GUIDANCE PAGES TO BE DELETED WHEN PUBLISHED

ASDEFCON (SUPPORT)

SECTION 1: GUIDANCE FOR DSD-ENG-SEC

(SYSTEM SECURITY SERVICES)

Status: Optional

Purpose: To identify requirements for security Services for Security Systems-of-Interest (SSoIs), their Targets of Security Assessment (ToSAs) (if applicable), and other Digitally Enabled Systems and Equipment (DESE) and Software.

Policy: Refer to the definition of Governing Security Documents in the Glossary.

Guidance: This DSD is required when the scope of security Services will involve the Contractor having overall security responsibility for the Mission System(s) identified in Annex A to the SOW, in those circumstances where the Contractor is:

1. the Original Equipment Manufacturer (OEM) or the Design Authority; and/or
2. required to provide system-level security responsibilities coordinated through a Technical Support Network (TSN) or Design Support Network (DSN).

In general, this DSD should not be invoked where:

1. the Contractor will not have system-level responsibilities for a Mission System (eg, the proposed Contract is for support of a range of Repairable Items (RIs) only); or
2. the Mission System and/or other Products Being Supported are not complex, the security implications associated with the use of the Products is not significant (eg, as determined through the assessed Business Impact Levels (BILs)), or another party has overall system-level responsibilities and the Contractor will simply be providing information (as part of the Services) to that other party to enable them to perform their security responsibilities.

If a decision is taken to not invoke this DSD, the DSD should be utilised as a source of applicable clauses to incorporate security-related Services into other DSDs (eg, DSD-ENG-SERV or DSD-MNT-SA) so that the scope of the Contractor’s security responsibilities is clear and will enable Commonwealth security obligations to be met.

DSD-ENG-SEC addresses all aspects of system security, including physical security, Emanation Security (EMSEC), Information and Communications Technology (ICT) security, cyber security and, if applicable, personnel security (ie, when Contractor Personnel will be responsible for operating, maintaining or upgrading a system/product). System security involves security as it applies to the systems, equipment and Software identified as Products Being Supported at Annex A to the SOW, but does not include the programmatic and contract-management aspects of security, which are addressed through SOW clause 3.13 and COC clause 11.10.

The four main categories of system security are identified separately because they typically involve different authorities in relation to Security Authorisations, as follows:

1. physical security: as identified under Principle 73 of the Defence Security Principles Framework (DSPF) (Physical Security Certification and Accreditation);
2. EMSEC: the delegate authorised by the Capability Manager or Australian Signals Directorate (ASD), depending upon the security levels involved;
3. ICT security: Defence Cyber and Information Assurance Branch (DCIAB) in Joint Capabilities Group (JCG); and
4. cyber security: the System Owner delegated by the relevant Capability Manager, with support and input from DCIAB in JCG, noting that the Chief of Joint Capabilities (CJC) is the ADF Cyberworthiness Authority.

Personnel security is principally addressed through COC clause 11.10, but has also been explicitly included in this DSD because Contractor Personnel form part of the Support System, which is one of the SSoIs. This approach enables any specific security issues with Contractor Personnel (eg, any implications associated with a configuration change to the Mission System) to be addressed in an ongoing way as part of the security Services.

There are a number of key terms that underpin and help to define the scope of the security Services, as follows:

1. Governing Security Documents;
2. Security Authorisation;
3. Security System of Interest (SSoI); and
4. Target of Security Assessment (ToSA).

Drafters should familiarise themselves with these terms before starting to amend the security clauses in this DSD, particularly the interactions between the terms ‘SSoI’ / ‘ToSA’ and the terms ‘Product’ and ‘Products Being Supported’. In particular, attention is drawn to the fact that SOW Annex A does not include a column in any of the tables to identify whether particular Products Being Supported are the subject of security Services. While there is an inference (eg, due to the inclusion of the DSD within Engineering Services) that the ‘Engineering Responsibility (Eng. Resp.)’ column in SOW Annex A would also apply to system security Services, this is not the case. The determination as to the Products that are the subject of security Services is defined through clause 6.1.1.1 of this DSD.

A significant proportion of the work required under this DSD supplements the work required under the main body of the SOW and other DSDs, such as DSD-ENG-SERV, DSD-ENG-SW and DSD-MNT-SA. As such, where the work is identified as an S&Q Service in the main DSD (eg, Developmental Activities for Major Changes in clause 6.2.5 of DSD-ENG-SERV), the security-related work for this activity is also undertaken as an S&Q Service. There is only one clause in DSD-ENG-SEC that identifies an S&Q Service, which is clause 6.2.10 relating to security advisory Services, and as such, there are no decisions to be made in this DSD in relation to deciding the payment methods for any of the security Services.

For further guidance on particular aspects of security, refer to the following information from the CASG intranet:

1. Security For Projects:

<http://modelpedia.dpe.protected.mil.au/PublishedWebsite/LatestFinal/%7B5E812EBC-90FE-4E4C-9064-3810D9E9C084%7D/Item/A7FCF0FC-1A2D-44BD-8D9B-4F10BC88C90B>; and

1. JCG Cyber Security Awareness intranet site at:

<http://drnet/defence/cybersecurity-awareness/Pages/default.aspx>

1. CASG Cyber Security Community of Practice (CoP), particularly the Cyber Security Guide, at:

<http://collab/CASG/Home/CyberSecurity/SitePages/Home.aspx>.

While the first location above is mainly applicable to projects (as per the name), it does have a number of useful links to the various security intranet pages.

Related Clauses/Documents:

DSD-ENG-SERV

DSD-ENG-CM

DSD-ENG-SW

DSD-MNT-SA

Refer also to guidance for individual clauses

Optional Clauses: None

# 5 Applicable Documents

Status: Core

Purpose: To identify the authoritative documents applicable to the system security Services.

Policy: Refer to the definition of Governing Security Documents in the Glossary.

Guidance: Drafters are to:

1. firstly, amend the definition of Governing Security Documents in the Glossary to suit the requirements of the Contract in accordance with the guidance provided below; and
2. only after having finalised the definition of Governing Security Documents, amend the list of applicable documents in clause 5 to identify any additional documents that will end up being specifically referenced in the DSD, noting that the various Data Item Descriptions (DIDs) include an array of applicable documents that do not need to be included here.

The template definition of Governing Security Documents includes both Government and Defence security policies, namely the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), DSPF, Essential Eight Maturity Model (E8MM), Security Classification and Categorisation Guide (SCCG) at Attachment J to the COC, optional policies in relation to EMSEC, and the ability for drafters to add Service-specific policies.

The definition should be amended to remove reference to any EMSEC standards that are not applicable to the required scope of work. If this is unclear to the drafter, they should refer to the applicable Service-specific EMSEC specialists. Additionally, Service-specific standards can be added, such as the Air Force Security Manual (AFSMAN) and ANP4605 ‘Navy Cyberworthiness’. Commercial standards should not be included because of the implications for scope and contract management through the operation of clause 6.1.2 (see guidance below), but they may be included in the list of applicable documents in clause 5.

The documents included in either location (the definition or clause 5) need only be identified by their number and title. Other than the policy documents identified in the definition of Governing Security Documents, drafters should not include references to Defence policy in either location, unless the policy explicitly states its application by contractors, because these are open to interpretation within a contract and their applicability is often limited to Defence personnel.

Drafters should note that the references identified in clause 5 are only applicable to the extent specified in the DSD. Clause 6.1.2 pulls the Governing Security Documents into the DSD; however, if other applicable documents are incorporated into clause 5:

1. they may need to be tailored to identify the portion of the applicable documents that are relevant to the system security Services; and
2. existing clauses will need to be tailored or new clauses will need to be introduced to refer to them.

Once both areas have been tailored, the list of applicable documents should be suitable for all Products included within the scope of security Services, the different types of security Services required, the domain, and the Services required by the DSD once tailored.

Related Clauses/Documents:

Definition of Governing Security Documents in the Glossary.

Optional Clauses: None

# 6.1.1 Scope

Status: Core

Purpose: To identify the scope of system security Services to be provided under this DSD.

Policy: Refer to the definition of Governing Security Documents in the Glossary.

Guidance: Clause 6.1.1.1 defines the scope of system security Services required under this DSD by summarising the range of Products for which system security Services are to be provided. As stated earlier, while the clause refers to SOW Annex A, where the individual Products are listed, it does not use SOW Annex A to identify whether security Services are applicable to those Products. Instead, the security Services are applicable to any Products that are, or form part of, an SSoI or ToSA and which:

1. could be susceptible to security vulnerabilities and/or
2. are the subject of, or included within the scope of, a Security Authorisation.

The scope of Products also includes (at clause 6.1.1.1b) any Products required by the Contractor to undertake the system security Services, such as may be required for security monitoring. This limb of the clause ensures that these additional Products will be incorporated into the scope of work, and the associated payments under the Contract, without having to be explicitly identified in SOW Annex A.

Clause 6.1.1.1 needs to be tailored to remove reference to any Products for which system security Services are not applicable, such as to remove reference to the Mission System if there are no Mission Systems identified in SOW Annex A and to remove any Security Authorisations in clause 6.1.1.1a(vii) that are not applicable to the identified Products.

Similarly, clause 6.1.1.2 needs to be tailored to incorporate the applicable categories of system security. In some cases, this will be obvious because the requirements will flow from any precursor or linked Contract (Acquisition), but if drafters are unsure, they should seek guidance from the relevant security authorities and Service-specific centres of expertise.

In relation to physical security, drafters should keep in mind that physical security associated with the provision of the Services is governed by clause 11.10 of the COC and clause 3.13 of the SOW. The physical security aspects included within the scope of this DSD only include those aspects relating to:

1. the physical security design of a SSoI / ToSA, as captured within the Security Authorisation for physical security for the SSoI / ToSA; or
2. the Contractor’s additional responsibilities when the Contractor is either operating a SSoI / ToSA, or performing Maintenance on the SSoI / ToSA on a Defence establishment (eg, in relation to security vulnerabilities and security incidents).

Related Clauses/Documents:

Draft SOW clause 2.1, Scope of Work

SOW Annex A, Products Being Supported

DSD-ENG-SERV, DSD-ENG-CM and DSD-ENG-SW

DID-SSM-ISSMP

Optional Clauses: None

# 6.1.2 System Security Standards

Status: Core

Purpose: To:

1. set out the process for ensuring that, to the extent practicable, security-related Services are always being conducted against the latest version of the Governing Security Documents; and
2. provide a ‘circuit-breaker’ when any changes to the Governing Security Documents result in a material change to the Contractor’s scope of work.

Policy: Refer to the definition of Governing Security Documents in the Glossary.

Guidance: In general, security Services must always be conducted against the most current versions of the Governing Security Documents. The increasing emphasis on cyber security, particularly the issues to be addressed and the mechanisms to be employed, means that Government and Defence security policy (and legislation) is evolving quickly, with a number of these core security policy documents being on a three-monthly update cycle.

COC clause 1.2.1i states: “In the Contract, unless the contrary intention appears: [...] a reference to a specification, publication, Commonwealth policy or other document is a reference to that specification, publication, Commonwealth policy or document, in effect on the Effective Date specified in the Details Schedule, or alternatively, a reference to another version of the document if agreed in writing between the parties”.

The ‘agreed in writing’ part of this clause includes notices, Approved Minutes of meetings, and other parts of the Contract such as the Glossary at Attachment M, which includes the words ‘as amended from time to time’ against a number of these standards, including the DSPF, E8MM, ISM and PSPF. Notwithstanding, it is easy for well-meaning drafters to incorporate specific versions of these documents into various part of the SOW (creating inconsistencies[[1]](#footnote-1)) and/or for tenderers to negotiate these words out of the resultant Contract because they perceive them as ‘unfair’.

Clause 6.1.2 specifies that the Contractor must comply with the latest version of the security documents, which aligns with the process that each of the Defence security authorities or their representatives will follow for the purposes of seeking associated Security Authorisations (ie, the assessment will always be conducted against the versions of the relevant security policies and practices that are in place at the time).

The clause also provides a timeframe (10WDs) for the Contractor to notify the Commonwealth of any material changes to their scope of work arising out of a change to a Governing Security Document. The Contractor is required to provide supporting evidence to justify that the change does materially increase their scope of work or otherwise impacts on their ability to perform their contractual obligations.

If the Commonwealth Representative is satisfied that a change to a Governing Security Document will cause a material change in scope, then clause 6.1.2.1e requires the parties to work together to agree a CCP to address the impact. This approach is a fair one, given that changes to security requirements can have significant cost and schedule implications. On a recent procurement, for example, there was a change to the data aggregation requirements, which (if implemented) would have resulted in a large cost increase and schedule extension. By having a framework similar to this one, the Commonwealth project team was able to negotiate a better outcome with the relevant security authority, which avoided the cost and schedule impacts.

Drafters should not amend this clause, without seeking specialist commercial advice, due to its sensitivity.

Related Clauses/Documents:

Definition of Governing Security Documents in the Glossary

Optional Clauses: None

# 6.2.1 Security Management Planning

Status: Optional

Purpose: To identify the planning requirements for the system security Services.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: If system security Services are required, then an appropriate level of planning is required to manage the program and to provide the Commonwealth Representative with an applicable level of visibility. For this DSD, however, there are no options to ‘roll up’ the In-Service Security Management Plan (ISSMP) into either the Contractor Engineering Management Plan (CEMP) or the Support Services Management Plan (SSMP). The rationale for this approach is that the DSD and the ISSMP go together: if the scope of work warrants the inclusion of this DSD, then the ISSMP should be included; if the scope of work does not warrant the inclusion of this DSD, then any relevant clauses should be included in other DSDs, such as DSD-ENG-SERV, which is governed by the CEMP.

The other reason for this approach is that the ISSMP incorporates the requirements for the three in-service plans required by the ISM: Incident Response Plan, Business Continuity and Disaster Recovery Plan (BCDRP), and Continuous Monitoring Plan. These three ISM-mandated plans are required for both ICT and cyber Security Authorisations and it is easier to manage these three aspects within one DID.

Of note, the Contractor’s responsibilities under these plans will vary depending upon the role of the Contractor. If, for example, the Contractor is required to operate the Mission System on behalf of Defence, and it is a reasonably self-contained system (eg, a communications system), then the Contractor is likely to have full responsibility for all aspects of the three ISM-mandated plans. Under a more-normal approach, where the Contractor is not operating the system, a shared-responsibility model[[2]](#footnote-2) would apply, and the Contractor will need to set out how this model operates, including the interfaces and interactions with the operators of the system, to ensure that the required outcomes through these plans are achieved.

Drafters should note that both *ASDEFCON (Strategic Materiel)*, and (optionally) *ASDEFCON (Complex Materiel) Volume 2*, require the Contractor (Acquisition) to develop an ISSMP, which should be ‘pulled into’ this Contract if a combined RFT is being considered. If this is the case, the optional clause should be selected and drafters should check the timing in the CDRL for delivery of this plan.

Related Clauses/Documents:

All other clauses under this DSD.

Optional Clauses: None

# 6.2.2 System Security Services – General

Status: Core

Purpose: To identify the minimum general requirements for system security Services.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: This clause sets out a range of general system security Services, and may be the only clause required in a simpler support contract (in which case, drafters may transfer the clause to DSD-ENG-SERV, rather than have a separate DSD).

While there are some minor overlaps with other clauses in DSD-ENG-SEC, this clause provides the essential security-specific requirements (albeit at a high level) that work in conjunction with:

1. clauses 3.6 and 3.13 of the main body of the SOW; and
2. clauses 6.2.3 to 6.2.6 of DSD-ENG-SERV.

If DSD-ENG-SEC is included in a draft Contract, drafters should not make any changes to this clause.

Related Clauses/Documents:

Draft SOW clause 3.6, Co‑ordination and Co-operation

Draft SOW clause 3.13, Defence Security Compliance

Draft SOW clause 5.5, Engineering Services

DSD-ENG-SERV clause 6.2.3, Engineering Investigations

DSD-ENG-SERV clause 6.2.4, Analysis of Change Requests

DSD-ENG-SERV clause 6.2.5, Developmental Activities for Major Changes

DSD-ENG-SERV clause 6.2.6, Technical Instruction Development

Optional Clauses: None

# 6.2.3 Security Monitoring and Testing

Status: Optional

Purpose: To require the Contractor to perform system security monitoring and testing when feasible to so.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: The ISM makes it clear that system monitoring is a core system security requirement. The Continuous Monitoring Plan, within the ISSMP, is used to both comply with the ISM and for obtaining and maintaining the Security Authorisations for ICT security and cyber security. Real-time monitoring of cyber threats, security risks, and controls associated with a SSoI / ToSA and its operating environment, as outlined in a Continuous Monitoring Plan, is essential for maintaining the security posture for an SSoI / ToSA. Continuous monitoring may identify events that necessitate additional security actions and activities based on the assessed risk. Such events may include:

1. changes in security policies relating to the system;
2. detection of new or emerging cyber threats to the system or its operating environment;
3. the discovery that controls for the system are not as effective as planned;
4. a major cyber security incident involving the system; and
5. major architectural changes to the system.[[3]](#footnote-3)

While these provisions are most appropriate for ICT security and cyber security, they can also be applicable to physical security and EMSEC.

The clause is optional because the nature of the Products Being Supported and the scope of the Contractor’s support responsibilities more generally may make it infeasible for the Contractor to perform the system-specific monitoring requirements. If, for example, the only feasible activities are those under clause 6.2.3.2a, then drafters should consider including this requirement into clause 6.2.2, and the clauses under clause 6.2.3 should then be deleted and replaced with a single ‘Not used’.

Drafters should understand how the Contractor is most likely to be able to perform the different monitoring functions to understand whether further tailoring of these clauses is required, if the GFM provisions need to be modified, or if arrangements external to the Contract need to be implemented. This may already be captured in an existing Continuous Monitoring Plan, but if not, relevant considerations include the following:

1. Does the SSoI incorporate functionality to enable system monitoring? If so, how does the functionality operate, what access is available, and how is the monitoring data captured and stored? Is the data in a proprietary data format?
2. Is remote monitoring allowed, noting that this would generally be unlikely for Defence systems / equipment, particularly deployable ones?
3. Is the Contractor responsible for operating the SSoI (or part thereof)? If so, can they also perform system monitoring to the extent that the system has been designed to enable this to occur?
4. Will the Contractor have access to the SSoI as part of performing Maintenance activities and, therefore, can they also gain access to the system monitoring data as part of Maintenance? How often is this likely to occur, and if the intervening period is too long, does the Commonwealth need to provide interim drops of the monitoring data as GFI or GFD? What is the classification of the monitoring data?
5. Will the Contractor require access to operational level Maintenance data, and if so, how will this occur? Does it need to be included as GFI/GFD? Will the Contractor be provided with access to the Defence Maintenance Management System (eg, as a Government Furnished Service (GFS))? What classification is the Maintenance data, particularly once aggregated?
6. How will the Contractor gain access to the Commonwealth operators and maintainers, when required? How will the Commonwealth facilitate this access, and how often?

If the draft Contract (Support) is linked to an accompanying Contract (Acquisition) as part of a single Request For Tender (RFT), then there is unlikely to be an existing Continuous Monitoring Plan and many of the above questions may be difficult to answer. Under these circumstances, it may also be difficult to know how to definitely tailor this clause because the system solution is either unknown or not understood sufficiently. Drafters should consider, therefore, whether to incorporate reference to this clause (or perhaps the whole DSD) in clause 2.6 of the main body of the SOW as part of the changes to the Phase In provisions introduced through the ASDEFCON Linkages Module (ALM).

Clause 6.2.3.3 is an optional clause for security testing to be included within the scope as an adjunct to system monitoring. Security testing can include, for example, penetration testing and specific test activities for different types of Products, such as for cryptographic devices, Software applications, and gateways.

Penetration testing involves exercising real-world scenarios in an attempt to achieve a specific goal, such as compromising critical systems or data. This type of testing can be expensive and involve specialist skills, and may not be required given the security posture of the SSoI / ToSA. Generally, the Continuous Monitoring Plan would identify whether such testing is required. If the need to include this requirement is unclear to the drafter, specialist security advice should be sought, such as from the individual Service subject matter experts, JCG security assessors, or the CASG Cyber Security Advisory & Assurance Directorate (CAAD).

Clause 6.2.3.4 identifies that if a security issue is suspected, the Contractor is required to undertake a security investigation in accordance with clause 6.2.9 and take subsequent actions, depending upon the significance and urgency of the issues identified in the Approved security investigation report. These actions could include:

1. changing the ISSMP (eg, to change the actions and activities in relation to business continuity);
2. changing the Security Standard Operating Procedures (SSOPs) (eg, to change how operators and maintainers interact with the system procedurally); and/or
3. developing one or more configuration changes to the SSoIs (or parts thereof).

Related Clauses/Documents:

Clause 6.2.1, Security Management Planning

Clause 6.2.5, System Security Documentation

Clause 6.2.8, Security Requirements for Configuration Changes

Clause 6.2.9, Security Investigations

DSD-ENG-SERV clause 6.2.6, Technical Instruction Development

Draft SOW clause 3.6, Co-ordination and Co-operation, for co‑ordinating access to platforms, systems and ADF operators and maintainers.

Draft Contract Attachment E, GFM and GFS

Optional Clauses: None

# 6.2.4 Security Tools

Status: Optional

Purpose: To set out the minimum requirements for managing and maintaining the Security-related Software licences for the applicable Products covered by the DSD.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: The clause only requires minor tailoring to cross-reference to where the general Software licence clause is located.

The clause is optional because there may be no security-related Software licences that require management, depending upon the nature of the Products Being Supported and the scope of the Contractor’s support responsibilities more generally. When the clause is not required, the clauses under clause 6.2.4 should be deleted and replaced with a single ‘Not used’.

The purpose of this clause is to ensure that the management of these security-specific Software licences are not accidentally overlooked, particularly given the evolving nature of the requirements for ICT/cyber security.

Drafters should consider if some or all of these Software licences should be provided by the Commonwealth, to ensure that there are no compatibility issues with Software being used by the Commonwealth on the DPN/DSN, while also potentially realising cost savings. If this approach is adopted, drafters should modify the clauses accordingly, and include the proposed Software in the GFM list at Attachment E.

Related Clauses/Documents:

DSD-MNT-SA clause 6.2.7, Software Licence Management

DSD-ENG-SW

Draft Contract Attachment E, GFM and GFS

Optional Clauses: None

# 6.2.5 System Security Documentation

Status: Optional

Purpose: To require the development and preparation of system security documentation, including updates when required.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: In general, system security documentation for a particular Security Authorisation will have been developed under the acquisition contract, but where this is not the case (eg, due to the evolving requirements for cyber Security Authorisations), the clause can provide for the initial development of these documents, noting that the same DIDs are used in both the acquisition and support templates.

The clause is optional because it may not be needed due to the nature of the Products Being Supported and the scope of the Contractor’s support responsibilities more generally, particularly if the Contractor does not have system-level responsibilities. If the clause is not required, the clauses under clause 6.2.5 should be deleted and replaced with a single ‘Not used’.

As drafted, the clause only includes the required security documentation for EMSEC, ICT security, and cyber security. If the drafter wishes to also include physical security, then the clause will need to be amended accordingly. Attention is drawn to the physical security DID in ASDEFCON (Strategic Materiel) (ie, DID-ENG-SOL-PSECDD – Physical Security Design Document).

The clause is deliberately separated from the ‘Support to Security Authorisations’ at clause 6.2.7 because there can be various activities that result in the security documentation needing to be developed or updated, including as an outcome of security monitoring (eg, which could result in changes to the ISSMP and/or SSOPs) and Major Changes to the SSoI / ToSA. The Security Authorisation documentation may also have been provided on the basis that a subsequent review or periodic review of the security posture and underpinning security basis for an SSoI / ToSA will be undertaken.

The clause includes an optional requirement for when the draft Contract (Support) is linked to an accompanying Contract (Acquisition) as part of a single RFT, thereby enabling the security-related data items developed under the acquisition contract to be pulled into the Contract when required. Under these circumstances, drafters should include the optional clause, and adjust the CDRL timings accordingly. If the two Contracts will operate in parallel for an extended period, as greater quantities of systems and equipment are Accepted under the Contract (Acquisition), drafters should also consider how the two Contracts will need to inter-relate in relation to the ongoing management of the security documentation (eg, does the Contractor (Acquisition) or the Contractor (Support) have carriage of the master set?).

The clause includes a second optional requirement for when:

1. the Contractor has responsibility under DSD-ENG-CM for maintaining the Functional Baselines (FBLs) for the Mission System and/or the Support System; and
2. either or both of these FBLs include a Cyber Security Assurance Basis (ie, the suite of requirements against which the Materiel System is assessed in relation to cyber security).

If neither of these circumstances apply, the clause should be deleted.

Note that the clause includes reference to Objective Evidence, which is likely to include detailed information and justification that underpins the identified data items and the associated Security Authorisations, similar to the types of Objective Evidence that underpin airworthiness, land-worthiness and seaworthiness. Clause 6.2.7 includes additional requirements in relation to the provision of this Objective Evidence, which, in general, will be essential to enable the Security Authorisations to be initially provided and subsequently updated and/or re-provided.

In those circumstances where the Contractor has system-level responsibilities, but is not the OEM, the Contractor will need to establish relationships with the OEM(s) through its TSN / DSN to enable the Contractor to meet its obligations under this (and other) clauses. Additionally, the Commonwealth may need to consider providing some or all of this data as GFM, noting that some of it is likely to be classified and/or subject to export controls from the country of origin.

Given the significance of this Objective Evidence to the Contractor’s obligations and the ability for the Commonwealth system managers to maintain the required Security Authorisations, clause 6.2.5.5 requires the Contractor to identify all Technical Data used to meet the security obligations of the Contract in the Technical Data List (TDL) required under clause 9.2 of the SOW.

If another contractor has the system-level security responsibilities, drafters should consider what data may need to be provided under this Contract to enable the other contractor meeting its security responsibilities (clause 3.6 of the main body of the SOW refers). No optional clauses are provided, but attention is drawn to DID-ENG-SOL-CSAI – Cyber Security Assessment Information, which may be suitable for this purpose.

Related Clauses/Documents:

Clause 6.2.3.4 (part of Security Monitoring and Testing)

Clause 6.2.7, Support to Security Authorisations

Clause 6.2.8, Security Requirements for Configuration Changes

DSD-ENG-CM clause 6.2.2, Baseline Management

Draft SOW clause 3.6, Co-ordination and Co-operation, for when information is passed to another party to perform system-level security requirements

Draft SOW clause 9.2, Technical Data

Draft Contract Attachment E, GFM and GFS

DID-SSM-TDL

All of the security-related DIDs, most of which are sourced from *ASDEFCON (Strategic Materiel)*

Optional Clauses: None

# 6.2.6 Cyber Supply Chain Security

Status: Optional

Purpose: To identify the requirements for management of the Cyber Supply Chain.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: Contractors have a general responsibility to manage their supply chain, but clause 6.2.6 extends that responsibility for the purposes of ICT security and cyber security to ensure that the SSoI-related goods and services (eg, cloud services) that will ultimately be delivered to Defence do not have security problems (eg, through the inclusion of Malware, ‘Trojan horses’, or other security vulnerabilities). Defence policy and practice requires Cyber Supply Chain security to be addressed as part of the ongoing management of an SSoI. For further information on this subject, see:

1. the Governing Security Documents, particularly the ISM and DSPF;
2. the Defence Cyber Supply Chain Risk Management portal at:

[Defence Cyber Supply Chain Risk Management - Home (sharepoint.com)](https://defencegovau.sharepoint.com/sites/DefenceCyberSupplyChainRiskManagement)

1. CAAD guidance at:

[8. Supply Chain Risk Management - CAAD Knowledge Base - DevOps Confluence - DPE Environment (mil.au)](https://devops-confluence.dpe.protected.mil.au/display/CAADKB/8.+Supply+Chain+Risk+Management)

1. ACSC guidance at:

[Cyber supply chains | Cyber.gov.au](https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains)

1. other guidance documents, such as the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161r1, ‘Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations’, May 2022.

The Defence Cyber Supply Chain risk-management approach focuses on Defence internal activities, whereby JCG provides “rapid Open Source Intelligence (OSINT) analysis of possible threats and vulnerabilities to the security of a supply chain, introduced by its vendors/companies/suppliers”. The ASDEFCON drafting, on the other hand, places significant responsibility for this activity on the Contractor, noting that the Contractor has responsibility under the Contract for supplying goods and services that are fit for purpose and do not contain Malware (eg, see clauses 5.16.2, 3.2 and 3.3 of the COC).

Clause 6.2.6 is focussed around the Cyber Supply Chain Risk Plan (CSCRP) and the associated Cyber Supply Chain threats, risk assessments, risk treatments and controls. In concept, it is very similar to the SRMP, which addresses design-related security risks in relation to end-items of equipment, such as the Mission System. The CSCRP, on the other hand, addresses Cyber Supply Chain risks, which can be thought of as design-related security risks in relation to the Support System.

The CSCRP is not a management plan, so there is no clause that states, “The Contractor shall do [XYZ] in accordance with the Approved CSCRP”. The Approved risk-management framework that underpins the CSCRP will be set out in the applicable governing plan, typically the Approved ISSMP (see clause 6.2.4 of DID-SSM-ISSMP). Commonwealth responsibilities with respect to the CSCRP are set out in clauses 6.2.6.4 and 6.2.6.5, which involves collaborating with the Contractor during the development and update of the CSCRP, with a particular view to ensure:

1. that risk assessments consider Defence’s unique perspective, including operational and support contexts, any classified threats that may be known only to the Commonwealth, and any prior assessments of, or determinations in relation to, similar risks made by the applicable security authority for similar SSoIs / ToSAs with similar operational / support contexts; and
2. the way forward for a particular item of DESE or Software from a particular supplier is agreed if the associated Cyber Supply Chain risk assessment results in a post-mitigated assessment of Medium or higher.

This discussion highlights the complexity associated with this requirement, particularly for any reasonably complex SSoI, such as a platform, which may contain hundreds of thousands of items of DESE and Software at multiple levels of the supply chain hierarchy. This complexity can be partially managed and reduced by:

1. the use of an appropriate supply chain strategy, which targets the use of trusted suppliers (although this could work against Australian Industry Capability (AIC) outcomes, particularly the use of Small-to-Medium Enterprises, and therefore, these considerations would need to be balanced);
2. the use of an appropriate security risk-assessment strategy, which targets the higher-risk elements first;
3. requiring Approved Subcontractors to also undertake similar Cyber Supply Chain risk-assessment activities (as required by clause 6.2.6.4b);
4. having an appropriate understanding of the design of the SSoI / ToSA and the potential for security threats to have negative consequences for the Security Outcomes; and
5. ensuring that any security-in-design aspects underpinning the design of the SSoI / ToSA are maintained and updated, as required, over the life-of-type.

Note that the Commonwealth’s involvement in these Cyber Supply Chain activities is not to dictate the use of particular suppliers or particular items of DESE or Software[[4]](#footnote-4), but to collaborate to mitigate particular Cyber Supply Chain risks, which may involve the Commonwealth having to fund a configuration change to address the risks. Commonwealth involvement should always occur on the basis that, unless exceptional circumstances apply, the Contractor remains accountable for contractual outcomes.

Similar to the requirements for security documentation, where the Contractor has system-level responsibilities but is not the OEM, the Contractor will need to establish relationships with the OEM(s) through its TSN / DSN in order to meet its obligations under this clause, particularly to better understand the supply chain details underpinning the SSoI / ToSA. Additionally, the Commonwealth may need to consider providing some or all of these supply chain details as GFM, noting that this may be challenging if the original acquisition contract(s) did not include such obligations.

Related Clauses/Documents:

DID-ENG-SOL-CSCRP (from *ASDEFCON (Strategic Materiel*)

DID-PM-AIC-SCMP, DID-PM-AIC-MPS and DID-PM-AIC-MPBC (from *ASDEFCON (Strategic Materiel*))

Optional Clauses: None

# 6.2.7 Support to Security Authorisations

Status: Optional

Purpose: To require the Contractor to support the Commonwealth’s activities in relation to the various Security Authorisations.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: As stated in the overall guidance at the start of this DSD, there are up to four separate Security Authorisations required for the four security categories of physical security, EMSEC, ICT security, and cyber security. Depending upon the security levels associated with each of those security categories, differing security authorities will be involved. For example, in relation to physical security Certification and Accreditation, detailed information on this subject can be found at: [Pages - Physical Security Accreditation, Recertification and Reaccreditation](http://drnet/eig/Defence-Security/Certification-Accreditation-Physical-Security-Zones/Pages/Security-Accreditation.aspx).

Additionally, there may be multiple SSoIs / ToSAs being supported under the Contract, which each require their own set of Security Authorisations. For example, a common communications system fitted to multiple ship classes may require Security Authorisations for ICT security and cyber security for each ship class (or at least the data to support these Security Authorisations for each ship class).

The responsibility for seeking a Security Authorisation from the relevant security authority resides with the contract-management team (ie, not the Contractor), who undertakes this activity with the support of security subject matter experts, such as people authorised under the Information Security Registered Assessors Program (IRAP) for ICT security (eg, see: [Pages – IRAP Assessor Guidance](http://drnet/JCG/CYBERCOMD/CFG/462SQN/462SQN%20Services/ICT%20Security%20Assessments/Pages/IRAP.aspx)). The Contractor’s responsibility is to provide the requisite Objective Evidence and to support the contract-management team in their endeavours to obtain the required Security Authorisations.

While it is likely that Security Authorisations would have been obtained during the acquisition contract, this may not have occurred (or did not align with current requirements) and this clause can be used to obtain the Contractor’s assistance for obtaining the required Security Authorisations. More typically, however, Contractor support for Security Authorisations would occur either due to a requirement for a periodic reassessment of an SSoI / ToSA, or due to a configuration change to an SSoI / ToSA (ie, either a Major Change or a major Deviation).

Clause 6.2.7.1 sets out the reasons why Security Authorisations may need to be reassessed or updated, which include periodic reassessments (eg, as set out in the Security Authorisation documentation) and as an outcome of configuration changes (see clause 6.2.8). In relation to ICT security, for example, Policy 11 of the PSPF (v2018.7) states, at paragraph 15:

*“15. Authorisation to operate is generally ongoing, however during the lifecycle of an ICT system, it may require a reassessment to continue operation or eventually be decommissioned (i.e. disposal at the end of its life). Examples of events that may trigger additional risk management activities for an ICT system include:*

1. *changes in security policies relating to the system*
2. *detection of new or emerging cyber threats to the system or its operating environment*
3. *the discovery that security controls for the system are not as effective as planned*
4. *a major cyber security incident involving the system*
5. *major architectural changes to the system.”*

Additionally, DSPF Control 23.1 ‘Cyber Security Assessment and Authorisation’ (10May24 version) states that the *“System Owner must ensure [...] systems are Re‑Assessed and Re‑Authorised throughout the system’s lifecycle in line with re‑assessment triggers and timeframes set by the Authorising Delegate”*. The quote above from the PSPF identifies the trigger categories, but drafters should ensure that the System Owner or authorising delegate for each SSoI / ToSA is consulted to ensure that the specific triggers relevant to that SSoI / ToSA are identified and, if applicable, incorporated into the DSD. These specific triggers would take into consideration (for example) the mission criticality, Business Impact Level (BIL), Defence Cyberworthiness System (DCwS) maturity assessment, relationship(s) with external systems, etc.

The Defence Cyber Security Assessment & Authorisation (CSAA) Framework, v4.2, 22 April 2024, also states at paragraph 2.9: *“If there is uncertainty regarding whether* [...] *Re‑Assessment and Re‑Authorisation is required, the CSAA Directorate should be engaged to provide confirmation”*. While this approach does not necessarily help with ensuring that the DSD properly defines the exact scope of work, drafters and contract managers should expect that the need for re‑assessment and re‑authorisation would be determined using the security risk-assessment methodologies underpinning the Governing Security Documents and the clauses in the DSD (ie, it would be determined on a case-by-case basis, taking into consideration the relevant security-related issues at the time).

In relation to terminology, the clauses use the terms ‘Major Change’ and ‘major Deviation’. The term ‘Major Change’ is defined in the Glossary, but the term ‘major Deviation’ is not; hence, for the purposes of clauses 6.2.7 and 6.2.8, a major Deviation is defined through clause 6.2.7.1b as “a Deviation that contains DESE or Software that could introduce security vulnerabilities into an SSoI / ToSA”. An example of a major Deviation is a trial modification, such as for a system or platform, where the system / platform is temporarily modified for the purposes of a trial. Clause 6.2.8 addresses the specific security considerations associated with these types of configuration changes.

The clause is optional because it may not be needed due to the nature of the Products Being Supported and the scope of the Contractor’s support responsibilities more generally, particularly if the Contractor does not have system-level responsibilities. When the clause is not required, the clauses under clause 6.2.7 should be deleted and replaced with a single ‘Not used’.

If the clause is required, the clause does not require tailoring for inclusion in the draft DSD.

Related Clauses/Documents:

Clause 6.2.5, System Security Documentation

Clause 6.2.8, Security Requirements for Configuration Changes

Optional Clauses: None

# 6.2.8 Security Requirements for Configuration Changes

Status: Optional

Purpose: To identify the security-specific requirements relating to configuration changes.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: Clause 6.2.8.1 highlights that there are a range of other clauses within ASDEFCON (Support) that address the management and implementation of configuration changes. DSD-ENG-SERV, for example, is the head DSD for the development of configuration changes, and drafters should ensure that they are familiar with all of the other template provisions before making changes to clause 6.2.8.

Drafters should also familiarise themselves with the definitions of ‘Major Change’ and ‘Minor Change’ in the Glossary. A ‘Major Change includes a range of generic aspects that would pick up security (eg, technical risk assessments, changes to the Functional Baseline, and both Adaptive Maintenance and Perfective Maintenance for Software). The definition explicitly includes: “[...] an engineering change that [...] affects requirements (other than the Functional Baseline) and/or the design, and the Commonwealth considers the change has a significant impact upon [...] the operational or performance characteristics of the Materiel System, including in relation to safety, security, survivability, reliability, maintainability, availability and supportability [...]”.

While qualifying terms like ‘significant’ can be open to interpretation, it would be expected that these terms would be underpinned by the applicable risk assessments, which for security, would include the normal threat and risk assessment activities. As such, a significant impact on security would be one that was shown to be significant through these standard security risk-assessment processes.

In relation to Major Changes, these could have been developed by the Contractor (eg, if they have Design Authority responsibilities) or arise due to a change to a component of the SSoI / ToSA issued by the OEM (eg, a Software Update in the form of a patch). Further information on patch management can be found at: [Pages - Cyber Security Compliance](http://drnet/JCG/CYBERCOMD/DCIAB/Pages/Cyber-Security-Compliance.aspx). Of note, DSD-ENG-SEC does not include any specific requirements in relation to patch management. Instead, ASDEFCON (Support) treats Software patches within the scope of Software Updates, which are managed in accordance with the applicable provisions in DSD-ENG-SW and the configuration change provisions in DSD-ENG-CM and DSD-ENG-SERV.

Applicable clauses under DSD-ENG-SERV and DSD-ENG-SW determine the type of Service and the associated payment requirements associated with the work under this clause 6.2.8. Both DSD-ENG-SERV and DSD-ENG-SW include specific requirements for configuration changes that need to be addressed within the scope of Recurring Services. For example, clause 6.2.5.7i in DSD-ENG-SERV requires a Major Change to be undertaken within the Recurring Services Fee if the Major Change “[...] is required to address a security vulnerability identified in the Products Being Supported”. If the conditions under clause 6.2.5.7i did not apply, the Major Change would need to be undertaken as an S&Q Service, or through the Contractor Standing Capability (CSC) if this requirement was included in the draft Contract.

This clause also inter-relates with other clauses under this DSD (eg, in relation to security documentation and Security Authorisations) to minimise duplication of requirements. As such, drafters should ensure that all related clauses are either included or omitted as a set in this DSD.

Similar to other clauses in this DSD, this clause is optional because it may not be needed due to the nature of the Products Being Supported and the scope of the Contractor’s support responsibilities more generally. However, unlike some of the other clauses, this clause may still be required even if the Contractor does not have system-level responsibilities to ensure that the security requirements associated with configuration changes are appropriately addressed. Alternatively, drafters could consider transferring some of the more detailed requirements into the applicable clauses in DSD-ENG-SERV and/or DSD-ENG-SW.

When the clause is not required, the clauses under clause 6.2.8 should be deleted and replaced with a single ‘Not used’.

If the clause is required, the clause does not require tailoring.

Related Clauses/Documents:

Clause 6.2.5, System Security Documentation

Clause 6.2.7, Support to Security Authorisations

DSD-ENG-SERV, DSD-ENG-SW and DSD-ENG-CM

SOW clause 11.4, Non-Conforming Services

Optional Clauses: None

# 6.2.9 Security Investigations

Status: Optional

Purpose: To provide the framework within which security investigations are to be conducted.

Policy: Refer to the definition of Governing Security Documents in the Glossary

Guidance: Clause 6.2.9 is reasonably self-explanatory and identifies the triggers against which security investigations should be undertaken, including as an outcome of Engineering Investigations conducted in accordance with clause 6.2.3 of DSD-ENG-SERV and Maintenance Investigations conducted in accordance with clause 6.2.7 of DSD-MNT-MGT. If a security investigation is required, clause 6.2.9.2 requires the Contractor to “undertake the security investigations and reporting required [...] as if they were engineering investigations in accordance with the process and pricing and payment arrangements set out in the Engineering Investigations clause in DSD-ENG-SERV”.

Clause 6.2.3 of DSD-ENG-SERV contain specific criteria and requirements that determine the type of Service and the associated payment requirements associated with the work under this clause 6.2.9. Clause 6.2.3.1 of DSD-ENG-SERV requires certain engineering investigations to be undertaken as Recurring Services, including engineering investigations required to “address security vulnerabilities identified in the Products Being Supported”. If the conditions under clause 6.2.3.1 of DSD-ENG-SERV did not apply, the engineering investigation would need to be undertaken as an S&Q Service, or through the CSC if a CSC was included in the draft Contract.

This clause is optional because it may not be needed due to the nature of the Products Being Supported and the scope of the Contractor’s support responsibilities more generally. However, unlike some of the other clauses, this clause may still be required even if the Contractor does not have system-level responsibilities to ensure that the triggers for security-related engineering investigations are addressed. Alternatively, drafters could consider transferring some of the more detailed requirements into clause 6.2.3 of DSD-ENG-SERV.

When the clause is not required, the clauses under clause 6.2.9 should be deleted and replaced with a single ‘Not used’.

If the clause is required, the clause does not require tailoring.

Related Clauses/Documents:

DSD-ENG-SERV Clause 6.2.3, Engineering Investigations

DSD-MNT-MGT Clause 6.2.7, Maintenance Investigations

Optional Clauses: None

# 6.2.10 Security Advisory Services

Status: Optional

Purpose: To require the Contractor to provide advisory Services in relation to security, particularly when Commonwealth expertise in the various security domains is limited.

Policy: Nil

Guidance: Given the significant changes to the security environment that have arisen over the last five years or so, the requirement for security expertise has risen commensurately. This clause provides procurement teams with security advisory Services, particularly for those situation when expertise is limited or unavailable.

The default position in the template is that, except where otherwise required through other Services, these clauses are performed as S&Q Services. This position has been adopted due to the difficulties with determining the level of effort involved with this requirement. Nevertheless, the effort associated with implementing S&Q Services for these Services may be excessive for small-scale needs. If drafters can define a level of effort (eg, one person-day per month in the context of significantly broader security Services), then drafters should consider amending clause 6.2.10.2 accordingly and bringing this work into the scope of Recurring Services.

The clause is optional and, if not required, the clauses under clause 6.2.10 should be deleted and replaced with a single ‘Not used’.

If the clause is required and other than the issue in relation to S&Q Services versus Recurring Services discussed above, the clause does not require tailoring.

Related Clauses/ Documents:

Nil

Optional Clauses: None

# 6.2.11 Security Working Groups (Optional)

Status: Optional

Purpose: To require the Contractor to participate in Security Working Groups (SWGs) when appropriate to the nature of the work.

Policy: Nil

Guidance: In general, SWG meetings are appropriate when the work involves considerable interaction with the Commonwealth and Associated Parties, such as in relation to new threats and vulnerabilities, development of updates to security documentation, Major Changes, requirements for new / updated Security Authorisations, and security-related requirements for co‑ordination and co‑operation under clause 3.6 of the SOW. If these circumstances exist and the nature and scope of the requirement warrant it, drafters should consider incorporating this clause into the DSD.

Drafters should note that the clause provides the ability for the Commonwealth to hold its own SWGs and require the Contractor to participate. This approach provides the Commonwealth with certainty that SWG meetings will be conducted when the Commonwealth considers it appropriate, but the Commonwealth contract-management team should also expect to see SWG requirements addressed through the ISSMP as well as in the plans developed for the more-significant Major Changes where security is a key consideration.

The clause includes also includes two optional requirements for when the draft Contract (Support) is linked to an accompanying Contract (Acquisition) as part of a single RFT, thereby requiring:

1. for the first optional clause, the Contractor to participate in the SWGs held under the Contract (Acquisition): and
2. for the second optional clause, for the Contractor to ensure that the Contractor (Acquisition) and Approved Subcontractors (Acquisition) participate in the SWG meetings held under the Contract.

Drafters should include either or both of these clauses, depending upon the envisaged circumstances across the two contracts.

Drafters should also note that the clause leverages off the Ad Hoc Meetings clause 3.4.6 in the main body of the SOW, which addresses requirements for chairing meetings, location, and requirements for Agendas and Minutes.

When the clause is not required, the clauses under clause 6.2.11 should be deleted and replaced with a single ‘Not used’.

If the clause is required and other than in relation to the two optional requirements, the clause does not require tailoring.

Related Clauses/ Documents:

Draft SOW clause 3.4.6, Ad Hoc Meetings

Draft SOW clause 3.6, Co‑ordination and Co-operation

Optional Clauses: None

Detailed Service Description

1. DSD NUMBER: DSD-ENG-SEC-V5.2
2. TITLE: SYSTEM SECURITY SERVICES
3. DESCRIPTION AND INTENDED USE

This DSD identifies the system security Services required to be provided by the Contractor to the Products specified at clause 6.1.1.1 of this DSD.

The requirements of this DSD, including as applicable to related DSDs, require a structured, well-planned and well-executed system security program to achieve the following objectives:

ensure that each Security System-of-Interest (SSoI) continues to achieve the Security Outcomes;

ensure that configuration changes to the SSoIs (including components and processes) satisfy security requirements and enable the Commonwealth’s security obligations and compliance requirements continue to be met as they pertain to:

protecting information, data and technology; and

controlling access to, and transfer of, information, data and technology;

gain from the relevant Security Authorities endorsement of the security-related design aspects of any configuration changes to an SSoI (or part thereof) throughout the design processes for those changes; and

support the Commonwealth in maintaining the required Security Authorisations for the SSoIs from the relevant authorities.

1. INTER-RELATIONSHIPS

This DSD forms part of the SOW.

This DSD must be applied in conjunction with the general security Services required by clause 11.10 of the COC and clause 3.13 of the SOW and the Engineering Services defined in the Engineering Support requirements of the SOW and related DSDs.

1. APPLICABLE DOCUMENTS

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

Note to drafters: Edit the list of documents in the table below to suit the requirements of this DSD (ie, include the relevant references that are applicable to system security Services).

|  |  |
| --- | --- |
| 1. Governing Security Documents | 1. (see the Glossary for the definition of this term) |

1. SERVICE DESCRIPTION
   1. Introduction
      1. Scope

Note to drafters: Amend the following clause to align with the Products listed in Annex A to the SOW. Drafters are advised that certain key terms in the Glossary (eg, Security Authorisation and SSoI) need to be amended to ensure that the scope of the system security program is clear.

The Contractor shall provide system security Services, as described in this DSD, for:

the following types of Products listed in Annex A to the SOW (to the extent that they are, or form part of, a SSoI or an associated Target of Security Assessment (ToSA)):

Mission System(s);

Repairable Items (RIs);

Non‑Repairable Items (Non-RIs);

Software; and

Technical Data,

which:

could be susceptible to security vulnerabilities that may affect the Commonwealth’s security obligations and compliance requirements (as would be determined by a competent contractor acting reasonably in making such a determination); and/or

are the subject of, or included within the scope of, a Security Authorisation, including in relation to physical security, Emanation Security (EMSEC), Information and Communications Technology (ICT) security, cyber security, and personnel security (but, for personnel security, only in relation to Contractor Personnel operating, maintaining or upgrading a SSoI / ToSA); and

other Products, which may or may not be listed in Annex A to the SOW, but which are required by the Contractor to undertake the system security Services.

The parties acknowledge and agree that the scope of the system security program:

includes:

|  |
| --- |
| Option: Include this option if physical security requirements apply to any of the SSoIs.  physical security; |

|  |
| --- |
| Option: Include this option if EMSEC requirements apply to any of the SSoIs.  Emanation Security (EMSEC); |

|  |
| --- |
| Option: Include this option if ICT Security Authorisation requirements apply to any of the SSoIs.  Note: The DSPF and ISM are continually evolving. The language below in relation to ICT security reflects the endorsed version of these policy documents, where the terms ‘ATO‑C’ and ‘ATO’ have replaced the long-standing terms, ‘PICTA’ and ‘ICTA’, respectively.  Information and Communications Technology (ICT) security (which leads to an Authorisation to Operate with Conditions (ATO‑C) or an Authorisation to Operate (ATO) by the relevant Security Authorisation authority); and |

cyber security (which leads to a cyber-maturity assessment against the Defence Cyberworthiness System (DCwS) and an assessment as part of the regulatory / assurance framework for the Contract),

as each of these security aspects are applied to the SSoIs / ToSAs (or parts thereof, such as Digitally Enabled Systems and Equipment (DESE) and Software); but

does not include the programmatic and contract-management aspects of security, which are addressed through clause 3.13 of the SOW.

* + 1. System Security Standards

The parties acknowledge and agree that:

the Governing Security Documents identified in the definition of this term in the Glossary are applicable to the provision of system security Services;

the versions of the Governing Security Documents are likely to change over the Term and, except where otherwise determined by the Commonwealth Representative, the required Security Authorisations for the SSoIs (or parts thereof) will need to be performed against the versions of the Governing Security Documents that are current at the time that the Security Authorisations for these SSoIs (or parts thereof) are required;

the Contractor shall undertake its activities and responsibilities, including in relation to supporting the achievement of the required Security Authorisations, against the version of the Governing Security Documents that are current at the time that the Contractor undertakes those activities and responsibilities;

where the Contractor assesses that a change to a Governing Security Document after the Effective Date results in a material change to the scope of work required under the Contract (including under an S&Q Order), the Contractor shall:

notify the Commonwealth within 10 Working Days of identifying the change; and

provide such supporting evidence as is reasonably required by the Commonwealth Representative to demonstrate that the change materially increases the level of effort required of the Contractor (or otherwise impacts on the Contractor performing its obligations under the Contract); and

where the Commonwealth Representative is satisfied on the basis of the evidence provided under 6.1.2.1d(ii) that the change to the Governing Security Documents materially increases the level of effort required of the Contractor (or otherwise impacts on the Contractor performing its obligations under the Contract), the parties shall meet and negotiate in good faith to agree a CCP in accordance with clause 11.1 of the COC to address the impact of the change.

* 1. Services
     1. Security Management Planning

The Contractor shall develop, deliver and update an In-Service Security Management Plan (ISSMP) in accordance with CDRL Line Number ENG-800.

|  |
| --- |
| Option: Include the following clause when the Contract will be tendered in conjunction with a linked Contract (Acquisition).  The Contractor shall use the ISSMP developed under the Contract (Acquisition) as the basis for the ISSMP required under clause 6.2.1.1. |

The Contractor shall make available to the Commonwealth, within 10 Working Days of a request, all associated plans, processes, procedures, logs, instructions and data supporting the Approved ISSMP.

The Contractor shall provide system security Services in accordance with the Approved ISSMP.

The Contractor shall ensure that all system security Services provided by Subcontractors are provided in accordance with the Approved ISSMP.

The Contractor shall have the systems, people and resources in place to ensure that its system security activities defined in the Approved ISSMP meet the requirements of the Governing Security Documents.

The Contractor acknowledges that the ISSMP incorporates the requirements for incident response planning, business continuity and disaster recovery planning, and continuous monitoring planning, all of which are required to achieve and be able to maintain the relevant Security Authorisations under the ISM.

The Contractor shall provide all facilities and assistance reasonably required by the Commonwealth to access the Contractor’s Incident Register and other security records for the Term.

* + 1. System Security Services – General

The Contractor shall conduct the following general system security Services as they apply to the Products specified at clause 6.1.1.1:

undertaking ongoing security management to consolidate, investigate, resolve and report on any security-related issues, which have been identified by stakeholders of an SSoI / ToSA (eg, system / equipment operators and maintainers);

providing advice to the Commonwealth on security-related matters as they apply to the SSoIs, ToSAs, DESE and Software;

ensuring that the Commonwealth Personnel and Contractor Personnel, who are operating and conducting Maintenance of the SSoIs / ToSAs and associated Support System Products, are kept apprised of emerging security-related issues and vulnerabilities so that they can take appropriate action when such issues or vulnerabilities arise;

monitoring the Cyber Supply Chains for the Contract and undertaking risk assessments of any proposed new suppliers to ensure that security vulnerabilities are not being introduced through the Cyber Supply Chains; and

conducting any other security-related activities to ensure that the objectives set out in clause 3.2 and the Contract Performance Measures are achieved, including any other activities set out in the Approved ISSMP.

* + 1. Security Monitoring and Testing

The Contractor acknowledges that the objectives of undertaking the security monitoring and testing requirements of this clause 6.2.3 are to:

identify a need for action based on observable behaviour and conditions; and

ensure that, to the maximum practicable extent, any security problem or Failure is resolved prior to any impact on operations and the SSoI users.

The Contractor shall:

continually monitor the Governing Security Documents, Defence security advisory notices (eg, in relation to particular threats or vulnerabilities, such as may be distributed by Defence or found on the DPN), other online sources of information for threats or vulnerabilities (eg, Australian Cyber Security Centre (ACSC) Cyber Threat Intelligence Sharing (CTIS) platform), and Original Equipment Manufacturer (OEM) equipment bulletins to identify any changes (eg, Software Updates to implement a patch) or vulnerabilities that could impact upon the security of the SSoIs;

seek feedback from system operators and maintainers (as facilitated by the Commonwealth Representative for Commonwealth operators and maintainers) to enable the continual monitoring of the performance of the SSoIs and associated Support System Products to identify any abnormal behaviour or other indications or symptoms that indicate that the SSoIs or Support System Products may have been compromised from a security perspective; and

notify the Commonwealth Representative, in writing, within the following timeframes for any changes identified pursuant to either subclauses a or b above:

within one Working Day for any change, which is assessed as a High (or higher) risk to the security or operation of the SSoIs or Support System Products (as determined in accordance with the Approved ISSMP);

Note: If the risk matrices from the Defence Security Principles Framework (DSPF) are used, the references to ‘Medium’ in the following clauses are to be interpreted as ‘Significant’.

within five Working Days for any change, which is assessed as a Medium (but no higher) risk to the security or operation of the SSoIs or Support System Products; and

as part of the standard Contract reporting for any other change, unless otherwise notified by the Commonwealth Representative that such reporting is not required.

|  |
| --- |
| Option: Include this option if one or more Mission Systems included at SOW Annex A are also SSoIs. Note that this requirement may require the Contractor to be provided with access to the Mission System(s) and Commonwealth Personnel, and additional clauses may need to be drafted to address how this would occur.  In addition to the security monitoring requirements of clause 6.2.3.1, the Contractor shall also conduct security testing activities at irregular periods, as defined in the Approved ISSMP, to test each different type of Mission System (or part thereof) and associated Mission System operators and maintainers to identify and assess system vulnerabilities, including system and personnel responses to new threats and the efficacy of mechanisms and practices for incident response, disaster recovery, and business continuity. |

If the Contractor’s security monitoring or security testing activities identify the potential presence of a security issue with the SSoIs or Support System Products (eg, abnormalities and potential compromises to information and system integrity), the Contractor shall:

undertake a security investigation in accordance with clause 6.2.9;

if the Approved security investigation report identifies that one or more changes are required to the ISSMP and/or the Security Standard Operating Procedures (SSOPs) to resolve the security issue, including to implement a workaround while a longer-term solution is identified and implemented, the Contractor shall:

if the security is assessed as a High (or higher) risk to the security or operation of the SSoIs or Support System Products (as determined in accordance with the Approved ISSMP), develop the required updates as a Technical Instruction in accordance with clause 6.2.6 of DSD-ENG-SERV; and

develop and deliver updates to the ISSMP and/or the SSOPs in accordance with clause 6.2.5 and within 40 Working Days after the security investigation report has been Approved; and

if the Approved security investigation report identifies that one or more configuration changes are required to the SSoIs (or parts thereof), the Contractor shall undertake the required work to implement the required configuration changes in accordance with clause 6.2.8.

* + 1. Security Tools

Note to drafters: Amend the following clause, depending upon whether the Software Licence Management clause is included in DSD-MNT-SA (clause 6.2.7) or is relocated to DSD-ENG-SW.

The Contractor shall manage and maintain all security-related Software licences for the Products specified at clause 6.1.1.1 in accordance with Software Licence Management clause of […INSERT 'DSD-MNT-SA' or 'DSD-ENG-SW'…], including, if applicable, Software licences required for:

system event monitoring;

security incident monitoring and vulnerability scanning;

endpoint protection; and

malware/virus checking.

The Contractor shall incorporate any required updates to the security tools (including Software) for the Products specified at clause 6.1.1.1 into its assessments of, planning for, and implementation of, configuration changes pursuant to clause 6.2.8.

* + 1. System Security Documentation

|  |
| --- |
| Option: Include the following clause when the Contract will be tendered in conjunction with a linked Contract (Acquisition).  To the extent applicable, the Contractor shall use the versions of the security-related data items developed under the Contract (Acquisition) as the basis for the data items required under this clause 6.2.5. |

The Contractor shall develop, deliver and update an Emanation Security Control Plan (ESCP) in accordance with CDRL Line Number ENG‑860.

The Contractor shall develop, deliver and update the following data items for the SSoIs / ToSAs, which provide part of the suite of Objective Evidence required by the System Owner for the applicable ICT and cyber Security Authorisations:

ISSMP in accordance with clause 6.2.1;

System Security Plan (SSP) in accordance with CDRL Line Number ENG-810;

Security Risk Management Plan (SRMP) in accordance with CDRL Line Number ENG‑820;

SSOPs in accordance with CDRL Line Number ENG-830; and

Cyber Security Case Report (CSCR) in accordance with CDRL Line Number ENG-840.

|  |
| --- |
| Option: Include and, if required, amend the following clause if the Contractor will have responsibility for the Functional Baselines for the Mission System and/or Support System under DSD-ENG-CM.  The Contractor shall also maintain and, where required, update:  the Cyber Security Assurance Basis, which forms part of the Functional Baseline for the Mission System and, where applicable, the Functional Baseline for the Support System; and  the Objective Evidence that is required, and/or has been used, to demonstrate that the Cyber Security Assurance Basis has been achieved,  in accordance with the Configuration Management requirements of DSD-ENG-CM. |

The Contractor shall identify all Technical Data used to meet the security obligations of the Contract, irrespective of whether or not this Technical Data is a data item, in the Technical Data List (TDL) required under clause 9.2 of the SOW.

The Contractor acknowledges that the timings for developing and updating the various items of security documentation under this clause 6.2.5 are tied to other security-related activities under this clause 6.2 (eg, clauses 6.2.3.4, 6.2.7 and 6.2.8 of this DSD) and elsewhere in the SOW (including DSDs).

* + 1. Cyber Supply Chain Security

|  |
| --- |
| Option: Include the following clause when the Contract will be tendered in conjunction with a linked Contract (Acquisition).  The parties acknowledge and agree that:  the Contractor conducted risk assessments and developed and implemented risk mitigation strategies in relation to its Cyber Supply Chains under the Contract (Acquisition); and  the requirements of this clause 6.2.6 only apply to the extent that the risk assessments and/or risk-mitigation strategies conducted under the Contract (Acquisition) no longer apply (eg, because a new Subcontractor has been identified/selected, there are changes to items of DESE and Software being procured, there are changes in the circumstances of existing Subcontractors, or new threats and vulnerabilities have been identified that impact upon particular items of DESE and/or Software). |

The Contractor shall develop, deliver and update a Cyber Supply Chain Risk Plan (CSCRP) in accordance with CDRL Line Number ENG‑850 to identify the Cyber Supply Chain risks associated with the provision of items of DESE and Software for the SSoIs, which will be procured by the Contractor from suppliers that either are, or may become, Subcontractors.

|  |
| --- |
| Option: Include the following clause when the Contract will be tendered in conjunction with a linked Contract (Acquisition).  The Contractor shall use the CSCRP developed under the Contract (Acquisition) as the basis for the CSCRP required under clause 6.2.6.2. |

Note: If the risk matrices from the DSPF are used, the references to ‘Medium’ in the following clauses are to be interpreted as ‘Significant’.

In developing the CSCRP, the Contractor shall:

collaborate with the Commonwealth to define the risk-mitigation strategies to address the potential Cyber Supply Chain risks associated with the supply of items of DESE or Software for the SSoIs, which are assessed as having a Cyber Supply Chain risk (pre-mitigation) of Medium or higher (as determined in accordance with the risk-management processes defined in the Approved ISSMP);

ensure that Approved Subcontractors undertake the identification of Cyber Supply Chain risks and the determination of risk-mitigation strategies for any items of DESE or Software for the SSoIs being provided by those Approved Subcontractors; and

consult with the Commonwealth to discuss and agree the way forward when the Contractor or an Approved Subcontractor is unable to mitigate the Cyber Supply Chain risks associated with the supply of an item of DESE or Software for an SSoI so that the post-mitigated assessment is below Medium (eg, by choosing a different item or by procuring the required item from a different supplier).

Except where otherwise agreed in writing by the Commonwealth Representative, the Contractor shall not utilise DESE or Software provided by a supplier for which the Cyber Supply Chain risk is assessed as Medium or higher.

The Contractor acknowledges that the timings for developing and updating the CSCRP are tied to other activities, including:

the security-related activities under this clause 6.2 (eg, clauses 6.2.7 and 6.2.8 of this DSD) and elsewhere in the SOW (including DSDs); and

the activities to seek DESE or Software from an alternative source of supply.

* + 1. Support to Security Authorisations

Note: As set out in the Glossary, the term ‘Security Authorisation’ embraces terms such as physical security Certification, EMSEC Certification/Accreditation and Authority To Operate (ATO) for ICT security.

The Contractor acknowledges that the applicable Security Authorisations:

are required to be reassessed and, if required, updated on a periodic basis in accordance with the timeframes established by the applicable security authority and documented in the associated Security Authorisation reports (which, for example, depending upon the level of compliance, may range from six months to three years for the Security Authorisations relating to ICT Security);

may need to be updated as part of a Major Change or major Deviation, where a major Deviation is one that, in the context of security considerations, is a Deviation that contains DESE or Software that could introduce security vulnerabilities into an SSoI / ToSA; and

may be required as an outcome of remediation activities to address security issues, as set out in this clause 6.2.7.

The Contractor shall provide support to the Commonwealth’s activities associated with the applicable Security Authorisations:

for any updates required as a result of a Major Change or major Deviation in accordance with clause 6.2.8; and

for periodic reassessments by:

undertaking a review of the SSoIs / ToSAs and the associated security documentation covered by the applicable Security Authorisations sufficiently in advance of the required reassessment date to enable any identified issues to be addressed prior to that date;

undertaking retesting, as determined on a risk basis, to provide assurance and confirm that the security requirements are still being met and that the security controls are still operating effectively in the context of evolving threats and vulnerabilities;

providing a report to the Commonwealth within 20 Working Days of completing its assessments under subclauses (i) and (ii) above, which identifies any issues that need to be addressed, the options for addressing the issues, the recommended approach, and an analysis of the associated costs, benefits and risks;

consulting, co-ordinating and co-operating with the Commonwealth Representative and the relevant Commonwealth security authority to address and resolve any questions of feedback on the report provided under subclause (iii) above;

developing and delivering updates to any data items required for the reassessment in accordance with clause 6.2.5;

developing and delivering any additional or updated Objective Evidence required for the reassessment in accordance with clause 6.2.7.3;

implementing any Major Changes or major Deviations required for the reassessment pursuant to clause 6.2.8; and

undertaking the required activities under this clause 6.2.7.2 in a timeframe that enables the required reassessment date to be achieved (or other timeframe agreed in writing by the Commonwealth Representative).

The Contractor shall provide the necessary Objective Evidence to support the applicable Security Authorisations for the SSoIs / ToSAs, including in relation to the activities being conducted by the Contractor and those being conducted by the Commonwealth. The Contractor shall collaborate with the Commonwealth to agree the data formats and schemas for the delivery of this Objective Evidence.

The Contractor acknowledges that the Commonwealth may raise a security assessment report in relation to a Security Authorisation for a SSoI / ToSA, and when this occurs, the Commonwealth may provide the Contractor with a copy of the report or relevant parts of the report.

The Contractor shall review and assess each Commonwealth-provided security assessment report (or part thereof) and identify remediation activities that are required in relation to the SSoI / ToSA, such that they will meet the requirements for the Security Authorisation.

Within 10 working days of receipt of a Commonwealth-provided security assessment report, the Contractor shall deliver a Remediation Recommendations Report in the Contractor’s format to the Commonwealth.

The Contractor acknowledges and agrees that the required activities to resolve any security shortfalls for a SSoI / ToSA will be determined by the Commonwealth Representative, taking into account the Contractor’s Remediation Recommendations Report.

The Contractor shall undertake the required activities determined by the Commonwealth Representative under clause 6.2.7.7:

as part of the Services for which the Security Authorisation was required; and

except where otherwise agreed by the Commonwealth Representative, in writing, within a timeframe that enables the date for assessment or reassessment (as applicable) to be met.

* + 1. Security Requirements for Configuration Changes

The Contractor shall address the security-related requirements associated with configuration changes to a SSoI / ToSA, including proposed and actual configuration changes arising out of the security monitoring and testing activities under clause 6.2.3, in accordance with:

the Approved CMP, Approved SEMP, Approved SWSP, Approved ISSMP, and other Approved supplementary management plans relevant to a configuration change;

for Major Changes and Minor Changes, the relevant provisions of DSD-ENG-SERV, DSD-ENG-CM and DSD-ENG-SW;

for Deviations, clause 11.4 of the SOW and the relevant provisions of DSD-ENG-CM; and

for configuration changes developed through S&Q Services, clause 3.15 of the COC.

In undertaking the security-related activities for configuration changes, the Contractor shall:

analyse each proposed change (including Software Updates provided by an OEM (eg, patches)) to determine whether or not the proposed change has security implications for the SSoI / ToSA, including undertaking a security risk assessment for each change likely to be classified as a Major Change or a major Deviation, identifying any additional security-related implications for the SSoI / ToSA arising from this risk assessment;

include in its analysis of the proposed change:

physical security, EMSEC, ICT security, cyber security and personnel security;

the implications for the applicable Security Authorisations;

the implications for the security documentation identified under clause 6.2.5; and

to the extent applicable, the other topics required to be addressed under the analysis of change clauses in DSD-ENG-SERV and DSD-ENG-SW;

incorporate its security-related analyses for each proposed change into the report required to be provided under the Analysis of Change Requests clause in DSD-ENG-SERV;

integrate any security-related activities for the configuration change (eg, secure code reviews, system vulnerability assessments and penetration testing) into the requirements for developing Major Changes and major Deviations (including those changes associated with Software Corrective Maintenance), as set out in DSD-ENG-SERV and DSD-ENG-SW, so that any required:

updates to the security documentation under clause 6.2.5;

amendments to the Security Authorisations; and

changes to the ongoing support arrangements,

are incorporated into the plans and processes for the configuration change, including:

for developing and/or updating the documentation for the configuration change (eg, the Baselines for the SSoI / ToSA);

for the design, development and implementation activities, including any associated MSRs;

for undertaking Verification, Validation and other contractually-required acceptance into service activities; and

for amending the Security Authorisations, including to recognise that updated Security Authorisations are necessary precursors to Acceptance of the major Deliverable(s) associated with the configuration change (eg, the modified SSoI, ToSA(s) or applicable Support System Products).

* + 1. Security Investigations

The Contractor shall undertake security investigations and related technical research into:

security incidents associated with the SSoI / ToSA that have arisen during operations and/or Maintenance;

security issues arising out of the Contractor’s security monitoring and testing activities under clauses 6.2.3 and 6.2.7;

security issues identified with DESE or Software delivered through the Contractor’s Cyber Supply Chain;

newly-identified threats and/or vulnerabilities applicable to the SSoI(s), ToSA(s), DESE or Software;

any security-related implications arising from investigations performed in accordance with Engineering Investigations clause in DSD-ENG-SERV or the Maintenance Investigations clause in DSD-MNT-MGT; and

any other security investigations required by the Approved ISSMP.

The Contractor shall undertake the security investigations and reporting required under this clause 6.2.9 as if they were engineering investigations in accordance with the process and pricing and payment arrangements set out in the Engineering Investigations clause in DSD-ENG-SERV.

* + 1. Security Advisory Services (Optional)

Note to drafters: If not required, delete the clause below and annotate the heading as ‘Not used’.

When requested by the Commonwealth Representative in writing, the Contractor shall provide advice on security-related matters, such as:

the implications on the SSoIs, ToSAs, and associated Support System Products arising out of changes to the Governing Security Documents;

the implications of newly-identified threats and/or vulnerabilities;

new/updated security-related tools and the associated costs, benefits and risks; and

potential methodologies for improving the security of the SSoIs, ToSAs and associated Support System Products.

Except to the extent already covered by the other provisions of the Contract (including this DSD) as Recurring Services, the Contractor shall provide the security advisory Services required under this clause 6.2.10 as S&Q Services.

* + 1. Security Working Groups (Optional)

Note to drafters: If not required, delete the clause below and annotate the heading as ‘Not used’.

The Contractor shall conduct Security Working Group (SWG) meetings to establish, refine and to ensure compliance and assurance with the security requirements under the Contract.

The Contractor shall also participate in Commonwealth-conducted SWG meetings, as a non-voting advisor, when requested by the Commonwealth Representative.

|  |
| --- |
| Option: Include the following clause when the Contract will be tendered in conjunction with a linked Contract (Acquisition).  The Contractor shall:  participate in the SWG meetings required under the Contract (Acquisition); and  conduct additional SWG meetings, as required, to address security-related issues with the SSoIs and associated Support System Products delivered under the Contract (Acquisition) and supported under the Contract. |

The Contractor shall conduct SWG meetings under clause 6.2.11.1 as ad hoc meetings in accordance with clause 3.4.6 of the SOW.

The Contractor shall conduct SWG meetings under clause 6.2.11.1 in accordance with the Approved ISSMP.

|  |
| --- |
| Option: Include the following clause when the Contract will be tendered in conjunction with a linked Contract (Acquisition).  The Contractor shall ensure that representatives of the Contractor (Acquisition) and Approved Subcontractors (Acquisition) participate in the SWG meetings under clause 6.2.11.1, where relevant to the work that they will undertake in relation to the Contract or the Contract (Acquisition). |

When the Contractor has been requested to attend a Commonwealth-conducted SWG, the parties shall conduct the preparation, notice and follow-up to the Commonwealth-conducted SWG as an ad hoc meeting in accordance with clause 3.4.6 of the SOW.

The anticipated level of effort required by the Contractor is:

for Commonwealth-conducted SWG meetings, no more than two meetings in any calendar year;

for each SWG, no more than four representatives of the Contractor will be required to attend unless prior Commonwealth approval has been provided, with each of these representatives required to be suitably qualified and experienced in the security domains to be addressed at each SWG; and

the maximum duration of each SWG is expected to be no more than one Working Day with a typical duration of half a Working Day.

SWG meetings may be appended to other meetings if agreed by both parties.

1. The Precedence of Documents clause 1.7 of the COC does not resolve this. While the Glossary has a higher precedence than the SOW, this precedence specifically excludes referenced documents identified in the Glossary. Hence, reference to a specific version in any part of SOW (including DSDs) will override the ‘as amended from time to time’ in the Glossary. [↑](#footnote-ref-1)
2. The ISM defines a shared responsibility model as: “A framework that describes the management and operational responsibilities between different parties for a system. Where responsibilities relating to specific controls are shared between multiple parties, enough detail is documented to provide clear demarcation between the parties.” [↑](#footnote-ref-2)
3. This paragraph was derived from page 4 of the ISM, under the heading ‘Monitor the system’. Further information can be found in the document, “17. ISM – Guidelines for System Monitoring”, which can be downloaded from the Australian Cyber Security Centre (ACSC) web pages. [↑](#footnote-ref-3)
4. The Commonwealth may dictate particular security-related products in high assurance environments, including for DESE or Software that is to be installed on, or interacts with, the Defence Standard Operating Environment (SOE). The Defence Approved Software List (DASL) is an example of this, as are cryptographic devices. [↑](#footnote-ref-4)