Tender DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-CSAI-V5.2
2. TITLE: CYBER SECURITY ASSESSMENT INFORMATION
3. DESCRIPTION AND INTENDED USE

The Cyber Security Assessment Information (CSAI) provides the necessary security information in relation to the Mission System solution (**‘System Solution’**) to enable the Commonwealth to:

judge the cyber-security risks and vulnerabilities associated with the System Solution, including when integrated into, or with, other system(s) and equipment;

incorporate the information into its broader security arguments for any system(s) into which the System Solution is being integrated (eg, for the purposes of achieving Information and Communications Technology (ICT) and cyber Security Authorisations for the system(s)); and

meet its security obligations under both Defence and Government policy requirements, including as required by the respective security authorities.

The Contractor uses the CSAI to provide the necessary information required by the Commonwealth for the purposes of ICT and cyber security, as set out in clause 3.1.

The Commonwealth uses the CSAI:

to determine whether the cyber threats to Defence operations and system integrity associated with the System Solution, as set out in the Contract, have been identified and addressed;

to understand any required changes to existing components of the System Solution or to a system into which the System Solution will be installed/integrated to address ICT and/or cyber security risks arising out of the use of the System Solution;

when applicable, as a basis for evaluating System Solution security prior to Acceptance of Supplies; and

as the basis for identifying, assessing and managing ICT and cyber risks associated with the System Solution.

1. INTER-RELATIONSHIPS

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

Project Management Plan (PMP);

Systems Engineering Management Plan (SEMP);

Software Management Plan (SWMP);

Support Services Management Plan (SSMP); and

Contractor Engineering Management Plan (CEMP).

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

Design Documentation; and

Technical Data List.

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. NIST SP 800-53A | 1. Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5, January 2022 |
| 1. ISA/IEC 62443 series | 1. Security for Industrial Automation and Control Systems |
| 1. NIST CSF 2.0 | 1. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Version 2.0, February 26, 2024 |
|  | 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 CSAI shall 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. System Solution Design Information

The CSAI shall provide a general description of the System Solution, 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 System Solution interfaces, including providing a brief description of the purpose of the interactions between the System Solution and each external system.

If known by the Contractor, the CSAI shall include a brief (one to three paragraphs) general description of the security environment that the System Solution operates within, including the context of that environment on a location basis (eg, when the System Solution is part of a larger system). This description shall include any environmental or technical factors that raise special security concerns.

For each of the interfaces to external systems, the CSAI shall describe the technical implementation of the data flows between the System Solution and the external systems, including where data is stored and transiting to, protocols, and what protection the data is given. This information only needs to be provided from the perspective of the System Solution.

The CSAI shall identify and describe the component subsystems of the System Solution, including:

internal network interface diagram(s);

System Solution block diagram(s);

internal System Solution interface block diagram(s); and

system / software architecture diagram(s).

* + 1. Security Controls

The CSAI shall describe the security controls implemented by the System Solution, including reference to the security controls from the ISM, DSPF and other applicable standards (eg, ISA/IEC 62443 or NIST 800-53A for Operational Technology Equipment) that are, and are not, applicable to security for the System Solution and the associated rationale for this assessment. This description shall address the controls applicable during System Solution build, operations and support to ensure the confidentiality, integrity and availability of data and information processed, stored and/or communicated by the System Solution.

The CSAI shall:

identify the eight mitigation strategies from the Essential Eight Maturity Model;

identify the assessed maturity level for the System Solution against each of these strategies; and

provide the associated justification for this assessment.

* + 1. Security Risk Assessment

The CSAI shall include a security risk assessment for the System Solution, which shall be undertaken in accordance with the risk management processes set out in the PMP or SSMP (as applicable) and using the consequence and likelihood descriptors for Security and Cyber from the CASG Risk Management Product Risk Matrix.

The CSAI shall address security risks in relation to:

confidentiality, integrity and availability of systems and data; and

the cybersecurity functions of Identify, Protect, Detect, Respond and Recover (as these terms are defined in NIST CSF 2.0).

authorised users.

The CSAI shall include the following information for each security risk:

title and unique identifier;

brief description, including threat type, likely source and characteristics;

asset(s) affected (ie, which subsystems are vulnerable to the threat);

overview (ie, a short description of how the threat sources and assets link to the threat for the System Solution);

likelihood of occurrence;

consequence of realisation in terms of confidentiality, integrity and availability of information, and the impacts of these three on the mission, safe operation of the Mission System, information security, or some other function or combination of functions;

existing controls;

resultant risk exposure;

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

treatment owner;

treatment recommendation(s);

residual likelihood of occurrence;

residual consequence of realisation; and

residual risk exposure.

The CSAI shall include an aggregate or summary of the overall security risk for the System Solution.