DATA ITEM DESCRIPTION

1. DID Number: DID-ENG-SOL-CSCRP-V5.3
2. TITLE: Cyber Supply Chain RISK PLAN
3. DESCRIPTION AND INTENDED USE

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).

The Contractor uses the CSCRP:

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);

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

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

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.

The Commonwealth uses the CSCRP:

1. 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;
2. 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);
3. to identify and understand the Commonwealth’s involvement in the Contractor’s Cyber Supply Chain program, including the monitoring of the Contractor’s program;
4. 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
5. 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.
6. INTER-RELATIONSHIPS

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

Project Management Plan (PMP);

Support Services Management Plan (SSMP);

Systems Engineering Management Plan (SEMP);

Contractor Engineering Management Plan (CEMP);

Materiel System Security Management Plan (MSSMP); and

In‑Service Security Management Plan (ISSMP).

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

1. System Architecture Description (SAD), which identifies the product breakdown structure or system breakdown structure for the relevant SSoIs;
2. Software List (SWLIST);
3. Configuration Status Accounting Report (CSAR);
4. any provisioning lists required under the Contract (eg, the Recommended Spares Provisioning List (RSPL) or the Recommended Provisioning List (RPL)); and
5. the security-related data items required under the Contract (other than those identified under clause 4.1).
6. APPLICABLE DOCUMENTS

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

|  |  |
| --- | --- |
| 1. Governing Security Documents | 1. (see the Glossary for the definition of this term) |
| 1. CTIS | 1. Australian Cyber Security Centre (ACSC) Cyber Threat Intelligence Sharing (CTIS) platform |
| 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. ISO/IEC 27005:2022 | 1. Information security, cybersecurity and privacy protection – Guidance on managing information security risks |
| 1. ASIO 18-9938 | 1. Security Manager’s Guide: Supply Chain Security, 2018 |
|  | 1. ACSC Publication, ‘Cyber Supply Chain Risk Management’, May 2023 |
|  | 1. ACSC Publication, ‘Identifying Cyber Supply Chain Risks’, May 2023 |
|  | 1. ACSC Publication, ‘Cloud Computing Security Considerations’, October 2021 |
| 1. Defence ICT/Cyber SCRM Framework | 1. The Defence ICT/Cyber Procurement Supply Chain Risk Management Framework, October 2020 |

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’.

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).

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.

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).

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.

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. Summary

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

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;

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

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

the significant conclusions of the CSCRP.

* + 1. Scope

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:

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

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

(hereinafter known as ‘**Vulnerable Components / Services**’).

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.

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.

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.

* + 1. Supply Chain Risk Assessment

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

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:

risks due to foreign control or interference;

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);

risks due to lack of transparency;

risks due to access and privileges; and

risks due to poor business practices.

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

the component/service title and unique identifier;

a component/service description;

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

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

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

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.

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

the treatment recommendation(s);

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

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

the residual risk exposure.

* + 1. 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.

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

reduce the likelihood and/or reduce the consequence; or

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.

Each risk-treatment plan shall include:

the position responsible within the Contractor’s or supplier’s organisation;

a brief description of the required scope of work;

the envisaged schedule for implementation, including the associated milestones;

the likely resources;

the envisaged cost; and

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

* + 1. Residual Risk Exposure

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:

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

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

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

the Contractor’s risk acceptance authority by title and organisation, and date of acceptance;

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

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