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-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-MGT-SEMP-2-V5.2

2. TITLE: SYSTEMS ENGINEERING MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Systems Engineering Management Plan (SEMP) describes the Contractor's strategy, plans, methodologies and processes for the management of a fully integrated engineering program in accordance with the Contract. The SEMP describes the relationships between concurrent activities as well as between sequential activities, to demonstrate that a fully integrated engineering program has been achieved.

3.2 The Contractor uses the SEMP to provide the primary direction and guidance to the technical team responsible for conducting the scope of work.

3.3 The Commonwealth uses the SEMP as a benchmark against which Contractor performance and changes in technical risk can be evaluated.

4. INTER-RELATIONSHIPS

4.1 The SEMP shall be consistent with, and subordinate to, the Project Management Plan (PMP).

4.2 The SEMP shall be the single planning and controlling document for all engineering program activities and related efforts, and shall have authority over, and give direction to, any subordinate engineering plans.

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

a. Integrated Support Plan (ISP);

b. Configuration Management Plan (CMP);

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

d. Quality Plan (QP).

5. APPLICABLE DOCUMENTS

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

ANSI/EIA-632-2003	*Processes for Engineering a System*
AS/NZS ISO/IEC/IEE 12207:2019	*Systems and Software Engineering - Software life cycle processes*
	The specialty engineering standards identified in the SOW (eg, in relation to system safety, system security and Electromagnetic Environmental Effects (E3))

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 SEMP 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 Technical Plan Summary

6.2.1.1 The SEMP shall describe the objectives, scope, constraints, and assumptions associated with the Contractor's systems engineering program.

6.2.1.2 Risks associated with the Contractor's systems engineering program, including risks associated with the development and implementation of the required products, shall be documented in the Risk Register; however, the SEMP shall describe the risk-management strategies associated with any risks where the mitigation strategy underpins the overall systems engineering program (clause 6.2.5 refers).

6.2.1.3 The SEMP shall define its relationship to other planning documentation, including subordinate engineering plans and key non-technical plans such as the PMP.

6.2.1.4 The SEMP shall define the scope and purpose of subordinate engineering plans, including the interrelationships between subordinate plans.

6.2.2 Systems Engineering Key Activities

6.2.2.1 The SEMP shall describe the Contract technical objectives, with reference to the proposed solution and with particular emphasis on the technical products to be delivered and the extent of development required for them.

6.2.2.2 The SEMP shall identify the key engineering elements and events of the Contract, including the key events in the lifecycle of each product in the design hierarchy, the interrelationships between them, and those significant engineering events within the Contract schedule.

6.2.3 Engineering Management

6.2.3.1 The SEMP shall define the engineering organisation for the Contract, including the key engineering positions and the partitioning of engineering effort between the various Contractor and Subcontractor organisations.

6.2.3.2 The SEMP shall describe how technical effort will be coordinated to meet cost, schedule and performance objectives.

6.2.3.3 The SEMP shall summarise planned personnel needs, applicable to the various phases of the Contract, by discipline and level of expertise.

6.2.3.4 The SEMP shall identify the standards (eg, EIA-632 and ISO 12207) to be utilised by the Contractor and Subcontractors to undertake the Systems Engineering, Software, Configuration Management (CM), and Verification and Validation (V&V) program activities, including the proposed tailoring of those standards to meet requirements of the Contract.

6.2.4 Systems Engineering Process

6.2.4.1 The SEMP shall define the tailored application of the Contractor's Systems Engineering process to the activities of the Contract, including:

a. the major products and/or increments to be delivered;

b. the major outcomes to be achieved;

c. the major Systems Engineering tools that will be used for the Contract;

d. the methods for documentation and control of engineering and technical information, including expected specifications and Configuration Baselines;

e. the methods and tools for analysis and Validation of system requirements;

f. the required implementation tasks, including the integration and assembly of the system; and

g. the approach, methods, procedures and tools to be used for systems analysis and control, including establishing and maintaining requirements traceability.

6.2.5 Technical Risk Management

6.2.5.1 Risks associated with the Systems Engineering program shall be documented in the Risk Register; however, the SEMP shall describe the risk management strategies associated with any global, engineering-related risks.

6.2.6 Software Development and Management

6.2.6.1 The SEMP shall define the tailored application of the Contractor's Software processes to the activities of the Contract, including:

a. the integration of Software activities into the systems engineering program for the various products and/or increments to be delivered;

b. the management of Software development activities undertaken by Subcontractors; and

c. the development of Software being undertaken by the Contractor.

6.2.7 Verification and Validation

6.2.7.1 The SEMP shall, for the Contractor's V&V program:

a. describe the V&V strategy, particularly describing how the V&V activities are integrated into the systems engineering program for the various products and/or increments to be delivered;

b. summarise the V&V program activities and schedule;

c. describe the use of the VCRM and the extent to which previous V&V results are proposed to be used for Acceptance Verification purposes;

d. describe the process for recording Failure reporting and analysis, and the approach to regression testing; and

e. identify the requirements for Commonwealth Personnel and other resources in order to conduct the V&V program.

6.2.8 Configuration Management

6.2.8.1 The SEMP shall describe the Contractor's CM methodology, processes and activities for meeting the CM requirements of the Contract, including:

a. the approach planned to establish and maintain Configuration Control and audit of identified system products and processes;

b. the requirements for establishing Configuration Baselines and the documentation to be used to define each baseline; and

c. the approach planned to establish and maintain control of external and internal interfaces, including (if applicable) the conduct of Interface Control Working Groups (ICWGs).

6.2.9 System Reviews

6.2.9.1 The SEMP shall describe the approach planned for the conduct of all System Reviews (ie, Mandated System Reviews (MSRs) and Internal System Reviews) required under the Contract.

6.2.9.2 The SEMP shall describe the objectives for each engineering-related System Review and the relationship between each System Review and other engineering program activities.

Note: The following clause only relates to the engineering-related System Reviews. The main governing plans for each of the Level 2 subject area clauses in the SOW address the other System Reviews (eg, the PMP addresses project management System Reviews, the ISP addresses ILS-related System Reviews, and the CMP or SEMP addresses CM-related System Reviews).

6.2.9.3 The SEMP shall detail the following information for each of the engineering-related System Reviews, incorporating the associated SOW requirements (including entry criteria, exit criteria and checklist items) for these System Reviews and supplemented where required by the Contractor's internal processes:

a. the organisations and individuals involved in the review and their specific review responsibilities;

b. the proposed review venue;

c. the pre-requisites for the conduct of the review (ie, entry criteria);

d. the checklist items to be addressed during the System Review, including the documentation to be reviewed;

e. the essential review completion criteria (ie, exit criteria); and

f. the applicable Milestone criteria specified in Attachment C, Delivery Schedule.

6.3 Specific Content – Specialty Engineering

6.3.1 Growth, Evolution and Obsolescence

6.3.1.1 If a growth, evolution and Obsolescence program is required under the Contract, the SEMP shall, for the growth, evolution and Obsolescence program:

a. describe the technical measures and methods to be used to identify and assess candidate elements (ie, those system elements that are candidates for change over the LOT due to the evolution of technology, changes to threats or user needs, or Obsolescence), including hardware and Software items, and the primary candidate elements to be addressed under the program;

b. describe the application of design aspects (eg, modularity and 'open architectures') to improve system growth, facilitate evolution, and to counter Obsolescence;

c. identify the steps to be undertaken during the acquisition phase to balance technological maturity and Obsolescence risks, and solutions to minimise the complexity (and cost) of through-life upgrades; and

d. identify the steps to be undertaken during the support phase to maintain effective and supportable equipment configurations and the expected need for upgrades.

6.3.2 Integrated Reliability, Maintainability and Testability Engineering

6.3.2.1 If an Integrated Reliability, Maintainability and Testability (IRMT) engineering program is required under the Contract, the SEMP shall, for the Contractor's IRMT engineering program:

a. outline the IRMT engineering activities, tools, and the products to be generated, consistent with the design activities and the integration of COTS / MOTS items;

b. identify the standards to be used (including those identified at clause 5.1), and describe the application of those standards to meet the IRMT-related requirements of the Materiel System;

c. describe the sources, methods and systems to be used to obtain, analyse and record IRMT-related data from internal and external sources;

d. describe how IRMT engineering program activities and outputs are integrated into the system engineering program for the various products, including identifying the outputs to be provided for the System Reviews; and

e. describe the Verification methods to be applied for the IRMT engineering program.

6.3.3 Human Engineering

6.3.3.1 If a Human Engineering (HE) program is required under the Contract, the SEMP shall, for the Contractor's HE program:

a. identify the standards to be used (including those identified at clause 5.1), and that have been used for COTS / MOTS items, and describe the application of those standards to meet the HE requirements of the Materiel System;

b. describe the expectations of the Contractor with respect to the Commonwealth in order to ensure the HE objectives are met;

c. describe the activities, including system functional requirements analysis, equipment design and procedures development activities, to be undertaken in order to meet the HE program required under the Contract;

d. describe how HE program activities and outputs are integrated into the system engineering program for the various products, including identifying the outputs to be provided for the System Reviews; and

e. describe the Verification methods to be applied for the HE program.

6.3.4 Electromagnetic Environmental Effects

6.3.4.1 If an Electromagnetic Environmental Effects (E3) program is required under the Contract, the SEMP shall, for the Contractor's E3 program:

a. identify the standards to be used (including those identified at clause 5.1), and that have been used for COTS / MOTS items, and describe the application of those standards to the Materiel System;

b. identify the E3-related requirements applicable to the Materiel System, including Certification and regulatory requirements;

c. describe the approach to ensure that the E3-related requirements are met and all applicable Certifications are obtained;

d. describe how E3 program activities and outputs are integrated into the system engineering program for the various products, including identifying the outputs to be provided for the System Reviews; and

e. describe the Verification methods to be used to assess that the Materiel System's E3-related requirements have been met.

6.3.5 System Safety

6.3.5.1 The SEMP shall, for the Contractor's system safety program:

a. identify the standards to be used (including those identified at clause 5.1), and that have been used for COTS / MOTS items, and describe the application of those standards to meet the system safety required under the Contract;

b. identify the Materiel Safety-related requirements applicable to the operation and support of the Materiel System, including Certification and regulatory requirements, and describe the approach to ensure that the Materiel Safety-related requirements are met and all applicable Certifications are obtained;

c. describe how system safety program activities and outputs are integrated into the system engineering program for the various products, including identifying the outputs to be provided for the System Reviews;

d. describe the hazard analyses to be undertaken to identify and assess health and safety hazards and risks in the Materiel System, and to eliminate hazards and reduce associated risks so far as is reasonably practicable;

e. describe the Verification methods to be used to assess the minimisation of Materiel Safety-related risks and the treatment of those residual risks; and

f. describe the approach to managing Materiel Safety data and the provision of documentary evidence to the Commonwealth, and regulatory authorities when applicable, in order to demonstrate that the Materiel System is, so far as is reasonably practicable, without risks to health and safety.

6.3.6 System Security

6.3.6.1 If a system security program is required under the Contract, the SEMP shall, for the Contractor's system security program:

a. identify the standards to be used (including those identified at clause 5.1), and that have been used for COTS / MOTS items, and describe the application of those standards to meet the system security requirements of the Contract;

b. identify the security-related requirements applicable to the Materiel System and summarise the approach to ensure that the security-related requirements are met;

c. if the Contractor will support the Commonwealth to obtain and/or maintain Security Authorisations in relation to ICT security and cyber security:

(i) identify each Security System-of-Interest (SSoI) and the Targets of Security Assessment (ToSAs) within each SSoI;

(ii) identify, as applicable, the System Owner, security requirements authorities, Security Authorisation authorities, and other Associated Parties;

(iii) describe the technical requirements that must be met in relation to each SSoI/ToSA (eg, as set out in the Governing Security Documents);

(iv) describe the risk management processes to be applied, including to conduct security threat and risk assessments and for maintaining a risk register; and

(v) explain the Contractor's role in achieving Security Authorisations to be obtained for each SSoI/ToSA;

d. if 'Cyber Security Assessment Information' is required, describe how this data item is to be prepared and how the security risk assessment details will be maintained;

e. describe how system security program activities and outputs are integrated into the system engineering program for the various products, including identifying the outputs to be provided for the System Reviews; and

f. describe the Verification methods to be used to assess that the Materiel System's security-related requirements have been met.

6.3.7 System Certification

6.3.7.1 If the Mission System requires Certification in accordance with the Contract, the SEMP shall, for the Contractor's system Certification program:

a. identify the Certification requirements, including related design standards, and the applicable certificating authorities that will be involved in the Certification process;

b. describe the approach to the collection, collation and presentation of Objective Evidence required for Certification; and

c. outline the Certification process to be followed and the interrelationships between the Certification process and applicable Milestones.

6.3.8 Environmental Engineering

6.3.8.1 If an environmental engineering program is required under the Contract, the SEMP shall, for the Contractor's environmental engineering program:

a. identify the standards to be used (including those identified at clause 5.1), and that have been used for COTS / MOTS items, and describe the application of those standards to meet the environmental engineering requirements of the Contract;

b. identify the environmental-related requirements, including regulatory requirements and environmental-protection aspects of the design, applicable to the operation and support of the Materiel System;

c. describe the approach to ensure that the environmental-related requirements are met and all applicable Certifications are obtained;

d. describe how environmental engineering program activities and outputs are integrated into the system engineering program for the various products, including identifying the outputs to be provided for the System Reviews; and

e. describe the Verification methods to be used to assess that the Materiel System's environmental-related requirements have been met.

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-ESCP-V5.3

2. TITLE: EMANATION SECURITY (EMSEC) CONTROL PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Emanation Security (EMSEC) Control Plan (ESCP) sets out the Contractor's plan to reduce the assessed risks arising from the potential exploitation by non-Defence parties of compromising emanations produced by the Mission System. The ESCP addresses the assessed risks through the management of the spatial environment and installation methods used for systems processing classified information above PROTECTED.

Notes:

- ***The EMSEC Threat Level (ETL) is stated within the Project EMSEC Threat Assessment (ETA), which is produced by Australian Signals Directorate (ASD) in accordance with ACSI 71D. A Project TEMPEST Requirements Statement (TRS) may also be produced by ASD, which provides guidance on the EMSEC installation requirements for the Mission System that will enable it to meet EMSEC testing required by ASD, given the assessed risk levels. The level and depth of the design-related and installation-related information provided in the ESCP are shaped by the guidance contained within the Project ETA and, if applicable, the Project TRS. Due to the classified nature of TEMPEST testing, the Commonwealth normally conducts this testing.***
- ***The Contractor prepares the ESCP under guidance from the Commonwealth Representative and the Commonwealth submits the document to the Certification authority in support of the EMSEC Certification and Accreditation of the Mission System.***

3.2 The Contractor uses the ESCP as one of the EMSEC artefacts:

a. to detail the design and installation methods to be used to reduce or eliminate compromising emanations produced by the Mission System;

b. to advise the Commonwealth and the associated Certification and Accreditation authorities, as prescribed by ASD, of the design and installation methods implemented to address the risks associated with the potential exploitation of compromising emanations; and

c. to provide assurance to the Commonwealth that the Contractor's EMSEC activities will enable the security requirements for the Mission System to be achieved.

3.3 The Commonwealth uses the ESCP:

a. to gain assurance that EMSEC considerations are taken into account during the design and installation activities for the Mission System;

b. to understand and evaluate the Contractor's approach to meeting the EMSEC requirements of the Contract as part of the system security program;

c. to identify and understand the Commonwealth's involvement in the Contractor's EMSEC 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 Certification and/or Accreditation for the Mission System; and

e. as one of the suite of EMSEC artefacts provided to the relevant Defence authorities as part of obtaining Certification and/or Accreditation for the Mission System.

4. INTER-RELATIONSHIPS

4.1 The ESCP 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); and

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

4.2 The ESCP 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;

b. the safety-related design artefacts (eg, Safety Case Report (SCR));

c. Mission System Technical Documentation Tree (MSTDT); and

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

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 requirements of the Contract. Do not include the documents included within the 'Governing Security Documents'.

Governing Security Documents	(see the Glossary for the definition of this term)
ACSI 71D	Australian Communications Security Instruction – Emanation Security Manual
ACSI 61D	Australian Communications Security Instruction – Emanation Security Installation Manual
DEF(AUST) 5000, Volume 6, Part 2, Section 12, Issue 2	Emanation Security
Project ETA	Project EMSEC Threat Assessment
Project TRS	Project TEMPEST Requirements Statement (if a Project TRS is required for the project)

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 The ESCP shall be classified in accordance with the requirements of the Security Classification and Categorisation Guide (SCCG) at Attachment J to the COC, but shall not be classified lower than OFFICIAL: SENSITIVE.

6.2 Specific Content

6.2.1 Introduction

6.2.1.1 The ESCP shall provide a brief overview of the purpose and background of the project and the Mission System.

6.2.1.2 The ESCP shall:

a. set out the aim of the ESCP;

b. set out the scope of the ESCP, including the applicable information from Sections 1 and 2 of ACSI 71D and Sections 1 and 2 of ACSI 61D;

c. provide a description of the Mission System in the form of a block diagram with signal flow paths;

d. provide a brief description of EMSEC and EMSEC control, including how EMSEC control management is to be conducted for the project; and

Note to drafters: Amend the following clause if PURPLE is not applicable to the Contract.

e. describe how conventions such as BLACK, RED and PURPLE (Classification Domains) will be used throughout the document.

6.2.2 Organisation and Management

6.2.2.1 To the extent not already addressed in the Approved governing plan (eg, SEMP, MSSMP or ISSMP), the ESCP shall describe the roles and responsibilities of the main personnel involved in the EMSEC program, including:

a. Contractor EMSEC Control Officer (appointed by the Contractor); and

b. Delivery Group EMSEC Control Officer (appointed by the Commonwealth).

6.2.3 General Requirements

6.2.3.1 The ESCP shall provide a summary of the EMSEC requirements to be met by the Mission System, including:

a. the requirements contained in the Specification(s) at Annex A to the SOW;

b. the requirements derived from the applicable documents identified at clause 5.1; and

c. any other requirement sources used by the Contractor.

6.2.3.2 The ESCP shall include a table that provides the allocation of the required controls, as derived from the applicable documents identified at clause 5.1, to the entity responsible for the implementation of that control (eg, Contractor or Commonwealth).

6.2.3.3 The ESCP shall identify and describe the EMSEC-related Technical Data that will be produced and/or delivered as part of the EMSEC program.

6.2.4 Design Concepts

6.2.4.1 The ESCP shall describe the design concepts that have been followed for the Mission System to ensure that the system complies with EMSEC requirements identified pursuant to clause 6.2.3.1 of this DID. Design concepts that should be considered include:

a. those set out in the Project TRS (if applicable);

b. those set out in Sections 3-5 of ACSI 61D; and

c. the following specific issues:

(i) physical design of the controlled space;

(ii) pipe work;

(iii) Heating, Ventilation and Air Conditioning (HVAC);

(iv) controlled space personnel access points;

(v) controlled space penetration points;

(vi) measures to minimise Electromagnetic Interference (EMI) and maximise Electromagnetic Compatibility (EMC);

(vii) equipment and material selection, including cable design characteristics;

Note to drafters: Amend the following clause if PURPLE is not applicable to the Contract.

(viii) BLACK, RED and PURPLE domains;

(ix) physical and electrical segregation, separation and isolation of equipment;

(x) grounding and bonding;

(xi) Radiofrequency (RF) earth management;

(xii) EMSEC controls for emission and conduction; and

(xiii) ICT equipment in TOP SECRET areas meets industry and government standards relating to EMI/EMC.

6.2.5 Installation Concepts

6.2.5.1 The ESCP shall describe the installation procedures and policies to be followed during the build phase of the Mission System to ensure that the system complies with EMSEC requirements identified pursuant to clause 6.2.3.1 of this DID. Installation concepts that should be considered in this section include:

a. those set out in the Project TRS (if applicable);

b. those set out in Sections 3-5 of ACSI 61D; and

c. the following specific issues:

(i) HVAC distribution;

(ii) cable distribution, isolation and routing;

(iii) cable design characteristics and modifications;

(iv) EMC, EMI and Radiation Hazards (RADHAZ);

(v) physical and electrical segregation, separation and isolation of equipment;

(vi) screening;

(vii) penetration;

(viii) filtering;

(ix) isolators;

(x) RF earthing via an RF earth tree diagram; and

(xi) logical system cable flows.

Note: The physical implementation of the EMSEC Control System is detailed in a series of Annexes as described below and are to be completed as the design progresses. The Contractor EMSEC Control Officer is to add any additional Annexes they deem necessary to facilitate the Verification process.

6.2.6 Annex A – Screened Compartment Implementation or Alteration

6.2.6.1 This Annex shall detail any new screened compartments that are required to be constructed and any existing screened compartment that requires alteration for the implementation of the Mission System.

6.2.6.2 This section shall describe how the attenuation characteristics of secure areas will not be degraded by the installation of systems and equipment into the Mission System (eg, through use of EMI/EMC penetrations/filters etc).

6.2.6.3 This Annex shall detail at least the following:

a. construction requirements;

b. personnel access point;

c. HVAC access points;

d. power access points; and

e. cable input / output access points.

6.2.7 Annex B – EMSEC Installation Directives

6.2.7.1 This Annex shall describe boundaries of all secure areas affected by the installation of systems and equipment into the Mission System. This will detail the boundaries of the following areas, including diagrams where applicable:

a. physical controlled space boundary; and

b. physical EMSEC boundary.

6.2.8 Annex C – Component Data Pack

6.2.8.1 This Annex shall contain the data files for the systems and equipment installed into the Mission System, which are used to ensure that the Mission System complies with the EMSEC requirements.

6.2.8.2 Components data sheets contained in this annex should include:

a. power filter data sheets;

b. telephone filter data sheets;

c. HVAC waveguide ventilating panels; and

d. EMC penetration glands.

6.2.9 Annex D – EMSEC Cable Register

6.2.9.1 This Annex shall detail all cables, listing the cable number, cable type and classification that enter or exit any controlled space within the Mission System.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-MSA-V5.2

2. TITLE: MATERIEL SAFETY ASSESSMENT

3. DESCRIPTION AND INTENDED USE

3.1 The Materiel Safety Assessment (MSA) provides evidence of safety hazards and their associated risks, and how they have been eliminated or treated, prior to test or operation of the system, following system modification, or prior to Acceptance of the applicable Supplies (ie, physical items including Mission Systems and applicable Support System Components, as applicable to the Contract). The MSA, including by reference to other safety related data items, 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 required to demonstrate that the Materiel Safety requirements of the Contract have been, or will be[1], met.

3.2 The Contractor uses the MSA to present an argument that:

a. when used in relation to the Acceptance of Supplies, the applicable Supplies are safe for the purpose or purposes contemplated by the Contract;

b. 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 MSA:

a. to determine that the hazards and risks 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 the applicable Supplies prior to the Acceptance of those Supplies;

d. to obtain the necessary safety certifications from Defence regulatory and safety authorities; and

e. as a basis for assessing and managing the health and safety risks of the applicable Supplies.

4. INTER-RELATIONSHIPS

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

a. Systems Engineering Management Plan (SEMP); and

b. Project Management Plan (PMP).

5. APPLICABLE DOCUMENTS

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

Nil.

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

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 MSA shall include a summary of the information presented as evidence of Materiel Safety for each item of plant (eg, new or modified equipment), structure and substances (eg, Consumables) delivered under the Contract (the 'applicable Supplies').

6.2.1.2 The MSA shall provide a description of the system safety program, including the processes employed by the Contractor to collect and confirm the validity of extant safety related data, to develop the assessment of Materiel Safety for the applicable Supplies.

6.2.2 Materiel Safety Assessment

6.2.2.1 The MSA shall contain adequate information to demonstrate the Materiel Safety of each of the applicable Supplies, including:

a. the purpose for which the item was designed and manufactured, including limits on equipment operation and allowable environmental conditions,

b. the results of any calculations, analysis, tests or examinations necessary to demonstrate the Materiel Safety of the applicable Supplies;

c. any conditions necessary to ensure that the Materiel Safety of the applicable Supplies is maintained;

d. any additional supporting evidence reasonably required by the Commonwealth for the purposes of demonstrating Materiel Safety; and

e. evidence that the requirements of relevant Australian legislation and applicable design and safety standards have been met.

6.2.2.2 The MSA shall include, 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, copies of the registration documents provided by the Commonwealth, State or Territory regulator.

6.2.2.3 The MSA shall include evidence that all applicable certifications (other than Australian design registration details included in accordance with clause 6.2.2.2) and necessary safety-related compliance assurance activities, as required by the applicable third party regulatory and safety authorities, have been met.

6.2.3 Safety Hazards and Risk Log

6.2.3.1 The MSA shall contain, at Annex A, a log of hazards and associated risks to health and safety, including:

a. hazard identification (eg, radiation leakage from waveguide);

b. a description of the hazard and its associated risks to health and safety;

c. identification of the relevant item, system element or component of the applicable Supplies;

d. if in relation to a Problematic Substance, the log details shall include:

(i) identification of the Problematic Substance, a cross-reference to the Safety Data Sheet (SDS), which shall be prepared in accordance with DID-PM-HSE-SDS and included as supporting information annexed to the MSA;

(ii) the location(s) of the Problematic Substance within the applicable Supplies and/or for use in Maintenance or other support processes; and

(iii) the quantity of the Problematic Substance in each location identified under clause 6.2.3.1d(ii);

e. other applicable factors (eg, equipment configuration, operating environment, system events or modes) when the hazard or risk are present;

f. identification of the risks associated with each hazard;

g. treatments that have been implemented to eliminate safety risks and to minimise residual risks where elimination was not reasonably practicable; and

h. references to information regarding safe practices and other measures relevant to minimising the remaining risks (eg, operator and maintenance manuals, training materials and other references).

6.3 Annexes

Annex A: Safety Hazards and Risk Log

Other Annexes as necessary to provide all Materiel Safety information required by this DID that has not already been provided under another data item in accordance with the Contract.

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-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-ILS-DEF-TRS-V5.3

2. TITLE: TRAINING REQUIREMENTS SPECIFICATION

3. DESCRIPTION AND INTENDED USE

3.1 A Training Requirements Specification (TRS) defines the requirements for a Training solution, to be implemented so that trained Personnel can perform a job relating to the operation or support of the Materiel System. In relation to the Systems Approach to Defence Learning (SADL) the TRS is SADL product AP9, and is prepared for a set of related performance needs and performance gaps identified for a particular job, where a 'job' represents a set of duties or related tasks (eg, to operate a piece of equipment or a software package). The TRS specifies the skills, knowledge, attitudes and behaviours to be attained, and provides a basis for evaluating the Training and assessment program, Training Equipment and Training Materials delivered under the Contract.

3.2 The Contractor uses the TRS:

a. to document, as a result its analyses, the learning and assessment requirements to be addressed through a Training solution; and

b. as the basis for seeking recognition of the Training program and/or Units of Competency (UOCs), within the national register of vocational education and training, where this is a requirement of the Contract.

3.3 The Commonwealth uses the TRS:

a. to understand the requirements for a Training solution, and the related scope of Training design and development activities to be undertaken by the Contractor;

b. as a basis for evaluating the Training courses, Training Equipment, and Training Materials as part of subsequent Verification and Validation (V&V) activities; and

c. to assist the Commonwealth attain recognition of the Training and/or UOCs within the national vocational education and training system, if the Commonwealth seeks this accreditation outside of the Contract.

4. INTER-RELATIONSHIPS

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

a. System Specification (SS);

b. Support System Specification (SSSPEC);

c. Verification Cross Reference Matrix (VCRM);

d. Integrated Support Plan (ISP);

e. Training Support Plan (TSP);

f. Support Services Management Plan (SSMP);

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

h. Performance Needs Analysis Report (PNAR);

i. Learning Management Packages (LMPs);

j. Support System Technical Data List (including the Training Materials List);

k. Training Equipment List (TEL); and

l. Recommended Provisioning List (RPL).

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
	Standards for Training Packages, National Skills Standards Council
	The applicable ADF Service Training Manual, as specified in the Statement of Work

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 Unless otherwise specified in the Contract, TRSs shall address Training for the:

a. Commonwealth,

b. Contractor (Support), and

c. Subcontractors (Support).

Note: Additional TRS information required in accordance with the SADL Guide (ie, not included in this DID) may be added by the Commonwealth following delivery of the data item.

6.1.3 The TRS shall accord to the requirements of the 'Analyse Phase' in the SADL Guide.

6.1.4 When the Contract has specified delivery of another data item that contains aspects of the required information, the TRS shall 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 The TRS shall have a heading that includes the job name for which the TRS is prepared.

6.2.2 Background

6.2.2.1 The TRS shall identify the input giving rise to the Training requirement (eg, to perform an activity that is related to an item delivered under the Contract).

6.2.2.2 The TRS shall include a job classification section that includes (as summarised from the job specification(s)):

a. job name / title;

b. job code number;

c. job designation;

d. job description; and

e. job function;

6.2.2.3 The TRS shall include a Training course summary section that includes:

a. course name / title;

b. course code number;

c. course description;

d. Defence sponsor, where this information is provided by the Commonwealth;

e. rank / level; and

f. organisational structure, identifying the organisation (eg, Commonwealth or Contractor (Support)) and business unit where the trained Personnel will work.

6.2.3 Aim

6.2.3.1 The TRS shall include a statement of aim, which refers to the identification of the most appropriate Training solution for the specific job.

6.2.4 Supporting and Associated Documentation

Note: The associated documents may be produced as part of the TRS or may otherwise be required in accordance with the Contract or the Approved TSP.

6.2.4.1 The TRS shall list the documents supporting or otherwise associated with the TRS including, as applicable, the:

a. Risk Assessment Summary (SADL product AP2);

b. Job Task Profile (SADL product AP3);

c. Job Specifications (SADL product AP4);

d. Target Population Profile (SADL product AP5);

e. Gap Analysis Statement (SADL product AP6);

f. Feasibility Analysis Report (SADL product AP7);

g. Business Case (SADL product AP10); and

h. Implementation Schedule (SADL product AP11).

6.2.4.2 If not otherwise delivered under the Contract, the documents listed under clause 6.2.4.1 shall be included in annexes to the TRS.

6.2.5 Training Requirement - People

6.2.5.1 The TRS shall describe the people who are candidates for Training in a Target Population Profile (SADL product AP5), including:

a. the number of people to be employed in the related job and the anticipated personnel turnover rate;

b. the expected numbers of trainees for Introduction into Service Training (including initial Training for training personnel as applicable); and

c. the expected throughput of trainees, per year, for Sustainment Training, Continuation Training and Conversion Training, as applicable.

6.2.5.2 The TRS shall include a trainee population profile, summarising the expectations for previous education and experience. If the Commonwealth provides details of the target population profile, such as career path and typical employment at Defence units, then the TRS shall incorporate the relevant information.

6.2.5.3 The TRS shall outline the new skills, knowledge, attitudes and behaviours required to fill the identified performance gap.

6.2.6 Feasibility Analysis Process

6.2.6.1 The TRS shall summarise the feasibility analysis of the Training options considered in a Feasibility Analysis Report (SADL product AP7), including the criteria and rationale for the recommended Training solution.

6.2.7 Recommendations

6.2.7.1 The TRS shall outline the Training required to fill the identified performance gap (ie, for the skills, knowledge, attitudes and behaviours identified in response to clause 6.2.5.3).

6.2.7.2 The TRS shall describe the strategy to provide Training including, as applicable:

a. how multiple Training components / modules may be combined into one Training solution, and the sequence for undertaking those Training activities;

b. why the Training solution is the most effective at closing the performance gap; and

c. the organisations responsible for the design, development, implementation and evaluation (ie, Verification) of Training Materials and Training Equipment.

6.2.8 Training and Assessment Specifications

6.2.8.1 The TRS shall specify, as applicable:

a. the tasks / duty for the job that have resulted in an identified performance gap, explicitly identifying the gap, including when the gap is less than the whole task;

b. *mandatory qualifications* (eg, licences) that are to be achieved as a result of successful Training and assessment;

c. *desirable qualifications* that may be achieved as a result of successful Training and assessment; and

d. the Personnel Competencies to be attained from the Training, as described in accordance with clauses 6.2.8.2 and 6.2.8.3.

6.2.8.2 The TRS shall include a table that summarises the Personnel Competencies to be attained from the Training and which details the:

a. unit code, which is a unique reference number for the UOC from the national register of vocational education and training, where the UOC and training standard already exists;

b. unit title, which is a succinct statement of the broad area of competency covered and which is expressed in terms of the outcome;

c. related duty / task numbers for the job;

d. prerequisite competencies (by unit code and unit title);

e. co-requisite competencies (by unit code and unit title); and

f. type of Training required or recommended (eg, course based, on-the-job, etc).

Note: Further explanation of competency details may be obtained from the SADL Guide and Part 2 of the Standards for Training Packages.

6.2.8.3 The TRS shall include, as annexes, specifications for the UOCs including:

a. unit code for the UOC, when applicable;

b. unit title;

c. elements of competency, being the functions that combine to form the competency;

d. required knowledge, skills and attitudes required, including the generic key competencies that underpin the competency;

e. performance criteria by which the successful achievement of the competency elements are evaluated;

f. range statement that specifies the conditions under which the related tasks will be performed; and

g. an evidence guide that states how an assessment of competency will be achieved.

6.2.9 Resource Implications

6.2.9.1 The TRS shall summarise the resources required to sustain the Training program, following introduction, including the numbers of Personnel required, the Facilities needed, and resources for the support of Training Equipment.

6.2.9.2 If a *Feasibility Analysis Report* recommends that a significant item of Training Equipment or other Support Resource may be required, the TRS shall include, or cross-reference, a business case that justifies the proposed Support Resource on a cost-benefit basis (ie, a Support Resource may be justified by use with several courses and the full business case should not be repeated in each *Feasibility Analysis Report*).

6.2.10 Risk

6.2.10.1 Risks associated with the Training strategy, to implement the Training requirements, shall be documented in the Risk Register. However, the TRS shall include a risk assessment summary (in an annex) that highlights:

a. the risk of not implementing the recommended Training solution; and

b. any significant risks to the design, development and implementation of the Training solution and the associated risk-management strategies.

6.2.11 Conclusion

6.2.11.1 The TRS shall include a conclusion regarding the recommended Training course solution and a summary of the proposed course of action for design and development.

6.3 Annexes

6.3.1.1 The TRS shall include annexes (or cross-references) for the applicable:

a. Job Task Profile (SADL product AP3);

b. Job Specifications (SADL product AP4);

c. Gap Analysis Statements (SADL product AP6);

d. Feasibility Analysis Report (SADL product AP7);

e. Risk Assessment Summary (SADL product AP2);

f. Business Case (SADL product AP10); and

g. Implementation Schedule (SADL product AP11).

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ILS-MGT-ISP-2-V5.2

2. TITLE: INTEGRATED SUPPORT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The Integrated Support Plan (ISP) describes the Contractor's strategy, plans, methodologies and processes for meeting the ILS program requirements of the Contract.

3.2 The Contractor uses the ISP to:

a. define, manage and monitor the ILS program;

b. ensure that those parties who are undertaking ILS activities understand their responsibilities, the processes to be used, and the time-frames involved; and

c. ensure that those parties who are providing data to enable ILS activities to be undertaken understand their responsibilities, the data required and the time-frames for providing that data.

3.3 The Commonwealth uses the ISP to:

a. understand the Contractor’s approach to meeting the ILS program requirements;

b. form the basis for monitoring the Contractor’s progress under the ILS program; and

c. understand the Contractor’s expectations for Commonwealth’s involvement in the ILS program.

4. INTER-RELATIONSHIPS

4.1 The ISP is subordinate to, the Project Management Plan (PMP).

4.2 The ISP shall be the single planning and controlling document for all ILS program activities and related efforts, and shall have authority over, and give direction to, any subordinate ILS plans.

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

a. Systems Engineering Management Plan (SEMP);

b. Configuration Management Plan (CMP);

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

d. the support-related data items derived from the Master Technical Data Index (MTDI), particularly the Support System Technical Data List (SSTDL);

e. Training Recommendations Report (TNGRECR);

f. Learning Management Packages (LMPs);

g. all data items associated with the design, development, delivery, Verification and Validation (V&V) and, where applicable, Acceptance of Support Resources, including (for example) the Logistic Support Analysis Record (LSAR) and the Recommended Provisioning List (RPL);

h. Quality Plan (QP); and

i. 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)1000C	*ADF Packaging*
DEF(AUST)5629C	*Production of Military Technical Manuals*

DEF(AUST)IPS-5630	*Developing S1000D Interactive Electronic Technical Publications (IETPs)*
DEF(AUST)5691	*Logistic Support Analysis*
S1000D™	*International specification for technical publications using a common source database*, Issue 5.0
SADL Guide	*Systems Approach to Defence Learning (SADL) Practitioner Guide*
	ADF Service Training Manual(s), as specified in the Statement of Work
	ADF Service Publication standard(s) for Technical Data, as specified in the Statement of Work

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The ISP 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 ISP 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 ILS Program Organisation

6.2.1.1 The ISP shall describe the organisational arrangements for the ILS program, including the identification of the individual within the Contractor's organisation who will have managerial responsibility and accountability for meeting the ILS requirements of the Contract.

6.2.1.2 Risks associated with the ILS program shall be documented in the Risk Register; however, the ISP shall describe the risk-management strategies associated with any risks where the mitigation strategy underpins the overall ILS program.

6.2.2 ILS Program Activities

6.2.2.1 The ISP shall describe the Contractor's program for meeting the ILS requirements of the Contract, including:

a. the major activities to be undertaken, when, and by whom, showing the linkages between these activities and the ILS outcomes required;

b. the integration of Subcontractors into the Contractor's ILS program;

c. the hierarchy of ILS program plans, showing the relationships between plans;

d. the processes and procedures to be used to undertake the ILS activities;

e. for any new or modified procedures, an overview of their scope and the responsibilities and timeframes for developing and approving those procedures;

f. the strategy for the use of any extant data when undertaking logistics-related analyses and Support System development;

g. the personnel (including categories, numbers and associated skills/competencies) required by the Contractor and Subcontractors to meet the ILS requirements of the Contract, including the proposed sources for obtaining those personnel;

h. the interfaces between the ILS program and the Systems Engineering (SE), the Configuration Management (CM), and Verification and Validation (V&V) programs, including the mechanisms for ensuring that ILS-related activities are integrated with

these other programs, to ensure that the objectives of the ILS program and other programs are achieved;

i. the proposed interfaces between the Commonwealth and the Contractor, including the role of ILS personnel within the Resident Personnel (RP) team, if applicable;

j. the expectations for Commonwealth input into the Contractor's ILS program; and

k. the provision of any training required by Commonwealth Personnel to enable them to undertake the review of Contractor analyses and any other expected roles identified by the Contractor, including details of proposed courses.

6.2.2.2 Standards

6.2.2.2.1 The ISP shall identify the standards (eg, DEF(AUST)5691, *Logistic Support Analysis)* to be used by the Contractor and Subcontractors to undertake the ILS program.

6.2.2.2.2 The ISP shall describe, in annexes to the ISP (with separate annexes for each standard), the Contractor's tailoring of the identified standards to meet the ILS-related requirements of the Contract.

6.2.2.2.3 The ISP shall describe how the Contractor will integrate the identified standards with each other and with other ILS-related activities to achieve the ILS-related outcomes required under the Contract.

6.2.2.3 Candidate Items

6.2.2.3.1 The ISP shall describe the processes for identifying Candidate Items.

6.2.2.3.2 The ISP shall identify the hardware and Software items for which Support Resource determination will be performed and documented. The list shall include each item's name, CWBS reference number for both the Mission System and the Support System Components (if a CWBS is required under the Contract), NATO Stock Number (if available), and reason(s) for selection.

6.2.2.3.3 The ISP shall identify the candidate items that have been the subject of previous analyses and for which the Contractor expects to only perform a Validation activity.

6.2.2.4 Verification and Validation Planning

6.2.2.4.1 The ISP shall describe the strategy for the Verification and, if required under the Contract, the Validation of the Support System and Support System Components.

6.2.3 ILS Program Data Management

6.2.3.1 Logistic Support Analysis Record

6.2.3.1.1 Where the Contract requires a Logistic Support Analysis Record (LSAR), the ISP shall:

a. describe the LSA control numbering structure to be used; and

b. identify the LSAR tables and data elements to be used to document, disseminate and control LSA data.

6.2.3.2 Data from External Sources

6.2.3.2.1 The ISP shall outline the information that the Contractor needs to obtain from organisations external to the Contractor's organisation (eg, Subcontractors, the Commonwealth, overseas agencies, and other company divisions) to conduct the ILS program.

6.2.3.3 Configuration Management

6.2.3.3.1 The ISP shall describe the approach planned to establish and maintain Configuration Control of Support Resources.

6.2.4 System Reviews

6.2.4.1 The ISP shall describe the approach planned for the conduct ILS-related System Reviews (ie, Mandated System Reviews (MSRs) and Internal System Reviews) and ILS involvement in other MSRs, necessary for effective conduct of the ILS program.

6.2.4.2 The ISP shall describe the objectives for each ILS-related System Review and the relationship between each System Review and other ILS program activities.

Note: The following clause only relates to the ILS-related System Reviews. The main governing plans for each of the Level 2 subject area clauses in the SOW address the other System Reviews (eg, the PMP addresses project management System Reviews, the SEMP addresses engineering-related System Reviews, and the CMP or SEMP addresses CM-related System Reviews).

6.2.4.3 The ISP shall detail the following information for each of the ILS-related System Reviews (cross-referring to the SEMP where appropriate), incorporating the associated SOW requirements (including entry criteria, exit criteria and checklist items) for these System Reviews and supplemented where required by the Contractor's internal processes:

a. the organisations and individuals involved in the review and their specific review responsibilities;

b. the proposed review venue;

c. the pre-requisites for conducting the review (ie, entry criteria);

d. the checklist items to be addressed during the System Review, including the documentation to be reviewed;

e. the essential review completion criteria (ie, exit criteria); and

f. the applicable Milestone criteria specified in Attachment C, Delivery Schedule.

6.2.5 ILS Sub-Programs

6.2.5.1 General

6.2.5.1.1 The ISP shall describe the Contractor's program of activities associated with, as applicable, the identification, design, development, acquisition, installation, set-to-work, commissioning, and Verification and, if required under the Contract, Validation of:

a. Spares and packaging;

b. Technical Data;

c. Training (including Training Equipment and Training Materials);

d. Support and Test Equipment (S&TE);

e. Facilities; and

f. Software support.

6.2.5.2 General Support Resource Requirements

6.2.5.2.1 The ISP shall, for each category of Support Resources required under the Contract, detail the strategy, methodology, and activities for:

a. performing item / product range and quantity analyses and to identify the locations / echelons of support (including Commonwealth locations and support contractors) where Support Resources would be located;

b. undertaking standardisation and offsetting of identified Support Resources with corresponding Support Resources already in service with the Commonwealth;

c. confirming that the proposed Spares, Packaging, S&TE, and Training Equipment are able to be accommodated, in terms of space, installation and required services at Defence facilities or within the Mission System (eg, on-board as applicable);

d. categorising each type of Support Resource based on its intended purpose, origin / supplier, management approach or other applicable criteria;

e. provisioning of the Support Resources, including Long Lead Time Items (LLTIs) and Life-of-Type (LOT) procurements;

f. the compilation and management of Codification Data (to be provided in accordance with DID-ILS-TDATA-CDATA);

g. providing and tracking of certificates of conformance, where applicable;

h. the packaging, delivery, installation, commissioning and testing of Support Resources (as applicable);

i. identification and labelling of Support Resources (eg, 'Unique ID' (UID) and bar-coding), including referencing applicable standards;

j. identification and management of security requirements, releasability issues and transportation requirements associated with classified items (eg, COMSEC);

k. identification and management of safety requirements, including Problematic Substances within the Support Resources;

l. identification and management of special transportation, handling and storage requirements for the Support Resources;

m. preparing for and enabling the Acceptance of Support Resources;

n. Validation of the provisioning list for recommended Support Resources;

o. Verification of the Support Resources;

p. the provision of any training associated with the delivery and/or set-up of the Support Resources; and

q. the identification of configuration documentation for each item of the Support Resources.

6.2.5.3 Technical Data

Note: In accordance with clause 6.1.2, the ISP should only include a summary of the approach to Technical Data when a separate TDP is required under the Contract.

6.2.5.3.1 The ISP shall describe any issues or implications for the development and delivery of, or access to, Technical Data required for the Support System, which arise from restrictions on Technical Data and Software rights, export licences, Technical Assistance Agreements, security issues, or other.

6.2.5.3.2 The ISP shall describe how existing Technical Data, which is to be delivered as a whole or incorporated into other manuals and publications that are to be delivered, will be evaluated and updated, as required, for the configuration, role, environment and target users of the Materiel System.

6.2.5.3.3 In addition to clause 6.2.5.2, the ISP shall describe:

a. the Contractor's strategy, methodology and processes for the identification, development and delivery of publications, including the procedures to identify required amendments to existing Commonwealth publications and other Technical Data;

b. the software tools to be applied to the generation and interpretation (authoring and viewing) of Technical Data;

c. the procedures, by category of Technical Data, for the receipt, review, Configuration Control, amendment, production and delivery of all Technical Data for the Mission System and Support System;

d. the procedures for the management and update of the MTDI, including the SSTDL;

e. the strategy, methodology and processes for validating the MTDI, including the SSTDL;

f. the standards, by Technical Data category, for the preparation of Technical Data;

g. the procedures to identify the amendments required to existing Commonwealth publications and the management of amendment incorporation;

h. the strategy, methodology and processes to meet any associated regulatory / assurance requirements as they relate to Technical Data;

Note: The terms 'validate' and 'verify' in the following sub-clauses are derived from DEF(AUST) 5629C and DEF(AUST)IPS-5630, are unique to the standards, and do not apply to other sections of the Contract.

i. the strategy, methodology and processes for the Contractor to validate Technical Data, including an indicative schedule and the standards to be used; and

j. the proposed strategy and methodology for the Contractor to assist the Commonwealth in verifying Technical Data.

Note: The term 'Business Rules' in the following clause has the meaning given in DEF(AUST)IPS-5630.

6.2.5.3.4 If S1000D Technical Data is applicable to the Contract, the ISP shall, for Technical Data that is produced as Common Source Database (CSDB) Objects in accordance with DEF(AUST)IPS-5630 and S1000D™:

a. include (as an annex) a Business Rules Index that:

(i) includes the (common) Defence Business Rules specified in DEF(AUST)IPS-5630 and 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;

Note: Commonwealth agreement to the Contractor-proposed BRDP will be provided through Approval of the ISP.

(ii) specifies 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"; and

(iii) if applicable, identifies the Business Rules applicable to the update of legacy publications produced in previous versions of S1000D (ie, prior to issue 5);

b. describe the methodology and processes to validate that the structure and set of the eXtensible Markup Language (XML) accords with the required Business Rules; and

c. describe the method of data exchange and transfer, including data transfer points, in accordance with DEF(AUST)IPS-5630, or as otherwise agreed by the Commonwealth.

6.2.5.4 Training

Notes:

a. In accordance with clause 6.1.2, the ISP should only include a summary of the approach to Training when a separate TSP is required under the Contract.

b. While the SADL Guide recognises different methods of learning, the Contract seeks formal Training methods that can be delivered by a Defence unit or support contractor.

6.2.5.4.1 The ISP shall summarise the objectives, scope, constraints, global risks and assumptions for the Contractor's learning development and Training systems implementation activities.

6.2.5.4.2 The ISP shall list the positions and personnel, or groups of personnel, involved in the learning development program, the delivery of the Training system solution, and the implementation of any Training courses delivered under the Contract. This list shall contain the following information:

a. position title or role;

b. names of personnel (if available) in management / team leader roles;

c. formal qualifications; and

d. as applicable, teaching experience and related technical / subject matter experience.

6.2.5.4.3 In addition to clause 6.2.5.2, the ISP shall describe the Contractor's strategy, methodology, standards and processes (highlighting any differences from the SADL and any ADF Service Training Manuals identified in the SOW) for undertaking and managing, as applicable:

a. the analysis of performance needs and identification of recommended Training solutions (intervention solutions) including:

Note: Refer to the Analyse Phase in the SADL for a description of a full-scale analysis process.

(i) the identification of job / task requirements and the specification of new / modified performance needs for operators and support Personnel;

(ii) analysis of the gap between baseline competencies (including skills, knowledge, attitudes and behaviours) and the identified performance needs;

(iii) the identification of learning / Training methods to satisfy the performance needs, and the risk and feasibility analyses for their implementation; and

(iv) the identification and evaluation of existing LMPs, and the need for new or modified LMPs, leading to the recommendation of Training requirements (as required to be delivered in the TNGRECR);

b. the reuse, update, or design and development of the LMPs, including:

Note: If an existing LMP requires substantial update, or a new LMP is to be developed, refer to the SADL for detailed guidance for the sections of an LMP.

(i) learning management information;

(ii) the course curricula, including the derivation / review of required learning outcomes and course design;

(iii) the identification and evaluation of major resource requirements, including personnel and Training Equipment requirements; and

(iv) the development and/or update of Training Materials (including learning and assessment materials);

c. when applicable, accreditation against nationally recognised Units of Competency.

6.2.5.4.4 The ISP shall describe any additional standards, methodologies and processes to be used for the development of deliverables under the Contract, including:

a. the Training Requirements Report (TNGRECR);

b. draft Learning Management Packages (LMPs);

c. complete (final) LMPs, including Training Materials;

d. the Training Materials List (TML);

e. the Training Equipment list as part of the Recommended Provisioning List (RPL); and

f. Training course evaluation reporting requirements.

6.2.5.4.5 The ISP shall describe the strategy, methodology and processes to be used for the implementation and evaluation of the Training and Training Support solution, including (as applicable):

a. the development and implementation of Training Equipment;

b. Training courses to be delivered under the Contract, including the conduct of any trial courses; and

c. Training course evaluation requirements, including in relation to the V&V program and the Acceptance of Training and Training Support solutions under the Contract.

6.2.5.5 Facilities

6.2.5.5.1 In addition to clause 6.2.5.2, the ISP shall detail the Contractor's strategy, methodology, and processes for:

a. confirming the suitability of the existing Commonwealth facilities for the Contractor's proposed Mission System and associated Support System Components; and

b. if required under the Contract, undertaking a facilities requirements analysis (and documenting outcomes in the Facilities Requirements Analysis Report (FRAR)).

6.2.5.5.2 The ISP shall detail the applicable requirements for any Facilities to be built or modified, by the Contractor or the Commonwealth, including specific requirements for:

a. security (including physical security, emanations security and cyber security);

b. Work Health and Safety; and

c. Environmental Outcomes.

6.2.6 ILS Program Traceability Matrix

6.2.6.1 The ISP shall include a traceability matrix, showing how the ILS requirements of the Contract will be accomplished by the Contractor's ILS program.

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-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-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-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.
QAR authority reference no.

Applicant requests decision by

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-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-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.