SSRO

Single Source
Regulations Office

DefCARS Future: Specialist Support

Appendix 1: Specification

1. Introduction

1.1 The Single Source Regulations Office or SSRO is an executive non-departmental public body, sponsored by the Ministry of Defence (MOD). We play a key role in the regulation of single source, or non-competitive defence contracts.

1.2 When undertaking our statutory functions, we aim to ensure that good value for money is obtained in government expenditure on qualifying defence contracts, and that persons who are parties to qualifying defence contracts are paid a fair and reasonable price under those contracts.

1.3 The Defence Reform Act 2014 ('the Act') created a regulatory framework for single source defence contracts. The framework came fully into force in December 2014, following Parliamentary approval of the Single Source Contract Regulations 2014 ('the Regulations'). The framework places controls on the prices of qualifying contracts and requires greater transparency on the part of defence contractors. The SSRO is at the heart of the regulatory framework, supporting its operation.

1.4 Additional general information about the SSRO, can be found on our website: **http://www.gov.uk/government/organisations/single-source-regulations-office**

2. Defence Contracts Analysis and Reporting System (DefCARS)

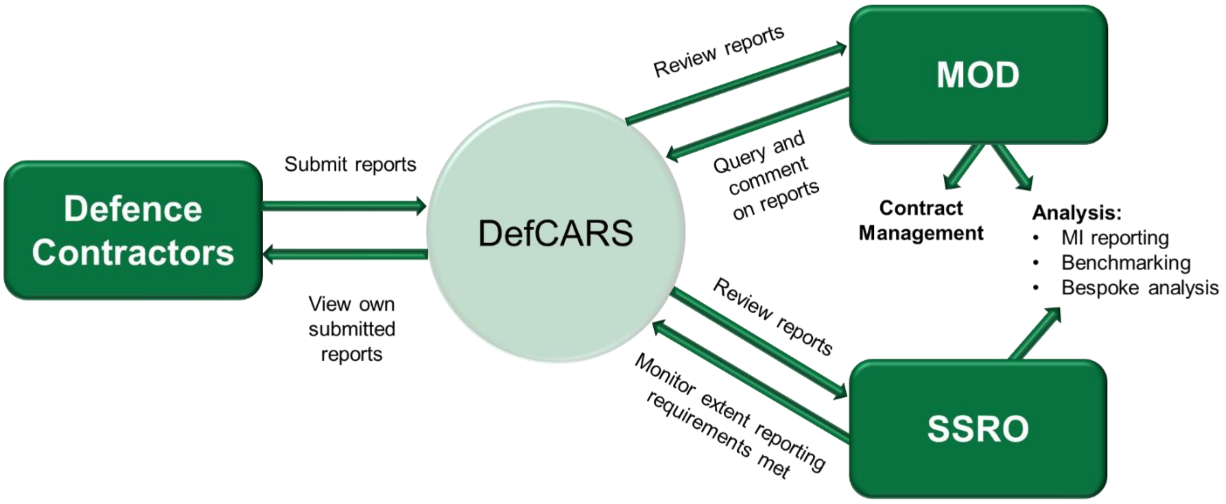
2.1 Defence contractors are required to provide reports to the SSRO and the MOD if they hold qualifying contracts under the regulatory framework. The Regulations prescribe the types of reports, their contents and the circumstances in which they must be provided.

2.2 The SSRO has established the Defence Contracts Analysis and Reporting System (DefCARS) as a secure, online system that is easy to use for the capture, storage and analysis of all electronic data reported by defence contractors and suppliers in accordance with the Act and the Regulations. DefCARS is accessed by industry, MOD and the SSRO and it:

- Enables defence contractors to submit statutory reports and access their data.
- Facilitates monitoring of compliance with reporting requirements by the SSRO[1], and facilitates the review of reports by the MOD.
- Holds reported data and makes it accessible.
- Produces reports and supports analysis of reported data.

[1] **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/915749/Compliance_and_review_methodology_January_2020_A.pdf**

Figure 1: DefCARS current functionality



2.3 The current system is a web-based tool, which was launched in 2017 and replaced an earlier system that had been in operation from commencement of the Regulations.

2.4 DefCARS is intended to provide a user-friendly web interface and facilitate both reporting obligations and the discharge of several of the SSRO's functions. Reports are predominantly financial in nature, in addition to some project information such as milestones.

2.5 DefCARS has approximately 1,500 users and is accessed via a User Interface built using a Microsoft ASP.NET framework. These users range from occasional (once per year) contractor users, to those making regular use including finance professionals from large defence contractors and analysts from SSRO and the MOD. The data is submitted by external defence contractors and, therefore, security and auditability of the data submitted within DefCARS is one of the SSRO's key priorities.

2.6 DefCARS is designed to allow defence contractors to input data in an efficient way. The front-end application allows manual data entry into fixed fields, as well as copy and paste functionality into larger expandable tables. Certain data required across multiple reports will only need to be entered once and is auto populated from one report to another and validation checks (warnings and errors) will provide the submitter with assistance when reviewing data entered. The SSRO publishes Reporting guidance[2] (including guidance on DefCARS functionality), to which defence contractors must have regard when preparing reports.

2.7 DefCARS is a bespoke system, built by third party developers and hosted in their secure private datacentre. Ongoing development, support, and maintenance is carried out by Synectics Solutions Ltd, under a contract that ends in 2022. The system runs from a Microsoft Technology Stack: the front end is a Microsoft ASP.NET MVC Web App, data is held in a Microsoft SQL Server database, and MI/BI is produced using a bespoke query builder and report builder based on SQL Server Reporting Services. The SSRO has ownership of the code behind DefCARS and the data.

[2] **https://www.gov.uk/guidance/contract-and-supplier-reporting-defcars-and-associated-guidance**

3. DefCARS Future

3.1 The SSRO's Corporate Plan 2020-23[3] sets out that the SSRO wants "to reduce the administrative burden for industry and the MOD in using DefCARS. We intend to pursue opportunities for further digital transformation where we can make the regime more streamlined and efficient, and we will seek targeted, one-off capital investments to enable this. We will seek innovations in DefCARS that allow us to work better with stakeholders and we will consider:

- supporting data analytics and decision support including interfacing with MOD systems;
- automated transfers between industry systems and DefCARS in a highly secure way; and
- developing DefCARS into modular services that can be delivered and developed flexibly."

3.2 An internal SSRO project has begun to assess the strategic future of the DefCARS regulatory reporting database and the team is investigating the possible directions the system may take. For the purposes of the project, the function of the system has been broken down into several key areas; Data capture, Data storage and Data use, in addition to overall integration as well as technology and security design considerations. The potential areas of enhancement include:

- Capture:

  (a) Facilitate automated and bulk upload of data (through import templates and/or API) for defence contractors by revisiting the design of the Graphical User Interface (GUI);

  (b) Improve flexibility to changing data requirements if required by legislation or MOD, by reconfiguring the GUI;

  (c) Enhance the compliance process (a messaging functionality currently provided through a bespoke interface) which could be more easily maintained and improved by using new technologies, such as data analytics and visualisation, or machine learning;

- Store:

  (a) Reduce cost and improve data accessibility for MOD by moving DefCARS from a private data centre to the Cloud;

  (b) Make data more personalised and available to MOD analysts by redesigning the analytical database;

- Use: Create and automate bespoke management and business information reporting for MOD and SSRO; and
- Integration: Support effective procurement and system flexibility by creating a modular system using more off-the-shelf software products.

3.3 We are considering whether options are best pursued by developing the current system in the short term and/or in a subsequent contractual arrangement.

[3] **https://www.gov.uk/government/publications/ssro-corporate-plan-2020-2023**

4. The requirement

The SSRO is seeking to appoint an expert in digital services (the ‘Contractor’) to carry out the Core Services described below and, potentially, further Optional Services also referred to.

Core Services

4.1 The SSRO requires the Contractor to look at the current version of DefCARS (‘as is’) and to map out what the technology opportunities and risks are in transitioning to a range of possible future states, within the context of our budget and the potential enhancements identified (paragraph 3.2). The overall aim is that the additional clarity provided by the Contractor’s outputs will allow the options for the overall project to be assessed with significantly increased confidence, allowing more informed commercial decisions to be made.

4.2 The Contractor is required to deliver the following:

- A written report, mapping out what the technology opportunities and risks are in transitioning to a range of future states, within the context of our budget and the potential enhancements identified (paragraph 3.2). The report must consider / include:

  (i) Commentary and feedback on the ‘as is’ position, considering longevity and risks, and an assessment of the gap between the current system and potential future enhancements;

  (ii) The provision of a high level ‘menu’ of options for the future of the system, setting out how the design and build of the system could transition from the ‘as is’ position to a future state, and a high-level transition timeline;

  (iii) For the options, identification of potential providers and off-the-shelf products, cost and timescale estimates, and identify the key parameters that the SSRO could use to evaluate and choose between the options;

  (iv) Identified interdependencies of modular changes, and suggesting sequencing of these developments via step changes, and one-off investments that would improve the system;

  (v) The options to cover hosting, support / maintenance, as well as the high-level technical architecture database and MI architecture options; and

  (vi) Cost efficiency opportunities we may be able to achieve for the SSRO as well as for our users

- Three presentations to attendees from SSRO, MOD and industry, summarising the report and explaining the opportunities and challenges ahead of us and the MOD.

4.3 The Contractor must provide to the SSRO a draft report, to be revised based on comments received prior to the final report submission date.

4.4 The advice and report must take into account relevant requirements for DefCARS including that:

- The SSRO expects the broad user requirements set out in Figure 1 to remain unchanged (although we will be validating user requirements);

- DefCARS is accredited by MOD to hold and make available Official Sensitive – Commercial data. Any solution must continue to meet the requirements for accreditation;

- The data architecture must facilitate data analysis and re-use, the sharing of data and analysis securely between organisations, and data must be accessible outside of the core product for authorised users to perform additional analysis;

- Existing data will need to be migrated into any new product(s) and potential additional data could be sourced from relevant third parties;

- The database needs to meet audit requirements, including a full audit trail including an audit trail to understand interactions with the system; and

- The SSRO does not expect any future solution to require increases in the current on-going cash costs we incur but does require advice on the pricing of improvements that could be initiated with additional funding above our current system budget.

4.5 The advice and report must take into account relevant considerations including that:

- The SSRO expects that a transition will take place to a new system over a number of years, and is keen to explore whether this can provide a more cost-effective way forward than a ‘big bang’ change;

- While the current DefCARS provides a solution within a single contract and system, the SSRO is keen to explore whether a modular approach might deliver greater efficiencies and effectiveness;

- The SSRO has not set in stone any changes, and requires an independent view on the options that we face;

- The MOD and the SSRO already utilise Microsoft products including Office 365 and Power BI (although not with shared access), and so the options should include exploration of making wider use of the current Microsoft technical stack, e.g. Azure, SQL server, PowerBI, Power Automate;

- Defence contractors who are required to make reports all run separate IT systems often operating behind extensive security systems due to sensitive information, and there needs to be a simple way to access DefCARS to upload information. The SSRO only specifies very limited minimum technical requirements to operate DefCARS;

- The options must consider to what extent we can utilise custom build or Commercial-off-the-Shelf products (COTS) where cost efficiencies or flexibility is required; and

- DefCARS is delivered through a mix of external contractor and SSRO staff operating the system, and in future the SSRO expects there will continue to be a mix of internal/external resource, but perhaps a different mix.

4.6 The SSRO will make available any relevant documentation the Contractor reasonably requires to complete the report, including internal SSRO information on the system architecture and project documentation in the ‘as-is’ assessment. The SSRO expects that the Contractor may wish to interview the following (in respect of which the Contractor may be required to enter into Non-Disclosure Agreements), and the SSRO will facilitate access as reasonably required:

- SSRO senior staff, business analysts and subject matter experts.

- Our third-party provider (Synectics Solutions Ltd.)

- Our external Security Information Risk Advisor (SIRA) – Hex Ltd.

4.7 The following aspects are not within the required scope of the work:

- While SSRO will be engaging with users from MOD and industry during the course of the work to better understand user requirements. The Contractor is not required to produce detailed user requirements documentation.

- The Contractor will only have supervised access to DefCARS or data from it. A detailed assessment of the operation of the current system is not required.

4.8 The Contractor must engage and correspond at working level with the SSRO in a way that enables it to monitor the progress of the work, respond to questions and comment on the findings of the draft report prior to it being finalised. The SSRO utilises Microsoft Teams for the purposes of telephone and video communications. The Contractor must have the ability to connect to participate in video and voice only calls held via Microsoft Teams or provide their own capability that the SSRO can access to communicate using audio and video. The SSRO will provide a point of contact for the Contractor to provide relevant information and answer questions.

4.9 The Contractor must complete the Core Services work by 31 March 2021 (the “Long-stop Completion Date”). The following timetable sets out the proposed milestones for delivering the Core Services work, variations to which (other than the Long-stop Completion Date) may be agreed between the Contractor and the SSRO.

Milestone	Date due
Draft report	26 February 2021
Final report	12 March 2021
Presentations	Weeks commencing 15 and 22 March 2021

Optional Services

4.10 The SSRO may, at its sole discretion, also require the provision of additional support days up to 31 March 2022 for additional or follow up work related to the Core Services. The SSRO does not guarantee any minimum level of work or spend in respect of these Optional Services, which it may draw upon as needed. The procedure for agreeing any Optional Services, including the scope, is set out in clause 5 of the contract.

5. Service approach / management

5.1 The Contractor must nominate a manager whose role is to:

- manage the service and relationship with the SSRO including the assignment of resources;
- ensure the quality and timelines of any deliverables;
- act as primary point of contact for the SSRO throughout the contract duration;
- ensure compliance with security requirements;
- remain consistently informed about the Contractor’s performance on all matters;
- be available to address issues in a timely manner and meet any urgent

requirements within an acceptable timeframe;

- ensure that the agreed price structure is followed and that costs are communicated to the SSRO on a routine basis throughout the service delivery; and
- be a point of contact for the SSRO's auditors if necessary.

6. Security Arrangements

6.1 In carrying out its corporate functions, the SSRO processes information of the following kinds:

- Official information, which may be marked OFFICIAL SENSITIVE with the Government Security Classifications.
- Confidential or commercially sensitive information, which the SSRO would not disclose under the Freedom of Information Act 2000 by reason of the application of one of the exemptions in that Act.
- Personal data or special category data within the meaning of the General Data Protection Regulation and the Data Protection Act 2018 which must be processed in accordance with applicable data protection law.

6.2 The Contractor must handle all materials and communication in connection with the services in a confidential manner. Confidentiality will attach to all information given to the Contractor by the SSRO or a third party, or materials or communication generated by the Contractor, in connection with delivery of the Services. The Contractor's attention is drawn to Schedules 1 and 2 of the Contract, which sets out the Contractor's obligations in this respect.

6.3 The Contractor must ensure that all personnel assigned to the contract have undergone personnel security checks equivalent to the HMG baseline personnel security standard. Should the Contractor designate any personnel with privileged access to SSRO information assets, those designated personnel must hold UK HMG security clearance at SC level or above.

6.4 The SSRO IT environment, policies and procedures are based on the following policies and procedures, and the Contractor must ensure that any proposed solution option will be consistent with the wider HMG digital service and security policy framework, including:

- HMG Security Policy Framework (SPF).
- NCSC Published Guidance, Cloud Security Principles and Security Design Principles.
- ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.
- Cyber Essentials Scheme: Requirement for Technical Protection from Cyber Attacks.

6.5 The Contractor must be, and continue to be for the contract duration, Cyber Essentials Plus as well as ISO27001 certified.

6.6 Where the Contractor has confirmed that it holds any industry recognised security and data handling schemes / accreditations / certificates (such as ISO security standards), the Contractor must comply and act in accordance with such standards in the delivery of the services throughout the duration of the contract.

6.7 The SSRO IT environment uses the Microsoft platform including Windows 10, Office 365, Intune and Enterprise Mobility and Security. This is complemented by infrastructure services including Azure virtualisation, Cisco Switches and ASA firewalls, a VPN solution which uses Cisco AnyConnect VPN client software, and wireless network using Meraki Wireless Access Points.

6.8 The Contractor should provide a secure file sharing platform for a small number of SSRO project team staff to minimise the need to email sensitive information.

7. Conflicts of interest

7.1 The avoidance of Conflicts of Interest is critical to the SSRO. Its minimum requirements are set out in clause 30 of the contract.