SSRO

Single Source
Regulations Office

Security and Information Risk Advisor (SIRA) services

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 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. The Service Specification

Background

2.1 The most valuable of the SSRO's assets is its information. Measures need to be taken to protect this information, not only to ensure compliance with legal and contractual obligations, but also to retain a high degree of trust with the SSRO's sponsoring department (MOD), the business industry and the public. Maintaining this trust is essential to the effective operation of the SSRO. It is for this reason that the Defence Reform Act (2014) provides for a specific criminal offence relating to the unlawful disclosure of information obtained through the SSRO's work. The protection of information is the responsibility of everyone within the SSRO, including staff, contractors and Board members as directed by the Senior Information Risk Owner (SIRO).

2.2 The MOD, as the SSRO's sponsoring department, provides security advice to the SSRO, and the SSRO adheres (to the extent required by the SSRO) to the requirements of the HMG Security Policy Framework and MOD security policies, as well as NCSC policies and guidance. The SSRO SIRO directs a sensible balance between ensuring that the organisation's assets are protected from harm and ensuring that people who have the right to use its assets are able to do so.

2.3 The SSRO is outsourcing a service which helps to manage, analyse and report on Single Source Defence Contracts (Defence Contracts Analysis and Reporting System; DefCARS) and assist in the provision of transparency and fair outcomes for both public funds and defence contractors.

2.4 The SSRO DefCARS system is required to handle information at the OFFICIAL level and be capable of supporting special handling descriptors such as OFFICIAL-SENSITIVE COMMERCIAL. The service is being hosted on a private cloud environment and holds sensitive commercial information. The system needs to be accessed by the SSRO, authorised industry personnel and staff at the MOD, with specific restrictions placed on each user-type to limit access and functionality.

2.5 Full security accreditation for the DefCARS scope was issued to the SSRO by the MOD Defence Assurance and Information Security (DAIS) accreditor in February 2016 (Defence

Assurance Risk Tool Target of Assurance DART TOA 3411), following formal risk assessment, risk treatment, and assurance processes in accordance with HMG and MOD policy and evidenced in the DefCARS Risk Management and Accreditation Document Set (RMADS). The RMADS was prepared in accordance with HMG Information Assurance Standard No.1 and 2, GPG 47 – Information Risk Management and supported by a Technical Risk Assessment and Treatment Plan completed against HMG Information Assurance Standard No.1 and 2 Supplement.

2.6 In addition, the RMADS follow the guidance provided in the HMG SPF to preserve the confidentiality, integrity and availability of all assets identified within the accreditation scope and to ensure that they operate effectively and securely. The accreditation scope includes all assets used to store, transmit and/or process information as part of the SSRO DefCARS service.

2.7 The management and support of the SSRO's corporate IT environment, which uses MS Azure and Office365, is also outsourced. This includes the provision of secure cloud connectivity and a 24/7 Security Operations Centre. During the annual accreditation review in March 2019, the SSRO's corporate IT environment was added to the accreditation scope and the RMADS updated to reflect this accordingly.

2.8 The SSRO uses a Governance, Compliance and Risk tool, Acuity Stream, and all DefCARS related accreditation information has been loaded into the tool with a view to undertaking the 2020 annual accreditation review using the tool and reports from the tool. The annual accreditation review is expected to be conducted based on the threat list established from NIST SP 800-30 and a short exercise will need to be undertaken before the review with the aim of confirming this change in approach.

Service requirements

2.9 The SSRO requires Security and information Risk Advisor (SIRA) services to provide it with advice on the management of security and information risk consistent with the UK Government's information assurance policy and other sector specific guidance, with particular emphasis on the specific requirements of the Single Source Regulations Office as an independent agency of the Ministry of Defence.

2.10 Individual(s) assigned to this engagement must be SIRA Certified Cyber Professionals (CCP), a certification scheme operated by the National Cyber Security Centre (NCSC). The contract and overall service must be overseen and managed by a Lead Practitioner; most of the work is expected to be carried out by a Senior Practitioner.

2.11 Based on previous requirements, the SSRO anticipates that it will need between eight and fifteen days of service per annum (or approximately 50 days over the contract period) for the purposes of the programme of planned activities (paragraph 2.14) including the preparation and delivery of security accreditation projects, Board-level briefings, training and ad hoc advice. Most of the engagement expected is in relation to the security accreditation of DefCARS and SSRO's MS Azure & Office365 environments. For the purposes of the potential additional services (paragraph 2.17) the SSRO anticipates that it may require up to 35 days service over the entire contract period.

2.12 Throughout the contract period, the SSRO will make available to the Contractor any relevant documentation, data etc. required for the Contractor to deliver the services. The SSRO's IT suppliers, MOD staff and the SSRO team (including the SIRO) will be available for interviews, meetings workshops. Meeting and desk facilities at the SSRO offices are available to support the engagement.

2.13 All documentation produced as part of the engagement must be supplied in PDF as well as in editable Microsoft Office formats, and must use the SSRO house style and branding. This

may require reformatting where Contractor templates, tools or documents are used in this engagement. The Contractor's branding must not appear on any such documentation, unless the SSRO require it (e.g. accreditation documents).

Programme of planned activities

2.14 A rolling programme, including recurring and one-off activities, will be jointly planned between the SSRO and the Contractor and regularly reviewed so that internal resources can be allocated to the engagement. The programme for the 18 months from January 2020 (expected contract commencement date) covers:

- Feb 2020: Refresh of an ISO27001 gap analysis which was completed by an external agency in 2016
- Feb 2020: Review and recommendation of the security accreditation approach
- Feb/Mar 2020: Annual security accreditation review including:
  (a) advising on scope and outcome of the system security health check and penetration testing;
  (b) reviewing and updating the RMADS/Stream liaising with the SSRO, DefCARS supplier and the MOD as necessary;
  (c) potentially a data centre visit (current DefCARS data centre location is Stoke-on-Trent);
  (d) running a joint accreditation review workshop of SSRO, DefCARS supplier and the MOD with focus on RMADS changes and residual risks;
  (e) completing all associated documentation.
- May 2020: Input to annual SSRO IT and Information Management Policy review undertaken by SSRO
- Feb/Mar 2021: Annual security accreditation review
- Apr/May 2021: Input to annual SSRO IT and Information Management Policy review undertaken by SSRO

Ad hoc services

2.15 There will be occasional need for the Contractor to advise the SSRO on specific queries in relation to cyber security and information risk management matters, as well as a requirement for general keeping in touch with the MOD accreditor and the SSRO.

2.16 The SSRO would expect to benefit from the Contractor's wider work in cyber security and information risk management through updates or briefings as appropriate.

Additional services

2.17 During the contract period, additional service requirements may emerge that cannot be covered by the rolling work programme. This could be more extensive Security Impact Assessments or input into substantive technology reviews or procurement projects. Any such additional services will need scoping and agreed funding before they can proceed.

Service approach / management

2.18 The Contractor must nominate a manager at SIRA Lead Practitioner level whose role is to:

- manage the service and relationship with the SSRO including the rolling work program and assignment of resources;
- ensure the quality and timelines of any deliverables;
- act as primary point of contact for the SSRO throughout the contract period;
- 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; and
- ensure that the agreed price structure is followed and that costs are communicated to the SSRO on a routine basis throughout the service delivery.

2.19 The SSRO expects ad hoc services (referred to at paragraphs 2.16 to 2.17) to be non-chargeable unless the frequency or complexity increase to a level that these cannot be provided serendipitously to the program of planned activities and potential additional services, in which case the arrangements will be agreed between the parties.

2.20 Much of the work can be delivered at the Contractor's site(s), though full or part day attendance at the SSRO's office and occasionally at an MOD site (DAIS) or DefCARS supplier site will be required as necessary for the effective delivery of the engagement.

Security Arrangements

2.21 Delivering the services will necessitate the Contractor processing confidential and commercially sensitive information. The Contractor's attention is drawn to Schedules 1 and 2 of the Contract, which sets out the Contractor's obligations in this respect.

2.22 The SSRO maintains Cyber Essentials Plus certification and the Contractor must be Cyber Essentials Plus certified.

2.23 Individual(s) assigned to the contract, including the Lead Practitioner and Senior Practitioner, must hold UK HMG security clearance at SC level or above.

2.24 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 contract period.

Conflicts of interest

2.25 In delivering the services, the Contractor shall always act in the best interests of the SSRO and shall at no time subordinate or otherwise undermine the SSRO's interests to the advantage of its own interests or those of any third party. The Contractor's attention is drawn to clause 30 of the Contract which contains the Contractor's obligations for managing potential and actual conflicts of interest.