SSRO

Single Source
Regulations Office

Security and Information Risk Advisor (SIRA) services

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**.

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 Act 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 Security Senior Responsible Owner (SRO).

2.2 The MOD, as the SSRO's sponsoring department, provides security advice to the SSRO, and the SSRO adheres (to the extent required) to the requirements of the HMG Security Policy Framework, Government Functional Standard 007:Security, and MOD security policies, as well as the National Cyber Security Centre (NCSC) policies and guidance. The SSRO's SRO directs a balance between ensuring that the organisation's assets are protected from harm and ensuring those who have the right to use its assets can.

2.3 The SSRO outsources a service to develop and maintain its Defence Contracts Analysis and Reporting System (DefCARS). This system helps to manage, analyse and report on qualifying contracts and assists in the provision of transparency and fair outcomes for both public funds and defence contractors.

2.4 DefCARS 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 hosted on a public 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 DefCARS was issued to the SSRO by the MOD Defence Assurance and Information Security (DAIS) accreditor in February 2016, 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. In addition, the RMADS followed 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 included all assets used to store, transmit and/or process information as part of the SSRO DefCARS service.

2.6 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.

2.7 More recently, following the MOD transition from an accreditation approach to the Secure by Design (SbD) approach published within JSP 440 Part 2 Leaflet 5C – Building Cyber Secure by Design Capabilities **Error! Reference source not found.**, the MOD Cyber Security Assessment and Advisory Services (CySAAS) team will no longer validate, authorise or accredit systems. For the SSRO, all decisions and acceptance of associated security risks continue to be made and carried out by the SRO.

2.8 DefCARS and the SSRO IT and Cloud-based Services were previously granted 'accreditation' under TOA-57887\2 until 31st July 2026. However, the SSRO completed the MOD SbD transition process in 2024 via the DART interim process under TOA-61367. With the completion of this, TOA-57887\2 has been retired and SSRO SbD submissions are now conducted through the MOD Cyber Assurance Activity Tracker (CAAT) application with support from the MOD's SSPS Data, Digital and Programme Office.

3. Service requirements

3.1 The SSRO requires Security and Information Risk Advisor (SIRA) services to provide it with expert advice on the management of security and information risk. Such advice must be consistent with the UK Government's information assurance policy and relevant sector specific guidance, with particular emphasis on the specific requirements of the SSRO as an independent body of the Ministry of Defence.

3.2 Individual(s) delivering services under this contract must, for the contract period, be any of i) SIRA Certified Cyber Professionals (CCP), a certification scheme driven by the National Cyber Security Centre (NCSC), or ii) members of the Chartered Institute of Information Security (CIISec), or iii) Chartered Cyber Security Professionals (ChCSP), or iv) equivalent. The contract and overall service must be overseen and managed by a Lead Practitioner (or equivalent); most of the work is expected to be carried out by a Senior Practitioner (or equivalent).

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

3.4 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 the Supplier's templates, tools or documents are used. The Supplier's branding must not appear on any such documentation, unless the SSRO requires it.

Programme of planned activities

3.5 Based on previous requirements, the SSRO is contracting for the following level of support: a fixed requirement of 15 planned days of service per annum for the purposes of the programme of planned activities. These planned activities include the preparation and delivery of security assurance activities and evidence (including quarterly and annual SbD reviews), Board-level briefings, training and ad hoc advice. Most of the engagement expected is in relation to the security assurance of DefCARS, the SSRO's MS Azure & Office365 environments and the SSRO's website.

3.6 A rolling programme, including recurring and one-off activities, will be jointly planned between the SSRO and the Supplier and regularly reviewed so that internal resources can be allocated to the engagement. The programme can be expected to include:

- Quarterly and annual assurance reviews to support the SbD process, including the review and delivery of the annual Security Case Report (SyCR), liaising with the SSRO, DefCARS supplier and the MOD as required to allow the SSRO to make submissions via the CAAT. This is to include:

    a) Reviewing the results of and advising on scope and outcome of the system security health check and penetration testing;

    b) Collating, reviewing and updating the required documentation, including maintaining the foundation and in service 'CAAT' questionnaire template updates; and

    c) Running joint assurance review workshops with the SSRO, DefCARS and IT Managed Service (ITMS) supplier and the MOD with a focus on risk management documentation, system changes and residual risks.

- Input into the SSRO's annual security and information management policy review programme; and

- Audit and Risk Committee (ARAC) and staff cyber security briefs.

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

Additional services

3.8 During the contract period, additional optional service requirements may emerge that cannot be covered by the rolling work programme. These days are not guaranteed by the SSRO but, if required, may be used variably across the contract period (for example, a higher number of days in one year and none in another), subject to the total number of days over the initial three-year period not exceeding 30. Any such additional services will to be agreed and commissioned in accordance with clause 5 of the contract (Optional Services)). Such additional services may include (but are not limited to) the following:

- More extensive Security Impact Assessments, facilitating Business Continuity exercises (including cyber resilience testing) or input into substantive technology reviews or procurement projects.

- Advice on specific queries in relation to cyber security and information risk management matters, as well as general keeping in touch with the MOD Cyber Security Assessor and the SSRO.

Service approach / management

3.9 The Supplier must nominate a manager at SIRA Lead Practitioner level who shall:

- manage the service and relationship with the SSRO including the rolling work programme 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 Supplier'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.

Ad hoc services

3.10 The SSRO may, from time to time, raise ad hoc queries with the Supplier or request short items of security advice of a low level of effort. Where such requests:

- are limited in scope and complexity;
- do not require significant investigation, analysis or formal deliverables; and
- are capable of being responded to promptly (normally within five (5) working days, subject to agreement),

these ad hoc services shall be provided at no additional charge and not be counted against the annual allowance of days for planned activities or any additional services. Where the frequency, urgency or complexity of ad hoc requests increases to a level such that they cannot reasonably be accommodated, the Supplier shall notify the SSRO promptly. In such circumstances, the parties shall agree how the work is to be treated, including whether it is to be delivered as part of the programme of planned activities or as additional services. Without limitation, chargeable triggers for such ad hoc services may include:

- recurring or repetitive tasks;
- requests requiring formal outputs or deliverables;
- requests requiring significant investigation or analysis; or
- urgent support requests that materially disrupt the agreed programme of planned activities or potential additional services.

3.11 Much of the work can be delivered at the Supplier's site(s). Full or part day attendance at the SSRO's office and occasionally at an MOD site or DefCARS / ITMS supplier site will be required as necessary for the effective delivery of the services (and the costs associated with such attendance, including travel, shall be included in the price/rate(s) stated in the Pricing Schedule).

4. Transition

4.1 The SSRO does not expect a significant amount of transition activity will be necessary between the Supplier and the outgoing supplier (where applicable). However, where such activities are required, the Supplier must undertake them and take the necessary measures to ensure continuity of business services (except for any planned and agreed downtime that may be required, as set out in the Tender). Such transition activities shall not be chargeable.

5. Security Arrangements

5.1 Delivering the services will necessitate the Supplier processing confidential and commercially sensitive information. The Supplier's attention is drawn to clause 23 of the Contract and Schedules 1 and 2 of the Contract, which sets out the Supplier's obligations in this respect.

5.2 The SSRO maintains Cyber Essentials Plus certification and the Supplier must be Cyber Essentials Plus certified throughout the Contract Period.

5.3 Individual(s) assigned to the delivery of the services under this contract, including the Lead Practitioner and Senior Practitioner, must hold UK HMG security clearance at SC level or above and be UK based (except with the express permission of the SSRO's SRO).

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

5.5 The Supplier shall ensure that the physical locations where it stores, processes or manages SSRO environment data:

- are not outside of the UK;
- do not prevent or hinder the security and assurance agreements under Secure by Design for the SSRO; and
- are in all respects consistent with, and adhere to, the terms of the Contract, including without limitation the security conditions set out in Schedule 1 of the Contract.

6. Conflicts of interest

6.1 In delivering the services, the Supplier 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.

6.2 The Supplier's attention is drawn to the contractual clause 34 which contain obligations for managing potential and actual conflicts of interest: