: Building Effective Assessment Plans, Revision 5, January 2022
	ACSC Publication, 'Strategies to Mitigate Cyber Security Incidents', February 2017
	ACSC Publication, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', February 2017
	ACSC Publication, 'Guidelines for System Monitoring', September 2023
	ACSC Publication, 'Guidelines for Security Documentation', September 2023
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection – Information security management systems – Requirements

ISO/IEC 27032:2023	Cybersecurity – Guidelines for internet security
ISA/IEC 62443 series	Security for Industrial Automation and Control Systems
AS/NZS HB 231: 2004	Information Security Risk Management Guidelines
Defence ICT/Cyber SCRM Framework	The Defence ICT/Cyber Procurement Supply Chain Risk Management Framework, October 2020
SCRM Procurement Tool	ICT/Cyber Procurement Supply Chain Risk Assessment (SCRA) Tool, version 1.0, April 2021
Form XP 188	Security Report

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 When the Contract has specified delivery of another data item that contains aspects of the required information, the ISSMP should summarise these aspects and refer to the other data item.

6.1.3 The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

6.2 Specific Content

Note: References to 'Contract' in this DID mean the Contract (Support) when this data item is being developed under an acquisition contract.

6.2.1 Overview

6.2.1.1 The ISSMP shall provide an overview of the security-related Services for each SSoI to be provided under the Contract, including:

a. defining the scope and purpose of the ISSMP;

b. describing the scope and objectives of the system security program for the in-service phase, including:

(i) providing an overview of each SSoI and, if applicable, each ToE, and identifying other applicable Support System Products from a security perspective; and

(ii) providing an overview of any shared responsibilities for system security between the Contractor and the Commonwealth (eg, in relation to responding to cyber incidents, ensuring business continuity and disaster recovery, and continuous monitoring);

c. identifying and describing the nature and significance of the security risks and threats that will be managed through the ISSMP; and

d. describing any constraints, assumptions and risks associated with the program.

6.2.1.2 The ISSMP shall provide a list of key stakeholders involved with the system security program for the Contract, including:

a. System Owner;

b. Security Authorisation authorities; and

c. where DESE supported under the Contract is either integrated into, or installed onto, Defence systems and platforms, the in-service agencies responsible for managing and supporting those systems and platforms.

6.2.1.3 The ISSMP shall describe the mechanisms by which the general requirements for security documentation, as set out in the Information Security Manual (ISM), will be satisfied, including (for example):

a. Control ISM-0188: “Security documentation is reviewed at least annually and includes a ‘current as at [date]’ or equivalent statement”; and

b. Control ISM-1602: “Security documentation, including notification of subsequent changes, is communicated to all stakeholders”.

6.2.2 System Security Organisation and Roles

6.2.2.1 The ISSMP shall describe the organisations and the roles of the organisations involved with the system security program for the Contract, including:

a. within the Contractor’s organisation;

b. Subcontractors, including original equipment manufacturers; and

c. Associated Parties, including Defence agencies, regulatory authorities and other Commonwealth Contractors, as applicable.

6.2.2.2 The ISSMP shall identify the technical / design support network of organisations, including:

a. identifying the Subcontractors and other companies, which provide technical advice for security activities; and

b. describing the nature and scope of the technical advice to be provided.

6.2.2.3 The ISSMP shall identify the qualifications and training required by persons filling any Key Staff Positions for the system security program for the Contract.

6.2.2.4 The ISSMP shall provide details of the Contractor’s security team that is dedicated to the provision of security-related Services for each SSoI / ToE, including numbers and skills.

6.2.3 System Security Risk Management

6.2.3.1 The ISSMP shall describe the risk management processes to be applied to the Contractor’s system security program for the Contract, cross-referring to the risk management elements of the Approved SSMP[1] and the applicable elements of the Approved ADF regulatory / assurance plans as appropriate, including:

a. the processes to be used to identify system security risks;

Note to drafters: The following clause refers to the CASG Risk Management Product Matrix included at Annex A to this DID. This enables a 5x5 matrix to be employed for the purposes of project or product risk management using the Predict! tool. The Security Authorisation process, however, requires the use of a 6x6 matrix in accordance with the DSPF. Drafters should amend the following clause and Annex A to suit their contract-management circumstances (ie, to select a risk matrix that will result in the least work for the contract-management team, either translating into the DSPF 6x6 matrix if the CASG matrix is retained, or translating into Predict! if the following clause and Annex A are amended to incorporate the DSPF matrix).

b. the processes to be used for analysing, assessing and evaluating system security risks, including the specific assessment criteria to be used, cross-referring to the CASG Risk Management Product Risk Matrix at Annex A in relation to assessing risks to security and cyber;

c. the risk register(s) to be used for recording each system security risk (eg, Security Risk Management Plan (SRMP) and Cyber Supply Chain Risk Plan (CSCRP)), including its attributes, evaluation and treatment(s);

d. the processes to be used to determine the specific risk treatment strategies to be employed, particularly the application of risk controls (eg, as per the ISM); and

e. the mechanisms to be used to keep the Commonwealth Representative apprised of any changes to system security risks.

6.2.3.2 The ISSMP shall describe how security requirements will be incorporated into the Contractor’s supply chains to address cyber security supply chain risks (eg, using the ICT/Cyber Procurement SCRA Tool in accordance with the Defence ICT/Cyber SCRM Framework), cross-referring to any CSCRP required under the Contract.

[1] An Approved SSMP is unlikely to exist if the ISSMP is developed under an acquisition contract.

6.2.4 System Security Program Activities – General

Note: In relation to security monitoring and testing, clause 6.2.7 of this DID provides additional requirements that the ISSMP must address.

6.2.4.1 The ISSMP shall describe the Contractor's processes for undertaking the security-related Services for the SSoIs, as required by the Contract, including:

a. an overview of the methodology to be employed to achieve the objectives, outcomes and requirements set out in clause 3 of this DID;

b. describing how the applicable standards and other documents, referred to under clause 5, will be adapted to the Contractor's system security program; and

c. describing how each of the system security requirements set out in the Contract will be undertaken, including when and by whom, and the processes and tools to be employed.

6.2.4.2 The ISSMP shall describe any simulation and other tools, instruments, items of equipment, Software, test facilities and any other major elements that will be required to satisfy the security requirements of the Contract.

6.2.4.3 The ISSMP shall contain a high-level schedule indicating key activities, events and milestones for the system security program for the Contract, including in relation to physical security, EMSEC, ICT security and cyber security.

6.2.5 Incident Response Plan

Note: A security incident is a suspicious approach, event or action (whether deliberate, reckless, negligent or accidental) that:

a. fails to meet the expected outcomes of Defence security as outlined in the DSPF;

b. compromises Defence's protective security arrangements; and

c. results in (or has the potential to result in) loss, damage, harm or disclosure to Defence information, assets and/or personnel.

6.2.5.1 The ISSMP shall document the Contractor's plan for responding to security incidents ('**Incident Response Plan**') pertaining to each SSoI, including:

a. the roles and responsibilities of all personnel (Commonwealth, Contractor and Subcontractors) during an incident, including:

(i) system users, system support staff, system administrators, etc based on the incident type;

(ii) the identification of the position that will have ultimate responsibility for the operational management of an incident; and

(iii) the authorised methods of communication between the various parties, particularly between the Commonwealth and the Contractor and between the Contractor and its Subcontractors;

b. the authorities within the Contractor's organisation responsible for initiating:

(i) a formal (administrative) investigation; and

(ii) a police investigation of an incident;

c. the minimum level of Training for investigators, users and system administrators (eg, Cert IV in Forensics and Security Investigations);

d. guidelines on what situations and scenarios constitute an incident;

e. the goals and objectives of the incident response based on incident type;

f. the types of incidents likely to be encountered and the expected response to each type (eg, malware, system intrusion, data compromise, and unauthorised system change), including the processes for threat containment and eradication for each incident type;

g. the steps necessary to ensure the availability of critical systems during an incident;

h. management of the vulnerability exploited within the compromised system elements;

i. system contingency measures and/or relationships to other response processes and procedures to ensure the continued safety and operational effectiveness of the SSoI;

Note: In accordance with DSPF Principle 77, "Once the risk of immediate harm has been effectively managed, a Security Report must be submitted to SICC [Security Incident Coordination Centre] via the Security Report within 24 hours of the incident occurrence or discovery". A copy of this report is also to be provided to the Commonwealth Representative at the same time, including any supporting information.

j. incident reporting mechanisms, including both internally (eg, using a Form XP 188) and externally to relevant operational authorities (eg, the Australian Cyber Security Centre) and including those parties that need to be informed in the event of a security incident;

k. criteria for investigation into a security incident involving external entities (eg, as could be requested from a law enforcement agency, the Australian Cyber Security Centre or other relevant authority); and

l. the steps necessary to ensure the integrity of evidence for use in investigation.

6.2.5.2 The Incident Response Plan shall detail the management of, and contents of, the Incident Register to be used to capture the necessary details associated with each security incident, including fields to allow the tracking of the following information:

a. the date the incident was discovered;

b. the date the incident occurred;

c. a description of the incident, including the people and locations involved;

d. the action taken;

e. lessons identified;

f. to whom the incident was reported; and

g. whether or not any further investigations were undertaken.

6.2.5.3 The Incident Response Plan shall describe the intervals and process for testing incident response and recovery capability, and for confirming that the plan remains fit for purpose.

6.2.6 Business Continuity and Disaster Recovery Plan

6.2.6.1 The ISSMP shall document the Contractor's plan for ensuring the continued operation of each SSoI (or critical elements thereof) in response to either:

a. a security incident or a series of security incidents that have a high likelihood of compromising Defence operations involving the SSoI; or

b. a disaster that would compromise Defence operations involving the SSoI,

('**Business Continuity and Disaster Recovery Plan**' or '**BCDRP**')

Note: Different elements of an SSoI may involve different considerations in relation to business continuity and/or disaster recovery. Where applicable, the BCDRP should identify these differences so that it is clear exactly what will occur for the different elements in relation to business continuity and disaster recovery.

6.2.6.2 The BCDRP shall:

a. identify the management structures and the roles and responsibilities of applicable personnel (Commonwealth, Contractor and Subcontractors) associated with business continuity and/or disaster management and recovery, including the relationships with incident response management;

b. identify the critical services, functions and assets associated with each SSoI in the context of Defence operations, cross-referring to the Business Impact Levels (BILs) in the Security Classification and Categorisation Guide (SCCG) at Attachment J to the Contract;

c. categorise the identified elements according to their priority for maintaining continuity of operations and/or for recovery after a disaster;

d. define the maximum acceptable outage time for the critical services and functions and the associated recovery time objective in the context of the maximum acceptable outage time;

e. describe credible scenarios that could cause a system interruption, such as a natural disaster, civil disturbance, major ICT failure or major cyberattack;

f. describe the strategies for maintaining business continuity in response to the identified scenarios and in the context of the prioritised services, functions and assets;

g. describe the strategies for disaster management and recovery in the context of the identified scenarios, the prioritised services, functions and assets, and the recovery time objectives;

h. describe the processes to be implemented to ensure that personnel are prepared for potential system disruptions that could compromise Defence operations using the SSoI, including, for example, the conduct of business continuity and disaster recovery exercises and testing;

i. describe the processes for activating and managing the business continuity and/or disaster management and recovery mechanisms and activities, including:

(i) identifying the likely triggers;

(ii) describing the potential requirements for relocating systems, equipment, personnel and other items during a disaster, including ensuring the safety of personnel as the highest priority;

(iii) describing the associated internal and external communications;

(iv) describing the coordination with other interested parties throughout a disruption; and

(v) describing the likely temporary arrangements to be implemented during a disruption;

j. describe the systems, processes and personnel necessary to return business / mission activities from the temporary measures adopted during the disruption to normal operations;

k. describe the processes for data backup and recovery to ensure that minimal data is lost in the event of an interruption to the SSoI and the SSoI can be recovered within the required timeframes, including the use of remote locations for data backup, testing backup and restoration processes, and security considerations for the data backups;

l. describe any other elements of the BCDRP (eg, employee contact lists, vital records, and alternate site operations, resources and transportation); and

m. describe the implementation and maintenance of communication and warning procedures, including those necessary to manage the incident response and coordination with other interested parties throughout a disruption.

6.2.6.3 The BCDRP shall describe the processes for maintaining capabilities and response readiness, such as table top exercises, and for confirming that the plan remains fit for purpose.

Note to drafters: The following requirements may not be applicable to any SSoI or to the Contractor's responsibilities under a Contract. If not applicable, the following clauses should be deleted and replaced with 'Not Used', and other clauses that reference continuous monitoring should also be amended.

6.2.7 Continuous Monitoring Plan

Note: The requirements of this clause are broader than the ISM requirements for a continuous monitoring plan.

6.2.7.1 The ISSMP shall document the Contractor's plan for undertaking continuous monitoring of each SSoI (or applicable element thereof) during the in-service phase, to proactively identify, prioritise and respond to security Issues (eg, vulnerabilities) ('**Continuous Monitoring Plan**'), including:

a. identifying the management structures and the roles and responsibilities of applicable personnel (Commonwealth, Contractor and Subcontractors) associated with continuous monitoring of each SSoI, including the relationships with incident response management and business continuity and disaster recovery management;

b. describing the use of agencies and websites that provide advice of known vulnerabilities, such as the ACSC Alerts and the Known Exploited Vulnerabilities (KEV) catalogue at www.cisa.gov/known-exploited-vulnerabilities-catalog;

c. describing the use of automated system event logging tools and processes (if applicable), as described in the ACSC Guidance Document, 'Guidelines for System Monitoring', to assist with the identification of security vulnerabilities and security incidents, including:

   (i) describing how the system event logging systems and processes have been implemented;

   (ii) identifying the system events to be logged and the associated event details to be captured;

   (iii) describing the mechanisms for security vulnerability / incident identification and reporting based on the logged system events (eg, automatically to the system administrator and/or system security manager within particular timeframes); and

   (iv) management of the event log, including protection, retention, and auditing;

d. in addition to any automated system event processes, describing the types of intermittent monitoring and testing activities to be employed (eg, vulnerability assessments, vulnerability scans and penetration tests), including the likely nature and scope of these activities and the timeframes for conducting them;

e. describing the analysis and investigation activities to be undertaken when potential or actual security Issues (eg, vulnerabilities) are identified, including the stakeholders to be consulted and the report(s) to be provided to the Commonwealth;

f. describing the processes to be employed to prioritise the implementation of mitigations, taking into account the cost of mitigations and the implications for Defence operations, other Contract work, the health and safety of personnel, and the environment; and

g. describing how the mitigation work will be implemented and managed, particularly when configuration changes are required.

Annex:

A. CASG Risk Management Product Risk Matrix

DID-ENG-MGT-MSS
MP - Annex A Risk M

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-V&V-DEF-PV&VRP-V5.3

2. TITLE: CONTRACTOR'S PREVIOUS V&V RESULTS PACKAGE

3. DESCRIPTION AND INTENDED USE

3.1 The Contractor's Previous Verification and Validation (V&V) Results Package (PV&VRP) describes the previous V&V activities performed by the Contractor which are relevant to the Materiel System.

3.2 The Contractor uses the PV&VRP to provide, for Approval, details of previously conducted V&V activities that it proposes as precluding the requirement to conduct further specific V&V activities under the Contract. The Contractor will reference this intention in the V&V Plan or the SEMP (whichever is the governing plan for V&V under the Contract) and will cross-reference the details of the Approved PV&VRP in the Verification Cross Reference Matrix (VCRM).

3.3 The Commonwealth uses the PV&VRP to assess whether the Contractor's previous V&V activities are adequate to satisfy all or part of the V&V requirements of the Contract, and as a reference in assessing the suitability of the Supplies for Acceptance.

4. INTER-RELATIONSHIPS

4.1 The PV&VRP is subordinate to the following data items, where these data items are required under the Contract:

a. Systems Engineering Management Plan (SEMP);

b. Integrated Support Plan (ISP); and

c. Verification & Validation Plan (V&VP).

4.2 The PV&VRP inter-relates with the following data items, where these data items are required under the Contract:

a. Verification Cross Reference Matrix (VCRM).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 Any covering documentation developed by the Contractor for delivery of this data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 The V&V documents previously developed by the Contractor and delivered in response to this DID do not have to comply with the format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.2 Specific Content

6.2.1 General

6.2.1.1 The Contractor's PV&VRP shall identify the processes employed by the Contractor for planning, managing, implementing and recording any V&V activities conducted prior to the Contract, where the results of these activities are being used to demonstrate that some of the requirements of the Contract have been met.

6.2.2 Detail

6.2.2.1 The Contractor's PV&VRP shall comprise all V&V documents necessary to demonstrate that some of the specified requirements for the Materiel System are satisfied, including:

a. Verification and Validation Plans;

b. Verification Cross Reference Matrices;

c. Test Plans;

d. Test Procedures; and

e. Test Results and Reports.

6.2.2.2 The Contractor's PV&VRP shall identify the relationship between the Contractor's previous V&V programs and the V&V requirements of the Contract, and shall describe the rationale for not conducting specific Verification activities.

6.2.2.3 The Contractor's PV&VRP shall identify the relationship between the Test Plans, Procedures, Results and Reports, and the Supplies offered.

6.2.2.4 The Contractor's PV&VRP shall identify and describe deficiencies between the V&V programs previously conducted and the V&V requirements of the Contract.

6.2.2.5 The Contractor's PV&VRP shall be cross-referenced to the V&VP or the SEMP (whichever is the governing plan for V&V under the Contract) and the VCRM for the Contract.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-V&V-DEF-VCRM-V5.3

2. TITLE: VERIFICATION CROSS REFERENCE MATRIX

3. DESCRIPTION AND INTENDED USE

3.1 The Verification Cross-Reference Matrix (VCRM) is used to plan, and record the results of, the Contractor’s Verification activities.

3.2 The Contractor and the Commonwealth use the VCRM as the basis for common understanding and status of the Verification of requirements for each Mission System and the Support System.

4. INTER-RELATIONSHIPS

4.1 The VCRM is subordinate to the following data items, where these data items are required under the Contract:

a. Verification & Validation Plan (V&VP); and

b. Systems Engineering Management Plan (SEMP).

4.2 The VCRM inter-relates with the following data items, where these data items are required under the Contract:

a. System Specification (SS) for each Mission System;

b. Support System Specification (SSSPEC); and

c. Requirements Traceability Matrix (RTM).

5. APPLICABLE DOCUMENTS

5.1 The following documents form a part of this DID to the extent specified herein:

Nil.

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

6.2 Specific Content

6.2.1 General

6.2.1.1 The VCRM is expected to be an evolving document, which is used during the analysis and design phases of the program to capture agreement on the Verification program, and during the Verification phases to capture the ongoing status of the system with respect to Verification and Validation (V&V).

6.2.1.2 The VCRM is likely to be based in electronic form (eg, database or spreadsheet), but when printed, shall consist of a table with an entry for every requirement in the Functional Baseline(s).

6.2.1.3 The Commonwealth only requires the VCRM in order to manage Verification against the Functional Baseline(s); however, the Contractor may choose to include other levels of specification within the same document. In this case, the VCRM shall:

a. identify which entries pertain to the Verification of the Functional Baseline(s); and

b. where Verification results from lower levels of the system hierarchy are proposed to be used as evidence for Verification against a Functional Baseline, provide traceability between the applicable lower levels of the system and the Functional Baseline.

6.2.2 Part 1 Requirements

6.2.2.1 For delivery of the Part 1 VCRM requirements, each entry in the VCRM table shall contain at least:

a. a unique reference to the corresponding requirement in the Functional Baseline(s);

b. the requirement words or a brief precis of the requirement to provide context;

c. the proposed Verification method(s) (ie, one or more of inspection, demonstration, analysis, test, simulation, modelling, experiment, trial, walk-through, comparison, System Review, Audit, historical data and certification of conformance);

d. the phase during which the requirements will be Verified and the associated Verification method to be applied at this phase; noting that, where Verification across multiple phases may be proposed, the scope and aims of the activities at each phase must be clearly described;

e. a brief description of the proposed Verification method, intended as a vehicle for early agreement by both parties to define the scope of the Verification activities; and

f. other comments as required.

6.2.3 Part 2 Requirements

6.2.3.1 For delivery of the Part 2 VCRM requirements, each entry in the VCRM table shall contain at least:

a. the Part 1 requirements specified at clause 6.2.2 of this DID;

b. a reference to the specific Verification / test procedure(s) and relevant documentation, including unique version identifiers;

c. a reference to the report which contains the pertinent Verification results and, as required, data analysis (including any red-line mark-ups and signatures of witnesses to those results);

d. the progressive status of each phase of the Verification program with respect to the requirement;

e. a result summary (ie, PASS/FAIL or Verification incomplete if all of the Verification activities associated with the requirement have not been completed); and

f. other comments as required.