DATA ITEM DESCRIPTION

1. DID NAME: -
2. TITLE: SYSTEM SECURITY PLAN
3. DESCRIPTION and intended use

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.

The SSP serves two purposes:

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

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.

The Contractor uses the SSP:

1. 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;
2. 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;
3. 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;
4. to describe the plan to Verify that the implemented controls for a SSoI have been properly implemented and are effective; and
5. 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.

The Commonwealth uses the SSP:

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;

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;

to identify and understand the Commonwealth’s involvement in the Contractor’s ICT/cyber-security program, including the monitoring of the Contractor’s program;

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

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.

1. INTER-RELATIONSHIPS

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

1. Systems Engineering Management Plan (SEMP);
2. Contractor Engineering Management Plan (CEMP);
3. Materiel System Security Management Plan (MSSMP);
4. In‑Service Security Management Plan (ISSMP);
5. System Safety Program Plan (SSPP); and
6. In-service Materiel Safety Plan (IMSP).

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

1. System Specification (SS) for the SSoI including, if applicable, the associated Cyber Security Assurance Basis (as a component of this specification);
2. System Architecture Description (SAD);
3. Software List (SWLIST);
4. the security-related data items required under the Contract (other than those identified under clause 4.1);
5. the safety-related data items (eg, Hazard Log, Safety Case Report (SCR) and Materiel Safety Assessment (MSA)); and
6. 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).
7. APPLICABLE DOCUMENTS

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.

|  |  |
| --- | --- |
| 1. Governing Security Documents | 1. (see the Glossary for the definition of this term) |
| 1. NIST SP 800-82 | 1. Guide to Operational Technology Security, Revision 3, September 2023 |
| 1. ISA/IEC 62433 series | 1. Security for Industrial Automation and Control Systems |
| 1. Australian Government Australian Cyber Security Centre (ACSC) Guidance Documents | 1. Strategies to Mitigate Cyber Security Incidents, February 2017 2. Strategies to Mitigate Cyber Security Incidents – Mitigation Details, February 2017 3. System Security Plan (SSP) Annex Template |

1. Preparation Instructions
   1. Generic Format and Content

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’.

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.

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.

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.

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).

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.

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 – Part 1
     1. Scope

The SSP shall define the scope of the SSP, identifying the SSoI and the associated ToSA(s) being addressed through the plan.

The SSP shall identify any assumptions and constraints associated with the information provided in the SSP, including (where applicable) how and when:

the identified assumptions will be validated; and

the identified constraints will be ameliorated.

* + 1. System and Organisational Stakeholders

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.

* + 1. General System Overview

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.

The SSP shall identify and describe the component subsystems of the SSoI, including:

internal network interface diagram(s);

system block diagram(s);

internal system interface block diagram(s); and

system / software architecture diagram(s).

The SSP shall identify the ToSAs associated with the SSoI, including in relation to component subsystems of the SSoI and the external systems.

The SSP shall list:

all system-wide operating systems and software in use for the SSoI; and

the proposed system-wide security features (eg, cross-domain solutions, firewalls, and procedural controls).

* + 1. Security Architecture

When the Contract has specified the delivery of a System Architecture Description (SAD), the Security Architecture description required by this clause 6.2.4:

shall be consistent with the architectural views defined in the system architecture model underpinning the SAD; and

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.

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:

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.

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:

the authorisation for the connection to other systems or the sharing of information between those systems; and

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.

System Connectivity to Development or Test Environments: Describe any connectivity to development or test environments and how separation is maintained.

Accreditation Status of External Systems: Provide a table that details the ICT and cyber Security Authorisations of existing external systems, where interconnections are proposed.

Internal Data Flow Description and Protocols: Provide a description of the data flows internal to the SSoI, including their protocols. Include relevant diagrams.

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.

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.

User Matrix: Detail the types of roles/users, their access levels, responsibilities, clearances required and who authorises their access to the SSoI.

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:

physical security;

EMSEC;

ICT security; and

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.

* 1. Specific Content – Part 2
     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.

The SSP shall include, as an annex to the SSP, a statement of applicability for each ToSA covered by the plan, which identifies:

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;

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);

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);

any additional controls that need to be implemented as an outcome of the risk assessment for the ToSA(s) captured in the associated SRMP;

any exemptions that have been granted, including (if known) the details of when and by whom;

any approvals to operate that have been granted, including (if known) the details of when and by whom; and

through the inclusion of cross-references to the relevant risks in the associated SRMP, which risks have been mitigated by each control.

* + 1. System Security Plan – Design and Implementation Phases

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:

human system integration,

standard operating procedures,

incident management and disaster recovery, and

Cyber Supply Chain management.

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.

The SSP shall:

identify the eight mitigation strategies from the ACSC Essential Eight Maturity Model and associated ACSC guidance documentation;

identify the assessed maturity level for the SSoI against each of these strategies, including describing the implementation status of each control; and

provide the associated justification for this assessment.

The SSP shall describe the plan to Verify that the controls for each ToSA have been properly implemented and are effective, including references to:

industry, regulatory and legislative compliance requirements; and

the applicable V&VP, VCRM and associated data items (eg, ATPs).

* + 1. System Security Plan – ICT and Cyber Security Authorisation Phases

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.