DATA ITEM DESCRIPTION

1. DID NUMBER: -
2. TITLE: MATERIEL SYSTEM SECURITY mANAGEMENT pLAN
3. DESCRIPTION and intended use

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

The Contractor uses the MSSMP to:

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

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

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

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

The Commonwealth uses the MSSMP to:

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

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

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

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

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

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

1. INTER-RELATIONSHIPS

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

Systems Engineering Management Plan (SEMP);

Integrated Support Plan (ISP);

Configuration Management Plan (CMP); and

Quality Plan.

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

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

Support System Specification (SSSPEC);

System Architecture Description (SAD);

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

the Software-related data items required under the Contract;

Mission System Technical Documentation Tree (MSTDT);

Support System Technical Data List (SSTDL);

ADF regulatory / assurance plans;

Certification Plan (CERTP);

Electromagnetic Environmental Effects Management Plan (E3MP);

System Safety Program Plan (SSPP);

Disposal Plan (DISP);

Verification and Validation Plan (V&VP); and

Verification Cross Reference Matrix (VCRM).

1. APPLICABLE DOCUMENTS

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

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

|  |  |
| --- | --- |
| 1. Governing Security Documents | 1. (see the Glossary for the definition of this term) |
| 1. ANP4605 | 1. Navy Cyberworthiness |
| 1. AFSMAN | 1. Air Force Security Manual, Volume 1 |
|  | 1. National Institute of Standards and Technology (NIST), ‘Cybersecurity Framework (CSF)’, Version 2.0, February 26, 2024 |
| 1. AS/NZS ISO 31000:2018 | 1. Risk Management – Principles and Guidelines |
| 1. NIST SP 800-30 | 1. Guide for Conducting Risk Assessments, Revision 1, September 2012 |
| 1. NIST SP 800-37 | 1. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018 |
| 1. NIST SP 800-53A | 1. Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5, January 2022 |
|  | 1. ACSC Publication, ‘Strategies to Mitigate Cyber Security Incidents’, February 2017 |
|  | 1. ACSC Publication, ‘Strategies to Mitigate Cyber Security Incidents – Mitigation Details’, February 2017 |
| 1. ISO/IEC 27001:2022 | 1. Information security, cybersecurity and privacy protection – Information security management systems – Requirements |
| 1. ISO/IEC 27032:2023 | 1. Cybersecurity – Guidelines for internet security |
| 1. ISA/IEC 62443 series | 1. Security for Industrial Automation and Control Systems |
| 1. ISO/IEC 27005:2022 | 1. Information security, cybersecurity and privacy protection – Guidance on managing information security risks |
| 1. Defence ICT/Cyber SCRM Framework | 1. The Defence ICT/Cyber Procurement Supply Chain Risk Management Framework, October 2020 |
|  | 1. CASG Risk Management Product Risk Matrix |

1. Preparation Instructions
   1. Generic Format and Content

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

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

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.

* 1. Specific Content
     1. Overview

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

defining the scope and purpose of the MSSMP, including:

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

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

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

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

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

System Owner;

security requirements authorities;

Security Authorisation authorities; and

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

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

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

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

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

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

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

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

* + 1. Requirements

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

* + 1. Organisation and Communication

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

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

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

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

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

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

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

* + 1. Security Risk Management

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

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

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

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

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

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

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

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

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

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

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

* + 1. System Security Design Processes

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

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

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

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

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

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

analysis of threats and vulnerabilities;

implementation of system security controls and response mechanisms;

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

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

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

continuous review of threats and vulnerabilities; and

implementation of updates and control;

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

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

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

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

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

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

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

the expected outcomes associated with undertaking each activity or process;

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

how the outcomes will be documented;

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

the expected role of the Commonwealth in reviewing the outcomes.

* + 1. System Security and Support

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

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

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

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

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

countermeasures against malicious code;

intrusion detection strategies and detection mechanisms;

audit and event log analysis and alerting;

system integrity checking (system characterisation);

vulnerability monitoring, assessments and patching;

periodic revalidation of security controls;

user access management;

periodic audit of intrusion detection procedures;

systematic user Training and awareness programs; and

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

* + 1. Security Authorisations and Verification & Validation

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

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

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

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

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

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

mapping of cyber attack and engagement surfaces;

the confidentiality, integrity and availability of systems and data; and

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

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

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

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

* + 1. System Security Tools

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

* + 1. System Security Schedule

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

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