DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-CSCR-V5.3
2. TITLE: CYBER Security CASE REPORT
3. DESCRIPTION AND INTENDED USE

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.

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]](#footnote-1), met. The CSCR documents the consultation outcomes between the Commonwealth and Contractor and formal risk acceptance decisions made.

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

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;

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

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.

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

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;

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

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

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

1. INTER-RELATIONSHIPS

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

Systems Engineering Management Plan (SEMP);

Contractor Engineering Management Plan (CEMP);

Materiel System Security Management Plan (MSSMP); and

In-Service Security Management Plan (ISSMP).

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

Cyber Supply Chain Risk Plan (CSCRP);

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

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).

1. 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. 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 CSCR shall summarise these aspects and refer to the other data item as part of the body of evidence.

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. General

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.

The CSCR shall include an executive summary.

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

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

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.

* + 1. System Security Program

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).

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

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;

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

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);

details of relevant Security Authorisations; and

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

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).

* + 1. SSoI Cyber-Security Assessment

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.

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 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;

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

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

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:

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;

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

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

validate the performance of cyber security controls;

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;

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

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;

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

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.

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.

1. Reference to ‘will be’ acknowledges that some measures can only be established through Defence processes and training. [↑](#footnote-ref-1)