Annex D

Cyber Situation Awareness Package

Product Descriptions

Contents:

PRODUCT DESCRIPTION - CySAP COMMON STAFF REQUIREMENT

Version Control

Version No	Date	Author	Approval and Remarks
0.1	13 June 2014	EDA (Stace)	Initial draft for consideration at second meeting of the AHWG on 17/18 June 2014
1.0	20 June 14	AHWG	Agreed version of the CSR.

1. **Purpose**. The purpose of the CySAP Common Staff Requirement (CSR) is to:

   1.1. **expand user requirements** outlined within the scope of the CST in order to,

   1.2. describe the **system requirements** with sufficient detail to enable the potential users to understand capability requirements that have sufficient qualitative and quantitative detail to justify time and cost of subsequent programme implementation.

   1.3. **validate** user requirements within operational environments and scenarios, and with identified user (operational) communities.

2. **Composition**. The CySAP CSR shall be composed of the following:

   2.1. Executive Summary.

   2.2. Introduction.

   2.3. Part One – General Description.

      2.3.1. Origin of the Need. Supplement the 'Background' from the originating CST with any additional solution-focussed background. Conceptual requirements.

      2.3.2. Operational Context. Describe the associated Concept of Use (CONUSE) incorporating the operating environment.

2.3.3. Project Boundary. Explain where the boundary is, or how it will be determined. Identify if architectures or models are to be used or developed.

2.3.4. System Context. Describe any fundamental interdependencies with other systems, examples include hosting platform or infrastructure, and essential interoperability. Identify any other CSR / systems significantly contributing to the same CST.

2.3.5. Constraints. Highlight any constraints that will have a significant or abnormal impact on the system, and which are therefore worthy of management awareness. Include individual Defence Lines of Development (DLoD) 'policy-level' constraints.

2.3.6. Assumptions. Identify any significant overarching assumptions determined by the AHWG, additional to those identified in the CST.

2.3.7. Required In-Service Date (IOC/FOC definitions) based on an assessment of national requirements and associated national programme plans.

2.3.8. Priorities. Carry priorities forward from the CST, and supplemented if appropriate.

2.4. Part Two – Key System Requirements. Part 2 of CSR records the Key System Requirements (KSRs). The following notes apply:

2.4.1. Each KSR should be drawn from Part 3.

2.4.2. Sufficient operational evidence should be applied to reinforce the justification of the prioritisation as a key requirements. This could be the part where levels of capability are defined as core requirements

with subsequent iterations describing more advanced levels of capability.

2.5. Part Three – System Requirements. Part 3 of the CSR contains the complete, structured, set of individual system requirements and constraints. When deriving system requirements from user requirements, opportunities should be sought to cluster and consolidate requirements. Ideally there should be links between identified user requirements and system requirements and information presented in tabular form.

2.6. Part Four – References and Context Documents so that the CSR is self-contained and can stand-alone.

2.6.1. Context documents may be included at the discretion of the AHWG.

2.6.2. Most supporting documentation is included to provide additional understanding or because it is referred to frequently in the CSR.

2.6.3. Additional documents are particularly valuable to readers who may not be familiar with the background to the requirement, for example industry. All system requirements must be included in Part 3 of the CSR regardless of these documents.

2.6.4. Context documents must provide the supplementary information required for verification and system acceptance, expressing the conditions under which the performance must be achievable.

2.6.5. Possible context documents include:

2.6.5.1. The CST - Reference Documents.
2.6.5.2. The Acquisition Strategy.

2.6.5.3. The Acceptance Strategy and associated verification test conditions.

2.6.5.4. The Concept of Use (CONUSE) for the system.

2.6.5.5. The operational process or mission profiles that will use the system - not the system's operating procedure.

2.6.5.6. The system requirements or specification of the legacy system to be updated or upgraded - if applicable.

2.6.5.7. Reference to specifications for Defence Lines of Development (DLoD) solutions, including the Equipment Contract Specifications.

2.6.5.8. Reference to system requirements for interoperating systems, or associated Information Exchange Requirements (IERs) or Interface Control Documents if they exist.

2.6.5.9. Reference to associated architectures or models.

2.6.5.10. Operational Analysis and trade study reports, associated scenarios and vignettes.

2.6.5.11. Other references, policies or Standards.

3. **Derivation.** The sources for the CSR consist of the following:

3.1. CST and supporting references.

3.2. cMS national analysis (related to national capability requirements)

3.3. Outputs from the EDA External Assistance.

3.4. Bilateral and AdHoc research.

3.5. Results for AHWG Meetings and associated AHWG dialogue.

4. **Format and Presentation**. The CSR will be a written report in English (translation requirements?). Paragraphs will be numbered thus (1.1.1 etc (as per the CST)). Drafts will be line numbered and progressions of the Product will be via Comments Matrix. The CSR will be accompanied by a scripted PowerPoint presentation for use by national staff. This will be in English.

5. **Required CySAP CSR Development Competencies/Resources**. The development of the CSR will require a wide range of experience and competences drawn from the following disciplines:

5.1. Technical Expertise in:

5.1.1. Cyber defence technical capabilities (functional services)
5.1.2. Architectures (NAF v3).
5.1.3. Cyber threat intelligence processing.
5.1.4. Systems engineering.
5.1.5. C2 Information Systems and COP application.
5.1.6. Integration of systems and services within national HQs

5.2. Capability Development Expertise

5.2.1. Strategic Requirements
5.2.2. Capability Gap Analysis
5.2.3. User/Operation Requirement Validation
5.2.4. Threat Analysis
5.2.5. Operational Scenario
5.2.6. Dependencies
5.2.7. Strategic/programmatic interfaces (ie extant NATO and national plans)

5.3. System Accreditation Expertise

5.3.1. Security Requirements

6. **Quality Criteria**. cMS will describe what quality criteria will be applied by national staff who will ultimately be authorised to make a decisions based on the CySAP CSR. It is assumed that National capability acquisition decisions will be based on references, input from national subject matter experts and benchmarks/baselines against which CSR system requirements and key system requirements will be endorsed. During the

course of CSR development it is expected that cMS will determine what quantitative and qualitative evidence and criteria is needed to underpin the CSR.

7. **Quality Method**. As the CSR is developed, each national CySAP CSR review process will be determined and incorporated within the CSR together with details on how the Project will be integrated within national programmes and existing capabilities. This should describe responsibilities by post title and any particular national SMEs, resources, dependencies, risks, ambitions, priorities.

PRODUCT DESCRIPTION - CySAP BUSINESS CASE

Version Control

Version No	Date	Author	Approval and Remarks
0.1	9 June 2014	EDA (Stace)	Initial draft for consideration at second meeting of the AHWG on 17/18 June 2014
1.0	20 June 2014	AHWG	Accepted at AHWG Meeting on 18 June 2014

8. **Purpose**. The purpose of the CySAP Business Case (BC) is to justify to cMS authorities the initiation of a collaborative approach to implementing the CySAP modules within EU HQs and potentially other areas of cyber defence operational utilisation.

9. **Composition**. The CySAP BC shall be composed of the following chapters - based on text recommended in the 'EDA Guide to the Conduct of a Programme Preparation Phase':

9.1. Summary.
9.2. Issue.
9.3. Recommendation.
9.4. Timing - related to the recommendation.
9.5. Requirement.
9.6. Options (requirements solutions).
9.7. Option Analysis (cost/benefit analysis).
9.8. In-Service Support.
9.9. Education/Training.
9.10. Service Maintenance. Upgrades and capability growth.
9.11. Interoperability.
9.12. Affordability.
9.13. Procurement & Commercial Strategy. (different acquisition options).
9.14. International Co-operation.

9.15. Risks.

9.16. Legal.

9.17. Safety & Environmental Considerations.

9.18. High-level Plan.

9.19. Whole-life Costs (related to High Level Plan).

9.20. Strategic Context. and link to other.

10. **Derivation.** The sources for the BC consist of the following:

10.1. CST and supporting references.

10.2. TLMP

10.3. CSR

10.4. cMS national analysis (related to national capability requirements)

10.5. Outputs from the EDA External Assistance such as Industrial Analysis and

10.6. Bilateral and AdHoc research.

10.7. Results for AHWG Meetings and associated AHWG dialogue.

11. **Format and Presentation**. The BC will be a written report in English (translation requirements?). Paragraphs will be numbered thus (1.1.1 etc (as per the CST)). Drafts will be line numbered and progressions of the Product will be via Comments Matrix. The BC will be accompanied by a scripted PowerPoint presentation for use by national staff. This will be in English.

12. **Required CySAP BC Development Competencies/Resources**. The development of the BC will require a wide range of experience and competences drawn from the following disciplines:

12.1. Technical Expertise in:

12.1.1. Cyber defence technical capabilities (functional services)

12.1.2. Architectures

12.1.3. cyber threat intelligence processing

12.1.4. COP application and integration within national HQs

12.2. National Acquisition/Armament Expertise (procedural validation)

12.2.1. Economic Case

12.2.2. Commercial Case

12.2.3. Financial Case

12.2.4. Management (national process) Case

12.3. Capability Development Expertise

12.3.1. Strategic Case

12.3.2. Capability Gap Analysis

12.3.3. User/Operation Requirement Validation

12.3.4. Threat Analysis

12.3.5. Operational Scenario

12.3.6. Dependancies

12.3.7. Strategic/programmatic interfaces (ie extant NATO and national plans)

12.4. System Accreditation Expertise

12.4.1. Security Case

13. **Quality Criteria**.

cMS will describe what quality criteria will be applied by national staff who will ultimately be authorised to make a decision based on the CySAP BC Recommendation(s). It is assumed that National capability acquisition decisions will be based on references and benchmarks/baselines against which BC options will be assessed. What levels of quantitative and qualitative evidence is needed to enable decisions to be made? Each CySAP module may require different criteria.

14. **Quality Method**.

As the BC is developed, each national CySAP BC review process will be determined and incorporated within the BC together with details on how the Project will be integrated within national programmes. This is an opportunity for cMS to describe national process and timelines to support the progression of CySAP beyond the

Programme Preparation Phase. This should describe responsibilities by post title and any particular national skills, resources, dependencies, risks, ambitions, priorities.

PRODUCT DESCRIPTION - CySAP THROUGH LIFE MANAGEMENT PLAN

Version Control

Version No	Date	Author	Approval and Remarks
0.1	9 June 2014	EDA (Stace)	Initial draft for consideration at second meeting of the AHWG on 17/18 June 2014

1. **Purpose**. The purpose of the CySAP Through Life Management Plan(TLMP) is to provide cMS with the results of collaborative analysis on how the CySAP capability will be managed across its life cycle from Concept, Assessment (…of capability lines of development, business cases and acquisition options), Development & Demonstration, through to implementation into service and through life support to eventual withdrawal of service. The TLMP document supports the CySAP Business Case.

2. **Composition**. The CySAP TLMP shall be composed of the following chapters - based on text recommended in the 'EDA Guide to the Conduct of a Programme Preparation Phase':

    2.1. Summary.
    2.2. Mission & Objectives.
    2.3. Stakeholders.
    2.4. Strategies.
    2.5. Plans and Processes.
    2.6. Resources.
    2.7. Evaluation of Success.

3. **Derivation.** The sources for the TLMP consist of the following:

    3.1. CST and supporting references.
    3.2. CSR Process.
    3.3. cMS national analysis (related to national capability requirements)
    3.4. Outputs from the EDA External Assistance such as Industrial Analysis and

3.5. Bilateral and AdHoc research with industry partners.

3.6. Results from AHWG Meetings and associated AHWG dialogue.

3.7. TLMP Reference:
www.eda.europa.eu/EDSTAR/Libraries/Standards_Docs/eg13.sflb.ashx

4. **Format and Presentation**. The TLMP will be a written report in English (translation requirements?). Paragraphs will be numbered thus (1.1.1 etc (as per the CST)). Drafts will be line numbered and development of the Product will be via Comments Matrix. The TLMP will be accompanied by a scripted PowerPoint presentation for use by national staff. This will be in English.

5. **Required CySAP TLMP Development Competences**. The development of the TLMP will require a wide range of experience and competences drawn from the following disciplines:

5.1. Technical Expertise in:

5.1.1. Cyber defence technology life cycle.

5.1.2. Architectures - integration of TLMP within NAF (also see www.modaf.com)

5.1.3. TLMP relevance to system integration with Threat source and COP applications, and integration within national HQs

5.2. National Acquisition/Armament Expertise (alignment and coherence with national processes and procedural validation).

5.2.1. Whole Life Cost (WLC) planning.

5.2.2. Commercial analysis.

5.2.3. Financial - investment appraisals/cost modelling.

5.2.4. Management (national process) Case - resource programming.

5.3. Capability Development Expertise.

5.3.1. Strategic Case.

5.3.2. Dependancies

5.3.3. Strategic/programmatic interfaces (ie extant NATO and national plans)

5.4. System Accreditation Expertise.

5.4.1. Security Case coherence with national requirements.

6. **Quality Criteria**. The TLMP is a supporting document to the Business Case within the CSR process and as such there is no specific approval requirements by cMS. However, TLM is an important element of the CySAP capability and needs to be coherent with national ways and means of establishing the operation of such a capability. *What levels of quantitative and qualitative evidence is needed to enable such coherence to be established? Each CySAP module may require a different TLM solution.*

7. **Quality Method**. *This should describe each national CySAP TLMP review process and how the TLMP will be integrated within national programmes. This is an opportunity for cMS to describe national process and timelines to support the progression of CySAP beyond the Programme Preparation Phase. This should describe responsibilities by post title and any particular national skills, resources, dependencies, risks, ambitions, priorities.*